Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет навчально-науковий центр заочної форми навчання
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти перший (бакалаврський)

Програмні засоби адміністрування застосунків Google Workspace

(тема)

Виконав:
здобувач 4 року навчання,
групи КІУКІиз-21-1
Денис ФІЛОНОВ
(власне ім'я, прізвище)

Спеціальність
123 «Комп'ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма
Комп'ютерна інженерія
(повна назва освітньої програми)

Керівник: ст. викл. Дмитро РОСІНСЬКИЙ
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри ЕОМ _____ Андрій КОВАЛЕНКО
(підпис) (власне ім'я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет навчально-науковий центр заочної форми навчання

Кафедра електронних обчислювальних машин

Рівень вищої освіти перший (бакалаврський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Комп'ютерна інженерія
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Філонову Денису Романовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Програмні засоби адміністрування застосунків Google Workspace

затверджена наказом по університету від "05" травня 2025 р. № 73 Стз

2. Термін подання здобувачем роботи до екзаменаційної комісії 17 червня 2025 р.

3. Вхідні дані до роботи 1. Сервіси Google Workspace.
2. Програмна платформа – будь-яка.
3. Аналіз питань адміністрування, безпеки і моніторингу в Google Workspace.

4. Перелік питань, що потрібно опрацювати у роботі
1. Огляд технологій та програмних засобів адміністрування Google Workspace
2. Методологія адміністрування застосунків Google Workspace
3. Розробка та впровадження програмних засобів адміністрування Google Workspace
4. Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій

Слайд-презентація – 15 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / терміни виконання етапів роботи	Примітка
1	Огляд технологій та програмних засобів	06.05.25-09.05.25	
	адміністрування Google Workspace		
2	Методологія адміністрування застосунків	10.05.25-15.05.25	
	Google Workspace		
3	Розробка програмних засобів адміністрування	16.05.25-28.05.25	
4	Впровадження програмних засобів	29.05.25-05.06.25	
5	Оформлення матеріалів кваліфікаційної роботи	06.06.25-09.06.25	
6	Подання кваліфікаційної роботи керівникові та	10.06.25-11.06.25	
	її попередній захист		
7	Подання кваліфікаційної роботи на рецензу-	12.06.25-13.06.25	
	вання		

Дата видачі завдання " 05 " травня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ ст. викл. Дмитро РОСІНСЬКИЙ
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 62 с., 9 рис., 3 табл., 1 дод., 44 джерела.

АВТЕНТИФІКАЦІЯ, АДМІНІСТРУВАННЯ, ВЕБ-ТЕХНОЛОГІЇ, ПОЛІТИКИ БЕЗПЕКИ, ЦИФРОВА ІНФРАСТРУКТУРА, GOOGLE WORKSPACE.

Метою роботи є аналіз, проєктування та розробка програмних засобів для ефективного адміністрування застосунків Google Workspace, зокрема – з використанням вбудованих та сторонніх інструментів автоматизації. Об’єктом дослідження є процеси адміністрування хмарних застосунків, предметом дослідження – програмні інструменти та методи адміністрування компонентів Google Workspace.

Новизна полягає у: систематизації сучасних методів адміністрування Google Workspace; створенні власного інструментарію для автоматизованого управління користувачами та політиками доступу; формалізації підходу до розробки кастомних рішень на основі API Google Workspace.

Результати кваліфікаційної роботи можуть бути використані адміністраторами систем для: оптимізації керування користувачами, групами та політиками доступу; автоматизації рутинних процесів у Google Workspace; впровадження систем моніторингу й аналітики активності користувачів.

Розроблені програмні засоби можуть бути адаптовані під потреби освітніх закладів, компаній малого і середнього бізнесу, а також державних установ, що використовують хмарні технології Google.

ABSTRACT

Bachelor’s thesis: 62 pages, 9 figures, 3 tables, 1 appendix, 44 sources.

AUTHENTICATION, ADMINISTRATION, DIGITAL INFRASTRUCTURE, GOOGLE WORKSPACE, SECURITY POLICIES, WEB TECHNOLOGIES.

The aim of this study is to analyze, design, and develop software tools for the efficient administration of Google Workspace applications, particularly through the use of built-in and third-party automation tools. The object of the research is the administration processes of cloud-based applications, while the subject is the software tools and methods used for managing components of Google Workspace.

The novelty of the work lies in the following: the systematization of modern methods for administering Google Workspace; the development of a proprietary toolkit for automated management of users and access policies; and the formalization of an approach to the development of custom solutions based on the Google Workspace API.

The results of this qualification project can be used by system administrators to: optimize user, group, and access policy management; automate routine processes within Google Workspace; and implement systems for monitoring and analyzing user activity.

The developed software tools can be adapted to meet the needs of educational institutions, small and medium-sized enterprises, and government organizations that utilize Google cloud technologies.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ПЗ – програмне забезпечення

2FA – двофакторна аутентифікація (англ., Two Factor Authentication)

AI – штучний інтелект (англ., Artificial intelligence)

API – інтерфейс програмування застосунків (англ., Application Programming Interface)

DLP – налаштовувані правила, що виявляють і блокують надсилання конфіденційної інформації поза межі організації (англ., Data Loss Prevention)

OU – організаційний підрозділ (англ., Organizational Unit)

UI – інтерфейс користувача (англ., User Interface)

ВСТУП

У сучасних умовах цифрової трансформації бізнесу та освіти хмарні сервіси стали невід'ємною частиною інфраструктури інформаційних систем. Google Workspace – один із найпопулярніших хмарних офісних пакетів, який використовується мільйонами організацій по всьому світу [1]. Його компоненти забезпечують зручне середовище для спільної роботи, зберігання документів, планування, спілкування та управління інформацією.

Разом із поширенням Google Workspace зростає потреба в ефективному адмініструванні його застосунків. Адміністратор має забезпечити контроль доступу, безпеку даних, відповідність політикам організації та ефективне використання ресурсів. Це завдання ускладнюється через постійний розвиток сервісів Google, багатоваріантність сценаріїв використання та необхідність автоматизації рутинних дій.

Тема кваліфікаційної роботи є особливо актуальною в умовах гібридної та дистанційної роботи, коли швидкість налаштування сервісів, моніторинг активності та управління користувачами стають критично важливими.

Метою роботи є аналіз, проєктування та розробка програмних засобів для ефективного адміністрування застосунків Google Workspace, зокрема – з використанням вбудованих та сторонніх інструментів автоматизації.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- проаналізувати сучасні підходи до адміністрування Google Workspace;
- дослідити можливості API Google Workspace та Google Admin Console;
- розробити програмні засоби для автоматизації типових задач адміністрування;
- провести експериментальну оцінку ефективності розроблених рішень.

У роботі використовуються такі методи: аналіз і синтез інформаційних систем; порівняльний аналіз програмних рішень; методи програмної інженерії; експериментальне моделювання; статистична обробка результатів.

Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, переліку джерел посилання та додатків. У першому розділі розглянуто теоретичні основи та аналіз існуючих засобів адміністрування. Другий розділ присвячений методології адміністрування Google Workspace. У третьому розділі описано процес проєктування та реалізації програмних рішень. Четвертий розділ містить результати експериментального дослідження ефективності запропонованого підходу.

1 ОГЛЯД ТЕХНОЛОГІЙ ТА ПРОГРАМНИХ ЗАСОБІВ АДМІНІСТРУВАННЯ GOOGLE WORKSPACE

1.1 Загальна характеристика Google Workspace як хмарної платформи

У сучасному цифровому середовищі ефективна організація командної роботи, обміну інформацією та управління комунікацією потребує використання комплексних хмарних платформ. Однією з найпоширеніших і найбільш інтегрованих систем такого типу є Google Workspace (до жовтня 2020 року відомий як G Suite) – хмарне середовище офісного класу, розроблене компанією Google для бізнесу, освіти та державного сектору [1].

Google Workspace включає набір застосунків, які забезпечують:

- комунікацію (електронна пошта, відеозв’язок, обмін повідомленнями);
- спільну роботу з документами;
- зберігання та керування файлами;
- організацію подій та керування часом;
- централізоване адміністрування та безпеку.

Основні компоненти Google Workspace розглянуті далі.

Gmail – корпоративна електронна пошта з розширеними функціями пошуку, фільтрації, антиспаму та інтеграцією з іншими сервісами. Пошта працює під доменом організації та підтримує двофакторну аутентифікацію, архівування листів через Google Vault, і делегування прав доступу [2].

Google Drive – хмарне сховище для збереження, синхронізації та спільного використання файлів. Підтримує організацію прав доступу на рівні файлів, папок і груп користувачів. Кожен користувач має персональне сховище, доступне з будь-якого пристрою, а адміністратор може контролювати квоти та політики збереження [3].

Google Docs, Sheets, Slides – набір офісних застосунків для створення

документів, електронних таблиць і презентацій. Забезпечують спільне редагування в реальному часі, перегляд історії змін, коментування, автоматичне збереження в Google Drive та інтеграцію з Gmail [4].

Google Calendar – інструмент для планування подій, створення зустрічей, синхронізації з іншими календарями та резервування ресурсів (наприклад, кімнат для нарад). Дає змогу організувати спільні графіки та отримувати сповіщення про події.

Google Meet і Google Chat – засоби для відеоконференцій та миттєвого обміну повідомленнями. Meet забезпечує високоякісні відеозустрічі з можливістю запису, автоматичного субтитрування, розмиття фону, інтеграції з Calendar. Chat підтримує теми обговорення (threaded chats), боти, інтеграцію з іншими інструментами.

Google Forms, Sites, Keep – додаткові інструменти для створення опитувальників, внутрішніх сайтів і нотаток.

Google Admin Console – центральний інструмент адміністрування, проаналізований у підрозділі 1.2.

Google Vault – сервіс для збереження, архівування та пошуку електронної інформації з метою юридичної відповідності та аудиту [5].

Google Apps Script – середовище розробки на базі JavaScript для створення кастомізованих автоматизаційних рішень, що взаємодіють із продуктами Google Workspace [6].

До переваг хмарної платформи Google Workspace можна віднести такі:

- інтеграція – сервіси Google Workspace тісно взаємодіють між собою, що спрощує потік роботи (наприклад, додавання документів до листа, планування подій із листів, надання спільного доступу з Drive);

- хмарність – повний доступ з будь-якого пристрою з інтернетом, відсутність потреби в локальній інфраструктурі;

- масштабованість – система легко адаптується до організацій будь-якого розміру;

- безперервне оновлення – автоматичні оновлення функцій без

потреби ручної інсталяції;

- інструменти для безпеки та контролю – аудит доступу, налаштування політик, вбудовані механізми резервного копіювання та відновлення;
- автоматизація – через Apps Script, API, сторонні інструменти.

Недоліки платформи:

- залежність від інтернет-з'єднання – робота з великими файлами або в нестабільних мережах може бути обмежена;
- обмежений контроль над фізичною інфраструктурою – важливо в контексті суворих політик конфіденційності;
- платність ліцензій – для повного функціоналу потрібні платні пакети (Business Standard, Enterprise), що може бути затратним для малих організацій;
- потреба у навчанні користувачів – особливо для переходу з традиційних офісних середовищ.

Загалом, Google Workspace є потужним та адаптивним інструментом для цифрової трансформації організацій, однак ефективне його впровадження та експлуатація потребують належного адміністрування, що й зумовлює актуальність подальших досліджень.

1.2 Аналіз програмних засобів адміністрування Google Workspace

Ефективне адміністрування Google Workspace є критично важливим для забезпечення безпеки, продуктивності та керованості хмарного середовища організації [1]. Google пропонує набір вбудованих та сторонніх інструментів для адміністрування, які охоплюють управління користувачами, пристроями, службами, політиками безпеки, а також API для автоматизації і розширення функціональності.

Google Admin Console – це центральна панель управління, яка дозволяє адміністраторам організацій здійснювати конфігурацію та моніторинг усіх сервісів Google Workspace. Її функціональні можливості охоплюють різні

аспекти, розглянуті нижче.

Управління обліковими записами користувачів: створення, видалення, редагування, призначення ліцензій, налаштування підписів, делегування доступів [7].

Групи та організаційні підрозділи: логічне структурування користувачів для диференційованого застосування політик. Групи також використовуються для налаштування розсилок і дозволів на доступ до документів або ресурсів [8].

Безпека та політики доступу: підтримка багатофакторної аутентифікації (MFA), блокування доступу з ненадійних пристроїв, увімкнення журналів аудиту, налаштування політик захисту даних (DLP), виявлення фішингових спроб тощо [9].

Керування пристроями: консоль дозволяє додавати правила для керування мобільними пристроями (Android/iOS), контролювати десктопи (Chrome OS), а також застосовувати політики безпеки та видаляти дані при втраті пристрою [10].

Аналітика і звітність: у вкладці «Reports» адміністратор може отримати доступ до щоденних та користувацьких звітів про активність користувачів, логіни, зловживання, використання сервісів тощо.

Google Admin Console має зручний інтерфейс, однак не всі функції доступні в базових тарифах, а для автоматизації часто потрібна інтеграція з API або сторонні інструменти. Оскільки Admin Console має обмежені можливості автоматизації та кастомізації, багато організацій використовують сторонні інструменти, розглянуті далі, які розширюють функціональність адміністрування.

BetterCloud – SaaS-платформа для глибокої автоматизації процесів у Google Workspace:

- автоматичне створення акаунтів;
- управління підписами;
- детекція загроз;

- делегування адміністративних ролей з обмеженим доступом [11].

GAM (Google Apps Manager) – CLI-інструмент з відкритим кодом, що дозволяє адмініструвати Google Workspace через скрипти:

- пакетне додавання/видалення користувачів;
- зміна налаштувань пошти, груп;
- робота з підписами, автовідповідачами;
- масові оновлення політик [12].

GAT+ (Google Apps Tools) – потужний аналітичний інструмент з модулями моніторингу активності, перевірки контенту документів, виявлення витоків даних, контролю спільного доступу [13].

CloudM – рішення для міграції, управління обліковими записами, бекапів, онбордингу/оффбордингу користувачів.

SpinOne, AODocs, Steegle, LumApps – забезпечують резервне копіювання, контроль версій, автоматизоване керування доступами, внутрішні портали та документообіг.

Використання таких рішень дозволяє масштабувати управління, прискорювати адміністративні процеси, а також досягати вищого рівня безпеки і відповідності стандартам (наприклад, GDPR, ISO 27001).

Google Workspace надає розширену інфраструктуру API, яка дозволяє автоматизувати майже всі адміністративні процеси. Найбільш поширені API:

- Admin SDK:

а) Directory API – для управління користувачами, групами, доменами, автентифікацією;

б) Reports API – для аналітики, отримання звітів про активність, використання сервісів;

в) Audit API – доступ до журналів аудиту (включення, зміни налаштувань, вхід до системи);

г) Data Transfer API – міграція даних між користувачами (наприклад, при звільненні працівника) [14];

- Gmail API, Calendar API, Drive API – для управління

повідомленнями, подіями, файлами та правами доступу програмним шляхом.

- Google Apps Script – високорівнева платформа на JavaScript для створення автоматизованих скриптів:

а) тригери на події (наприклад, надсилання листа після створення користувача);

б) створення кастомних панелей адміністрування;

в) щоденне резервне копіювання;

г) формування динамічних звітів [6];

- OAuth 2.0 + Service Accounts – для створення безпечних авторизованих програмних рішень, що взаємодіють із Workspace без постійного втручання користувача.

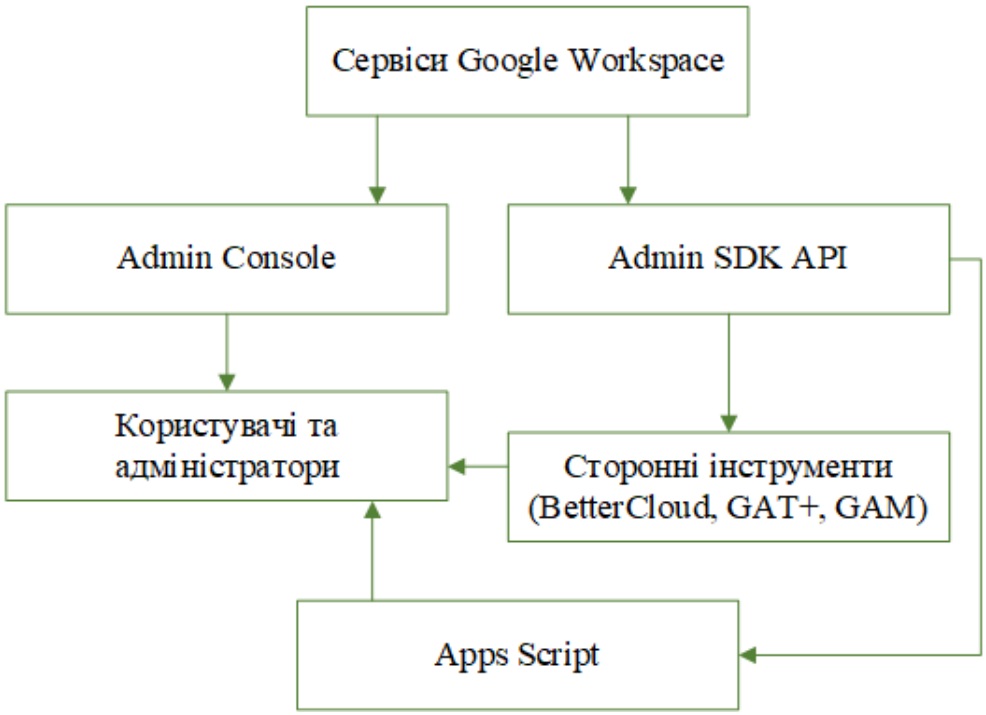

Рисунок 1.1 – Схема архітектури адміністрування Google Workspace

Інтеграція через API дозволяє організаціям реалізувати власні сценарії адміністрування, розширити функціональність стандартної консолі, адаптувати роботу до внутрішніх бізнес-процесів, а також забезпечити масштабування в умовах великої кількості користувачів.

Схема архітектури адміністрування Google Workspace (рисунок 1.1)

ілюструє взаємозв’язки між сервісами, Admin Console, API, скриптовими та сторонніми інструментами.

Порівняльна таблиця інструментів адміністрування Google Workspace (таблиця 1.1) дозволяє оцінити можливості кожного рішення за ключовими параметрами: автоматизація, масштабованість, тип, інтеграція тощо.

Таблиця 1.1 – Порівняння інструментів адміністрування Google Workspace

Інструмент	Тип	Автомати-зація	Масштабо-ваність	Інтеграція	Призначення
Admin Console	Вбудований GUI	Обмежена	Середня	Лише Google	Базове адміністрування
BetterCloud	SaaS платформа	Висока	Висока	Багатосервісна	Автоматизація та контроль
GAM	CLI-інструмент	Висока	Висока	Google Workspace	Скриптове адміністрування
GAT+	Аналітична платформа	Середня	Висока	Google Workspace	Моніторинг і безпека
Apps Script	Скриптовий інструмент	Висока	Середня	Google Workspace	Кастомні сценарії
Admin SDK API	REST API	Висока	Висока	Google Workspace	Розробка інструментів

1.3 Огляд актуальних досліджень та публікацій

Адміністрування хмарних середовищ Google Workspace розглядається в сучасних публікаціях з позицій ефективності, автоматизації, безпеки та впровадження інтелектуальних технологій. У цьому підрозділі здійснюється тематичний огляд і критичний аналіз ключових досліджень та галузевих кейсів, актуальних станом на 2021–2025 роки.

Ефективність Google Workspace в освітньому та корпоративному середовищі. В роботі [15] проведено емпіричне дослідження серед 50 респондентів в освітньому закладі у м. Макаті (Філіппіни), де Google

Workspace застосовувався для організації навчального процесу. Результати показали високий рівень задоволеності користувачів, особливо у контексті співпраці (середній бал – 4,61/5).

Критичний аналіз: незважаючи на позитивну оцінку, дослідження виявило обмеження у функціональності – брак дискового простору, складність адаптації нових користувачів і обмежена офлайн-доступність. Автор не подає кількісної оцінки продуктивності адміністратора чи показників навантаження, що обмежує репрезентативність досвіду з позицій IT-менеджменту.

Організаційна ефективність та бізнес-аналітика. Компанія Forrester Consulting провела дослідження Total Economic Impact (TEI), яке охоплювало понад 10 тис. користувачів у середовищі великих компаній [16]. За результатами дослідження, впровадження Google Workspace забезпечує економію 171 годин на одного працівника щорічно завдяки зменшенню надмірної електронної комунікації, дублювання документів та пришвидшенню спільної роботи.

Критичний аналіз: хоча наведені дані мають вражаючу аналітичну вагу, дослідження не розкриває специфіки адміністративних витрат або ефективності дій IT-відділів. Більшість результатів стосується саме кінцевих користувачів, а не адміністраторів, що звужує їх цінність у контексті теми кваліфікаційної роботи.

Автоматизація процесів адміністрування. Zenphi [17] демонструє кейси успішної no-code автоматизації управлінських процесів у Google Workspace:

- Gordon Food Service: зниження кількості звернень до служби підтримки на 83 %;
- Emerson College: скорочення часу на виконання адміністративних дій у 2,5 раза.

Критичний аналіз: рішення показують високу ефективність в умовах середніх і великих організацій, однак Zenphi потребує платної ліцензії, навчання персоналу та досвіду побудови логіки потоків дій. Відомості про

обробку конфліктів доступу, масштабованість у багатодоменних середовищах та логування дій обмежені.

Програмні засоби контролю безпеки. В роботі [18] автори проаналізували поведінку користувачів у Google Workspace щодо надання дозволів стороннім застосункам. Було встановлено, що користувачі часто не розуміють рівень доступу, який вони надають, що створює критичні вектори атаки для фішингу, витоку даних тощо.

Критичний аналіз: дослідження висвітлює важливу проблему слабкої обізнаності користувачів, однак фокус лише на кінцевих користувачах, а не адміністраторах. Водночас, не запропоновано практичних рекомендацій щодо автоматичного обмеження або моніторингу OAuth-доступу, що було б корисно для адміністраторів.

Інтеграція AI в адміністрування Workspace. Google презентував Gemini for Workspace [19] – платформу, що дозволяє автоматично генерувати відповіді на листи, структурувати таблиці та формувати документи за запитом. У Workspace інтегруються інтелектуальні агенти, здатні створювати «flows» – ланцюжки дій у відповідь на події.

Критичний аналіз: хоча це відкриває нову еру в адмініструванні, рішення перебувають на етапі обмеженого корпоративного впровадження. Продукти потребують додаткових модулів безпеки, аудитів, і вимагають перегляду існуючих політик ITSM у компанії. Також, адміністратор поки не має повноцінного контролю за логікою таких agent-based flows.

Інструменти адміністрування на базі API та скриптів. У дослідженні SheetMind [20] продемонстровано ефективність застосування LLM (Large Language Models) у Google Sheets як адміністративного середовища. Система досягла 80 % точності в простих адміністративних запитах (генерація звітів, зміна прав доступу тощо).

Критичний аналіз: хоча результати перспективні, поточна точність рішень LLM для складних сценаріїв (багатокрокових або умовних) ще недостатня для критично важливого адміністрування. Крім того, в

дослідженні не приділено уваги питанням безпеки дій, які виконує LLM.

На рисунку 1.2 наведена концептуальна мапа, яка відображає ключові напрями досліджень у сфері адміністрування Google Workspace. Центральною темою є адміністрування Google Workspace. Визначено чотири основні піднапрями:

- автоматизація;
- безпека;
- AI-інтеграція;
- освітнє використання.

До кожного напряму прив'язані конкретні інструменти, дослідники або приклади: наприклад, Zenphi і GAM для автоматизації, Gemini і SheetMind для AI, Vault/SSO для безпеки тощо.

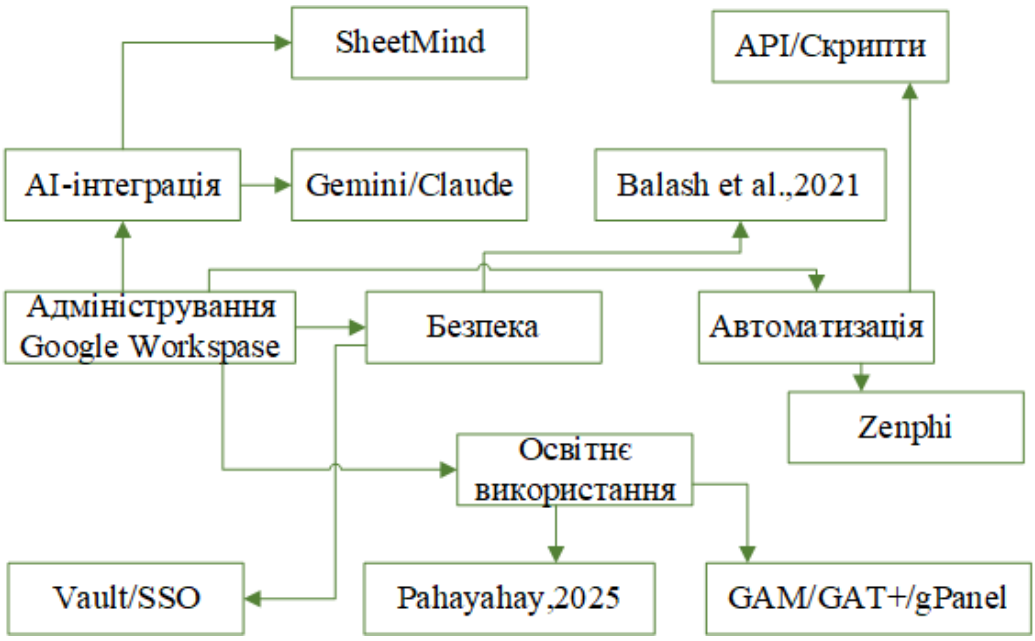

Рисунок 1.2 – Концептуальна мапа досліджень з адміністрування Google Workspace

1.4 Висновки до розділу

Сучасні дослідження одностайно визнають високу ефективність Google Workspace, проте існує помітна диференціація між ефективністю для

кінцевих користувачів і для адміністраторів. Інструменти автоматизації (Zenphi, SheetMind) показують високу потенційну цінність, але потребують впровадження механізмів контролю, журналювання та масштабованості. Інтеграція AI (Gemini, Claude) формує тренд на персоніфіковану автоматизацію, однак поки що такі рішення не мають широкої підтримки у адміністративному модулі.

Питання контролю сторонніх додатків та кібербезпеки залишаються відкритими, і потребують додаткових досліджень і розробки захисних стратегій.

2 МЕТОДОЛОГІЯ АДМІНІСТРУВАННЯ ЗАСТОСУНКІВ GOOGLE WORKSPACE

2.1 Підходи до адміністрування користувачів і груп

У хмарному середовищі Google Workspace, адміністрування користувачів і груп є критичним компонентом, який визначає, наскільки ефективно організація зможе забезпечити доступ до своїх ресурсів, керувати повноваженнями, дотримуватися політик безпеки та масштабувати свою структуру [1, 23]. В умовах динамічного зростання організацій, хибне або неструктуроване адміністрування може призвести до витоків даних, хаосу в доступі до ресурсів, перевантаження адміністраторів та неузгоджених бізнес-процесів.

У Google Workspace ця діяльність реалізується за допомогою кількох базових механізмів: керування акаунтами користувачів, адміністрування груп, а також призначення ролей та дозволів адміністраторам.

2.1.1 Керування акаунтами користувачів

У Google Workspace кожен користувач має унікальний обліковий запис у вигляді електронної адреси в межах домену організації (наприклад, user@company.com). Адміністратор організації відповідає за створення, налаштування, підтримку та видалення цих облікових записів [24].

Базові функції управління обліковими записами:

- створення облікового запису включає заповнення атрибутів (ім’я, прізвище, адреса, організаційний підрозділ, посада) через Google Admin Console або за допомогою скриптів і API (наприклад, Directory API);
- призначення ліцензій (наприклад, Business Starter, Business Standard, Education Plus) регламентує доступ користувача до таких сервісів, як Gmail,

Drive, Meet тощо;

- зміна властивостей облікового запису – переміщення між організаційними підрозділами (OU), оновлення атрибутів профілю, блокування або тимчасове призупинення доступу;

- видалення або деактивація користувача супроводжується передачею власності на документи іншому обліковому запису (через Data Transfer API або вручну в Admin Console);

- автоматизоване керування (наприклад, створення нових облікових записів при надходженні HR-запиту через Google Forms з Apps Script) зменшує ручну працю та ризик людських помилок.

Приклад: компанія з понад 500 співробітниками може інтегрувати HR-систему з Workspace через API, щоб при додаванні нового працівника автоматично створювався обліковий запис, призначалась ліцензія, налаштовувалась підпис електронної пошти та надавався доступ до потрібних груп і файлів.

Рекомендація: для великих організацій доцільно використовувати Google Cloud Directory Sync (GCDS) для автоматичного імпорту облікових записів із локальної Active Directory до Google Workspace.

2.1.2 Групові політики доступу

Групи – це логічні об’єднання користувачів, що дозволяють спростити керування доступом до спільних ресурсів [25]. Вони функціонують як розсилкові списки, групи безпеки та об'єкти керування політиками.

Типи груп у Google Workspace:

- розсилкові групи (mailing lists): використовуються для одночасного надсилання повідомлень великій кількості користувачів;

- групи доступу (access groups): контролюють надання прав до папок на Google Drive, календарів, спільних дисків, опитувальників;

- динамічні групи: формуються автоматично на основі певних

атрибутів користувачів (наприклад, підрозділ, місто). Налаштовуються через Directory API або Google Cloud Identity.

Керування групами включає:

- додавання/видалення учасників (вручну або пакетно);
- налаштування прав (читання, редагування, адміністрування);
- контроль, хто може надсилати листи на групу (усі, лише учасники, тільки адміністратори);
- можливість архівації листування групи (для службових розсилок).

Приклад: група hr@company.com може включати всі облікові записи HR-відділу, і використовуватись як для спілкування, так і для доступу до політик, форм, файлів у спільному диску.

Практика: для зниження навантаження адміністраторів рекомендується створювати вкладені групи (наприклад, staff@company.com може включати hr@, it@, sales@) і делегувати частину управління локальним адміністраторам груп.

2.1.3 Ролі та дозволи адміністраторів

Google Workspace підтримує рольову модель керування, що дозволяє розмежувати права доступу та делегувати частину адміністративних функцій, зберігаючи централізований контроль [26]. Схема ролевої моделі адміністраторів (рисунок 2.1) ілюструє ієрархію типових ролей у Google Workspace та можливість делегування повноважень від суперадміністратора.

Основні ролі:

- суперадміністратор (Super Admin): має повний доступ до всіх налаштувань, включно з користувачами, групами, сервісами, безпекою;
- адміністратор користувачів (User Management Admin): може створювати й змінювати акаунти, але не має доступу до фінансових, безпекових або конфіденційних налаштувань;
- адміністратор груп: управляє лише Google Groups;

- службовий адміністратор: має права лише на один або кілька сервісів (наприклад, тільки Gmail);
- кастомні ролі: можуть бути створені адміністратором із вибірковим набором дозволів (наприклад, «Адміністратор 1-го рівня підтримки», який може лише скидати паролі).

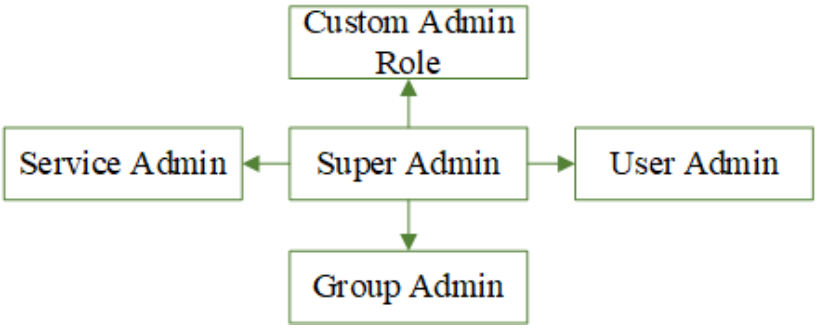

Рисунок 2.1 – Схема ролевої моделі адміністраторів у Google Workspace

Контроль за адміністраторами:

- усі дії адміністраторів фіксуються в Admin Audit Log;
- Google рекомендує використовувати багатофакторну автентифікацію для всіх адміністративних облікових записів;
- політика безпеки повинна передбачати регулярний аудит ролей та верифікацію їх актуальності.

Приклад: для відділу підтримки створюється роль з доступом лише до операцій скидання пароля й перевірки логінів, але без доступу до редагування груп чи перегляду Drive.

Таблиця типів груп у Google Workspace (таблиця 2.1) надає опис призначення, способів керування та прикладів використання.

Схема життєвого циклу облікового запису користувача (рисунок 2.2) показує послідовність дій від моменту запиту на створення облікового запису до його остаточного видалення.

Таблиця 2.1 – Таблиця типів груп у Google Workspace

Тип групи	Призначення	Керування	Приклад
Розсилка	Надсилання листів великій кількості адресатів	Адміністратор вручну / через API	staff@company.com
Група доступу	Налаштування доступу до ресурсів (Drive, Calendar)	Адміністратор / через OU / політики доступу	marketing-access@company.com
Динамічна група	Автоматичне формування за атрибутами користувачів	Автоматичне (через Directory API)	users-from-Kyiv@company.com

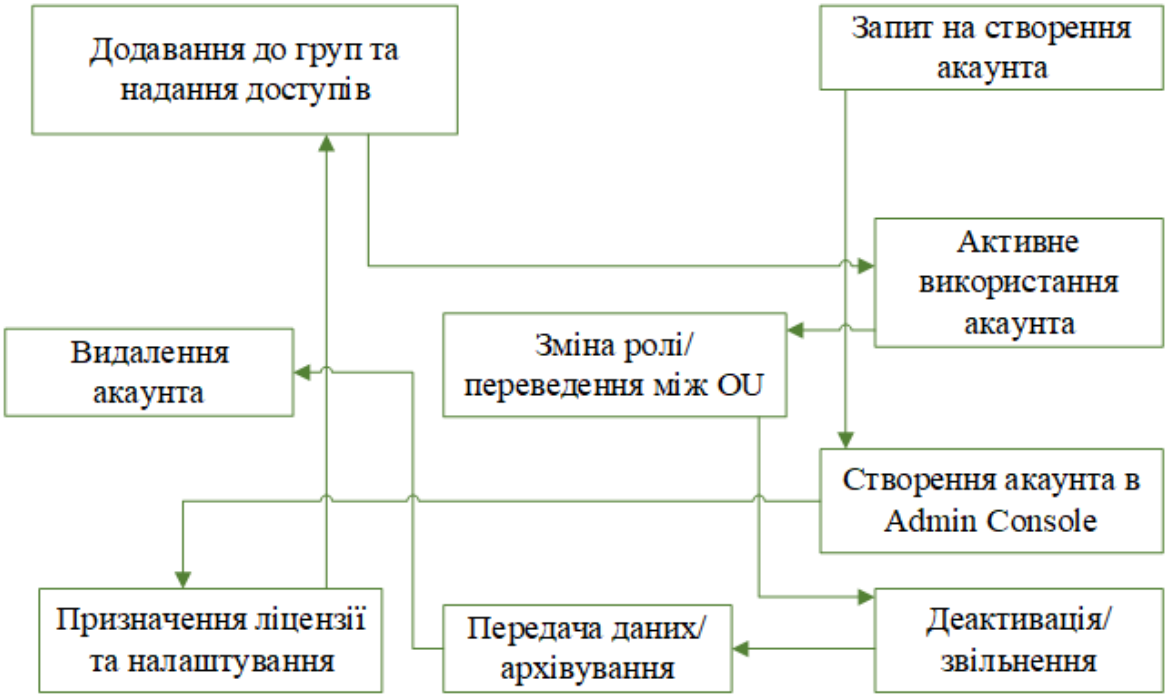

Рисунок 2.2 – Схема життєвого циклу облікового запису користувача у Google Workspace

2.2 Організація безпеки в Google Workspace

Інформаційна безпека є фундаментальним елементом будь-якої цифрової інфраструктури. У випадку Google Workspace – як корпоративної хмарної платформи – безпека охоплює не лише захист конфіденційності та цілісності даних, а й контроль доступу, моніторинг активності, аудит подій та відповідність міжнародним стандартам (наприклад, ISO/IEC 27001, GDPR, FedRAMP тощо) [28]. Даний підрозділ присвячено розгляду багаторівневої моделі захисту Google Workspace, а також методів автентифікації, авторизації та реагування на інциденти.

2.2.1 Багаторівневий захист інформації

Google Workspace реалізує багаторівневу архітектуру безпеки, яка включає фізичну, мережеву, прикладну і користувацьку складові. Захист даних базується на принципах, які розглянуті далі.

Шифрування даних на всіх етапах: Google Workspace використовує TLS 1.2/1.3 для шифрування трафіку між клієнтом і сервером, а також AES-256 для шифрування даних у стані спокою [29].

Сегментація даних: кожен користувач і організація має логічно ізольований набір даних.

Резервне копіювання і реплікація: дані зберігаються одночасно в кількох дата-центрах для забезпечення відмовостійкості.

Контроль доступу до інфраструктури: адміністратори можуть обмежити доступ до сервісів за IP-адресами, географічним розташуванням чи статусом пристрою (керований/некерований).

Приклад: політика «context-aware access» дозволяє надати користувачеві доступ до Gmail лише з корпоративного пристрою в робочий час і з певного регіону [30].

2.2.2 Управління аутентифікацією та авторизацією

Для запобігання несанкціонованому доступу Google Workspace пропонує розширені засоби автентифікації та контролю ідентифікації користувачів.

Багатофакторна автентифікація (2FA): підтримуються коди через SMS, Google Authenticator, апаратні ключі безпеки (FIDO2), push-підтвердження через додаток Google Prompt. За замовчуванням 2FA вмикається для адміністраторів [31].

Єдиний вхід (SSO): за допомогою протоколу SAML 2.0 можна інтегрувати Workspace з іншими системами автентифікації, такими як Microsoft Azure AD, Okta або Keycloak [32].

Password Alert & Strength Policies: система може вимагати складні паролі, забороняти повторне використання попередніх, та сповіщати про спроби входу з підозрілих локацій.

Безпечна автентифікація для API-доступу: доступ через OAuth 2.0 або службові облікові записи із ретельним контролем дозволів.

Рекомендація: варто налаштувати enforcement policy для обов’язкового використання 2FA, а також заборонити використання доступу до Workspace із пристроїв без екранного блокування або актуального антивірусного ПЗ.

2.2.3 Моніторинг і реагування на інциденти

Google Workspace містить вбудовані механізми моніторингу безпеки, які надають адміністраторам прозорість щодо дій користувачів, змін конфігурацій і можливих загроз. Основні інструменти перелічені далі.

Security Center: єдина панель огляду безпеки організації. Містить звіти про фішинг, витоки даних, нестандартну поведінку облікових записів.

Investigation Tool (для Enterprise версій): дозволяє виконувати детальне розслідування подій, пов’язаних із повідомленнями, файлами, входами в

систему.

Audit Logs:

- Admin Audit Log – дії адміністраторів (зміни паролів, додавання користувачів, редагування груп);
- Drive Audit Log – доступ до файлів, зміни дозволів, видалення/відновлення;
- Login Audit Log – вхід у систему, успішні/невдалі спроби, геолокація, пристрої.

Alert Center – центр сповіщень про критичні події безпеки, включно з витоками, підозрілими входами, несанкціонованими змінами.

DLP (Data Loss Prevention) – налаштовувані правила, що виявляють і блокують надсилання конфіденційної інформації (номери карток, паролі тощо) поза межі організації.

Приклад: адміністратор може отримати автоматичне сповіщення про надсилання листа з вкладеним PDF-файлом, що містить 16-значне число (підозра на кредитну картку), і заблокувати лист до розслідування.

Кращі практики:

- встановлювати сповіщення для всіх змін ролей адміністраторів;
- щоденно аналізувати звіти про підозрілу активність;
- використовувати хмарні SIEM-платформи (наприклад, Splunk, Exabeam, Chronicle) для агрегації подій із Workspace.

Схема архітектури безпеки Google Workspace (рисунок 2.3) відображає ключові компоненти захисту. Користувачі проходять автентифікацію через 2FA, SSO або OAuth. Політики доступу (Context-Aware Access) регулюють, чи може користувач отримати доступ до сервісів Workspace. Адміністратори мають доступ до інструментів безпеки (DLP, Alert Center), які керують і аналізують журнали подій. Журнали можуть бути інтегровані в зовнішні системи безпеки (SIEM). Вся інфраструктура розгорнута на Google Cloud Platform з вбудованими механізмами фізичного та мережевого захисту.

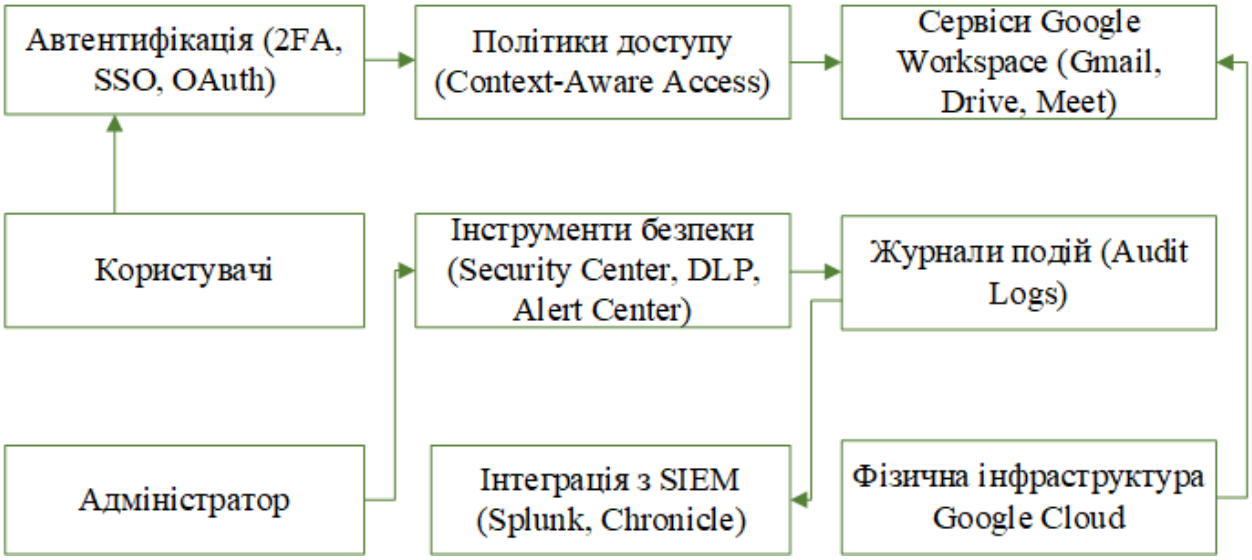

Рисунок 2.3 – Схема архітектури безпеки Google Workspace

2.3 Методи моніторингу та аналітики у Google Workspace

Моніторинг дій користувачів, системної активності та конфігурацій безпеки в Google Workspace є не лише інструментом контролю, але й засобом забезпечення відповідності політикам організації, виявлення загроз та оптимізації процесів управління. У порівнянні з традиційними локальними системами, хмарна платформа Google пропонує централізовані, автоматизовані та масштабовані інструменти, що охоплюють різні рівні аналізу – від перегляду історії активності окремих користувачів до глибокої кореляції подій у системах класу SIEM.

Google Workspace містить вбудовану систему логування, яка охоплює найважливіші області діяльності користувачів та адміністраторів. Ключовим джерелом інформації є Audit Logs – журнали, які фіксують дії у таких сервісах як Gmail, Google Drive, Google Meet, Google Calendar, Admin Console тощо. Вони містять відомості про те, хто, коли і з якого пристрою виконав певну дію: наприклад, перегляд або видалення документа, зміну пароля, створення події в календарі, додавання користувача до групи [33].

Такі журнали доступні через інтерфейс адміністратора (Admin Console → Reports → Audit log), а також через Reports API. Останнє є надзвичайно

важливим для автоматизованого збору та обробки даних, особливо у великих організаціях. Наприклад, з використанням Reports API можна щодня імпортувати дані до Google Sheets або до внутрішньої системи звітності для створення графіків використання сервісів, виявлення підозрілої поведінки або перегляду завантажень великої кількості файлів з одного акаунта [34].

Особливе значення має Admin Audit Log, який містить детальну інформацію про дії адміністратора: зміну політик, призначення ролей, активацію/деактивацію акаунтів. Це дозволяє відстежувати потенційно небезпечні або несанкціоновані дії навіть з боку внутрішнього персоналу [35].

Доповненням до логування є Alert Center – система сповіщення, яка попереджає про критичні події безпеки: спроби фішингових атак, зломи облікових записів, незвичайні спроби входу або втрати доступу. Вона має вбудовані шаблони оповіщень, а також можливість налаштування власних правил [36].

Інтегрованим аналітичним інструментом в Google Workspace є Security Dashboard, де доступна агрегована інформація про рівень безпеки організації: кількість активних користувачів з 2FA, сервіси з підвищеною кількістю інцидентів, підозрілі зовнішні додатки тощо. У версіях Enterprise та Education Plus доступна також система розслідування інцидентів – Investigation Tool – яка дозволяє проводити цілеспрямований пошук по логах, із застосуванням фільтрів і відповідних дій (наприклад, блокування користувача або доступу до файлу).

Приклад: за допомогою Drive Audit Log адміністратор може виявити, що певний працівник завантажив понад 100 файлів за одну сесію, а Alert Center повідомить, якщо він поділився цими файлами з особами поза організацією.

Хоча внутрішні засоби Google Workspace задовольняють більшість базових потреб, великі компанії, державні установи та організації, що підпадають під дію стандартів на зразок ISO 27001, HIPAA або GDPR,

потребують професійної інтеграції з системами класу SIEM (Security Information and Event Management).

До найпоширеніших рішень належать зазначені нижче.

Google Chronicle – власна SIEM-платформа, орієнтована на роботу з Google Workspace та Google Cloud Platform. Вона дозволяє обробляти сотні тисяч подій щосекунди, підтримує історичний аналіз на рівні місяців і років, а також має модулі на основі штучного інтелекту для виявлення аномалій [37].

Splunk – одна з найпотужніших комерційних SIEM-систем, яка дозволяє створювати кастомні панелі моніторингу, застосовувати правила для виявлення інцидентів, надсилати оповіщення і автоматично запускати сценарії реагування. Існує офіційний конектор до Google Workspace через API [38].

Datadog, Exabeam, IBM QRadar – ці рішення підтримують глибоку інтеграцію через конектори або API. З їх допомогою можна поєднати дані з Google Workspace із логами інших джерел: фаєрволів, антивірусів, проксі-серверів, VPN тощо.

Усі ці системи підтримують:

- довготривале зберігання логів;
- застосування інтелектуальних алгоритмів для аналізу поведінки користувачів (UEBA);
- створення тригерів на порушення політик;
- автоматизоване реагування на інциденти через SOAR-платформи.

Приклад: якщо користувач входить у свій акаунт з нетипового місцезнаходження без 2FA, система Splunk виявляє цю подію, створює інцидент, сповіщає адміністратора і запускає блокування доступу через API.

Схема архітектури інтеграції Google Workspace з системами моніторингу (рисунок 2.4) демонструє типову архітектуру інтеграції. Користувачі та адміністратори взаємодіють із сервісами Google Workspace. Події фіксуються у Audit Logs і доступні через Reports API. Журнали

передаються у SIEM / SOC системи (наприклад, Splunk, Chronicle, Datadog). Далі події аналізуються, візуалізуються в дашбордах, формуються оповіщення. У разі інциденту запускаються сценарії автоматизованого реагування (SOAR).

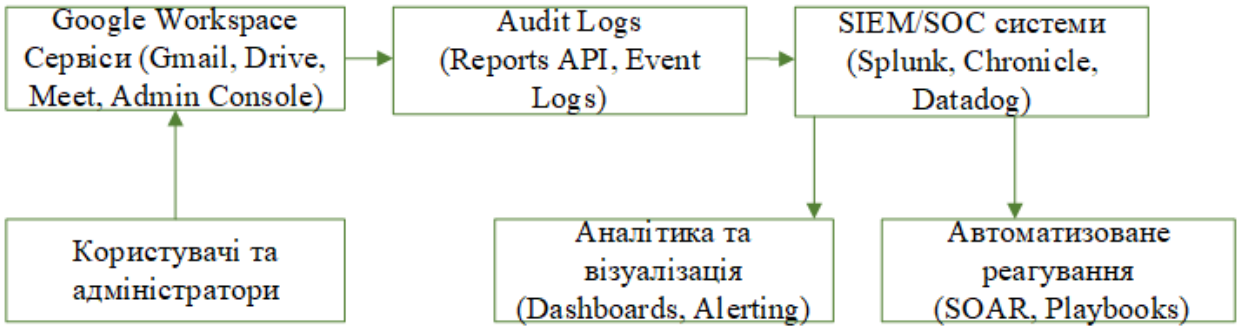

Рисунок 2.4 – Схема архітектури інтеграції Google Workspace з системами моніторингу

2.4 Висновки до розділу

Ефективне адміністрування користувачів і груп у Google Workspace базується на принципах:

- централізованого управління даними облікових записів із можливістю делегування;
- використання груп для побудови політик доступу;
- застосування гнучкої ролевої моделі для розподілу повноважень.

Інструменти Workspace дозволяють реалізувати ці принципи за допомогою Admin Console, API [27], сторонніх платформ і скриптів. Їх правильне поєднання є передумовою масштабованого, безпечного та ефективного адміністрування.

Google Workspace забезпечує високий рівень інформаційної безпеки завдяки комплексному багаторівневому підходу до захисту даних, підтримці сучасних протоколів автентифікації, а також інтегрованим механізмам моніторингу. Однак, реальна ефективність захисту залежить від політик, які

впроваджуються адміністраторами. Встановлення обов’язкової 2FA, регулярний аудит активності, налаштування DLP, розмежування прав доступу – критично важливі кроки для забезпечення надійної безпеки в організаціях, що працюють із Google Workspace.

Google Workspace реалізує потужну модель моніторингу та аналітики, яка поєднує в собі як візуальні, так і програмні інструменти для виявлення, аналізу та реагування на події. Вбудовані журнали, API для звітності та система оповіщення задовольняють потреби малих і середніх організацій. Водночас, для підприємств із високими вимогами до безпеки рекомендовано розгортання систем SIEM з глибокою інтеграцією через API. Завдяки цьому можливе вчасне виявлення загроз, контроль відповідності політик, аудит критичних змін і автоматизована реакція на інциденти.

3 РОЗРОБКА ТА ВПРОВАДЖЕННЯ ПРОГРАМНИХ ЗАСОБІВ АДМІНІСТРУВАННЯ GOOGLE WORKSPACE

3.1 Архітектура програмного рішення

Ефективне адміністрування Google Workspace потребує не лише ручного керування через Google Admin Console, але й створення автоматизованих, модульних і масштабованих програмних рішень. Ці рішення повинні враховувати як внутрішні вимоги організації, так і обмеження, пов’язані з API Google, політиками безпеки та захистом даних. У цьому підрозділі розглядається концептуальна архітектура таких засобів, їх компоненти, а також моделі взаємодії з API Google Workspace.

3.1.1 Загальна структура програмних компонентів

Архітектура програмного комплексу для адміністрування Google Workspace включає три основні рівні.

Інтерфейс користувача (UI Layer) – веб-застосунок або панель керування, через який адміністратор взаємодіє із системою. Розробляється з використанням HTML, CSS, JavaScript, Google Apps Script або сучасних фреймворків на зразок React.

Логіка застосунку (Application Layer) – реалізує основні функції: управління користувачами, групами, політиками доступу, запити до API, логування дій. Цей рівень також включає правила бізнес-логіки, обробку подій та авторизацію запитів.

Інтеграційний рівень (Integration Layer) – здійснює безпосередню взаємодію з Google Workspace API (Admin SDK, Directory API, Gmail API тощо). Також може містити шлюзи до зовнішніх сервісів (Slack, Jira, DataDog, Splunk).

Оскільки всі дії з адміністрування виконуються через безпечні інтерфейси REST API Google, важливо забезпечити коректну реалізацію механізмів автентифікації (OAuth 2.0) та обмеження доступу через Scopes [39].

Приклад: для створення інтерфейсу призначення користувача до групи, застосунок надсилає POST-запит до https://admin.googleapis.com/admin/directory/v1/groups/{groupKey}/members з відповідним тілом запиту та токеном доступу.

3.1.2 Інтеграція з Google Workspace API

Google Workspace надає розвинуту екосистему API, об’єднаних у Admin SDK, що включає:

- Directory API – керування акаунтами користувачів, групами, OU, політиками доступу;
- Reports API – доступ до журналів активності, звітів про використання;
- Gmail API – робота з поштовими скриньками, фільтрами, делегуванням;
- Calendar API, Drive API, Sites API, Groups Settings API – налаштування окремих сервісів;
- Chrome Policy API – централізоване керування пристроями.

Для авторизації використовується OAuth 2.0 або службові облікові записи (Service Accounts) з делегуванням доменної авторизації. Це дозволяє застосунку працювати від імені адміністратора без потреби вручну входити в обліковий запис [40].

Особливої уваги потребує правильне управління дозволами (scopes), адже доступ до API може відкривати повний контроль над акаунтами. З міркувань безпеки слід використовувати найменший необхідний рівень доступу (principle of least privilege).

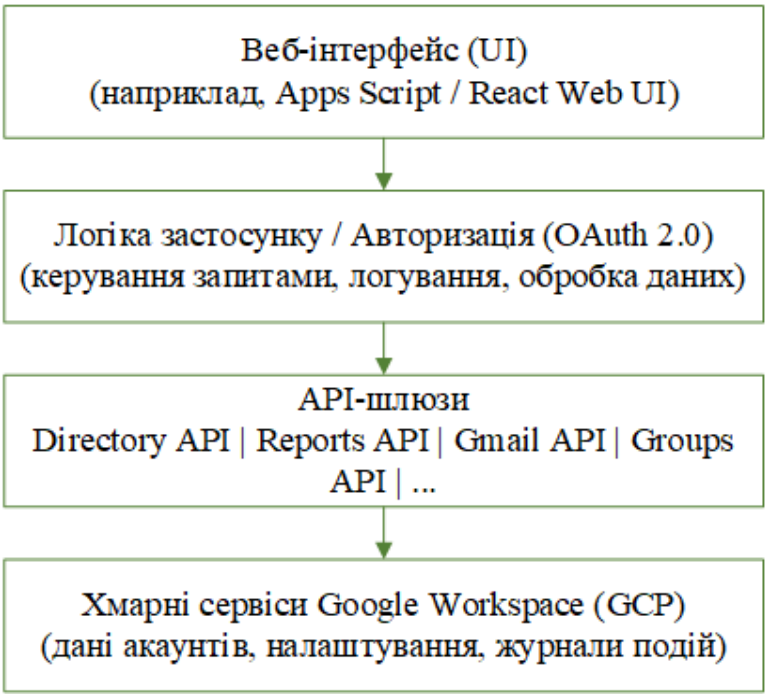

Рисунок 3.1 – Узагальнена архітектура системи

Отже, створення програмних засобів для адміністрування Google Workspace передбачає реалізацію багаторівневої архітектури, що включає інтерфейс користувача, логіку обробки запитів і захищену взаємодію з API Google. Завдяки доступності повнофункціонального SDK та потужних REST-інтерфейсів розробники мають змогу створювати як внутрішні утиліти, так і масштабовані корпоративні рішення, інтегровані з іншими інформаційними системами. Дотримання принципів мінімізації дозволів, контроль авторизації та забезпечення журналювання є обов’язковими умовами безпечного впровадження таких рішень.

3.2 Розробка програмних інструментів автоматизації адміністрування

Автоматизація процесів адміністрування Google Workspace дозволяє значно знизити навантаження на IT-персонал, підвищити точність виконання рутинних операцій та зменшити ймовірність помилок, пов’язаних з людським фактором. Основу для такої автоматизації становлять доступні API Google Workspace, мова Google Apps Script, можливості створення кастомних

інтерфейсів, а також механізми інтеграції з іншими хмарними системами.

3.2.1 Використання Google Apps Script для автоматизації

Google Apps Script є високорівневою скриптовою мовою, побудованою на основі JavaScript, яка дозволяє створювати автоматизовані сценарії для взаємодії з сервісами Google Workspace – Gmail, Drive, Calendar, Admin SDK, і т.ін. [41]. Основною перевагою Apps Script є його тісна інтеграція з інтерфейсами Google, що дозволяє без додаткового середовища виконувати сценарії з документів, форм або веб-застосунків.

Приклад автоматизації: створення Apps Script-функції, яка щодня перевіряє користувачів без активованої 2FA та надсилає їм автоматичне нагадування електронною поштою:

```
function notifyUsersWithout2FA() {
  const users = AdminDirectory.Users.list({domain:
'example.com'}).users;
  const nonCompliant = users.filter(u => !u.isEnrolledIn2Sv);
  for (const user of nonCompliant) {
    GmailApp.sendEmail(user.primaryEmail, "2FA Required",
"Please enable 2-step verification.");
  }
}
```

Apps Script також дозволяє створювати тригери на події, формувати кастомні звіти та публікувати інтерфейси у вигляді веб-додатків.

3.2.2 Створення веб-застосунків для управління користувачами

Для більших організацій доцільно розробляти веб-застосунки, які забезпечують інтерфейс для взаємодії з адміністративними функціями Google Workspace, приховуючи складність API від кінцевого користувача [42]. Наприклад, застосунок може включати наступні функції:

- створення нового користувача з прив’язкою до відповідного

підрозділу;

- масове оновлення політик доступу для груп користувачів;
- інтерактивне налаштування дозволів і доступу до документів;
- управління правами на Google Meet, Calendar, Shared Drives.

Такі веб-застосунки можуть бути реалізовані з використанням:

- frontend: React/Vue + Material UI;
- backend: Node.js / Python (Flask, FastAPI);
- автентифікація: OAuth 2.0 або авторизація через Google Identity Services [43];
- доступ до API: через SDK Google API Client Libraries.

Приклад: кастомний React-додаток для керування групами користувачів через Directory API із можливістю перегляду структури OU, додавання нових співробітників, інтеграції з внутрішньою кадровою системою.

3.2.3 Інтеграційні рішення із зовнішніми сервісами

Багато організацій інтегрують Google Workspace з іншими хмарними платформами для покращення керованості [44], зокрема:

- HR-системи (Workday, BambooHR) – автоматичне створення акаунтів нових співробітників;
- SIEM-платформи (Splunk, Chronicle) – передача логів безпеки для моніторингу;
- Trello, Jira, Slack – автоматичне створення завдань чи повідомлень на основі подій у Workspace;
- CRM-системи (Hubspot, Zoho) – інтеграція контактів і календарів.

Такі інтеграції реалізуються через REST API, Google Apps Script Webhooks, або використання Google Cloud Pub/Sub для подій. У більш складних випадках використовується проміжний сервер-шлюз, який конвертує події Google Workspace у формат, зрозумілий іншій системі.

Сценарій інтеграції: при звільненні працівника HR-система надсилає сигнал до API Google Workspace, який:

- видаляє доступ користувача;
- резервує дані поштової скриньки;
- пересилає листи на обліковий запис керівника;
- генерує запис у SIEM-системі.

3.3 Рішення для адміністрування Google Workspace

Яе було зазначено, автоматизація адміністративних процесів у Google Workspace можлива як за допомогою вбудованих засобів (Google Apps Script), так і шляхом створення повноцінних веб-застосунків та інтеграцій із зовнішніми сервісами. Такі рішення забезпечують масштабованість, гнучкість та відповідність політикам безпеки, водночас знижуючи навантаження на IT-персонал. Використання API, OAuth 2.0 та принципів мінімізації прав доступу є критичними для безпечного впровадження подібних інструментів.

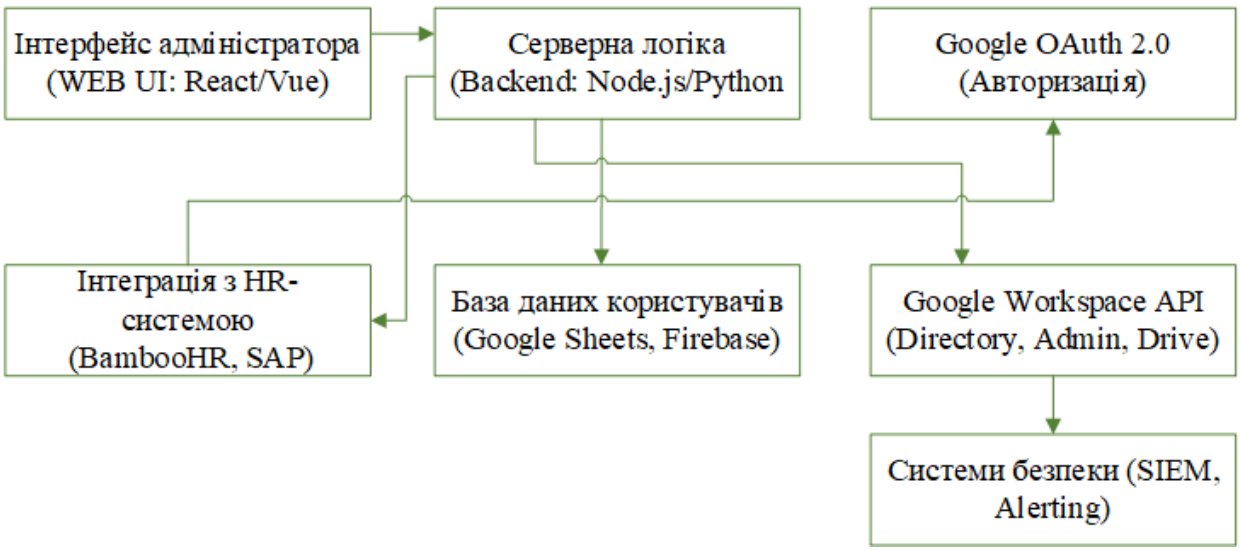

Рисунок 3.2 – Схема архітектури прикладного рішення для адміністрування Google Workspace

Схема архітектури прикладного рішення для адміністрування Google Workspace наведена на рисунку 3.2. Інтерфейс адміністратора (React/Vue) дозволяє взаємодіяти з сервером через API.

Серверна логіка (Node.js/Python) обробляє запити, керує доступом і взаємодіє з:

- Google OAuth 2.0 для авторизації;
- Google Workspace API для адміністрування облікових записів, груп, прав;
- базою даних користувачів (наприклад, Google Sheets або Firebase);
- HR-системою, що надсилає/отримує інформацію про працівників;
- системами безпеки (SIEM) для аудиту та реагування на події.

Запропонована схема процесу розробки та впровадження програмних засобів адміністрування Google Workspace показана на рисунку 3.3.

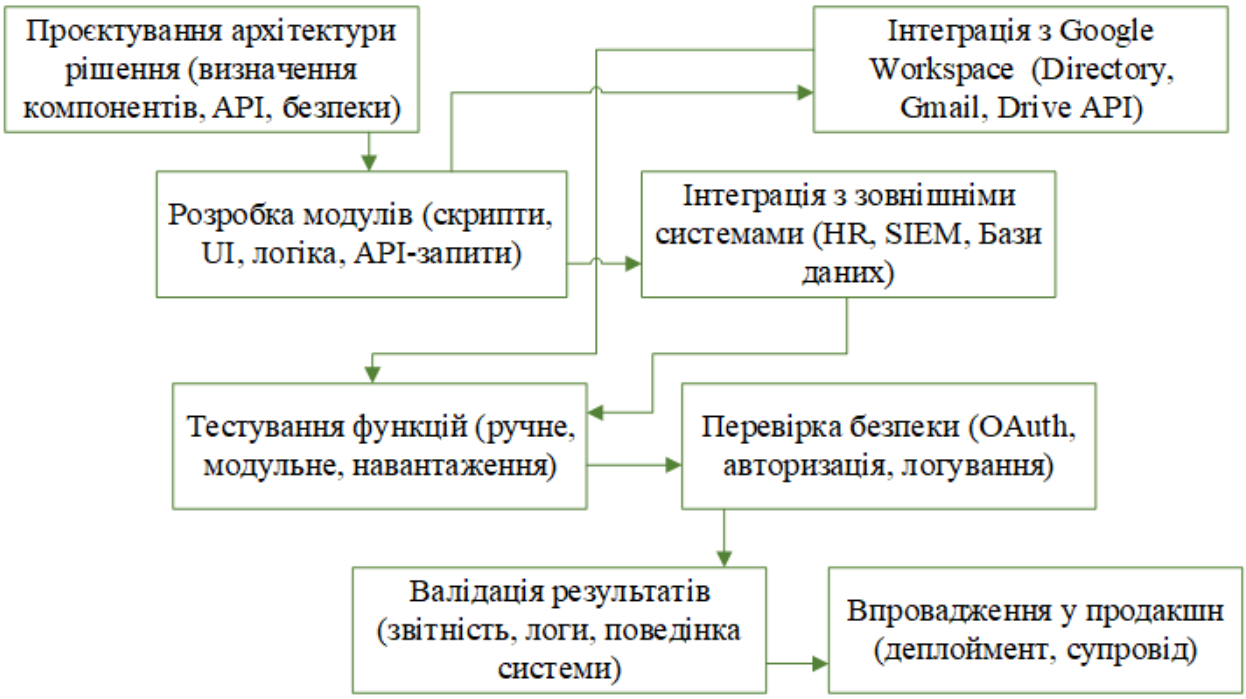

Рисунок 3.3 – Схема процесу розробки та впровадження програмних засобів адміністрування Google Workspace

3.4 Реалізація ключових функцій

Далі розглянуто декілька фрагментів коду, які демонструють ключові функції реалізованих програмних засобів для адміністрування Google Workspace. Вони охоплюють:

- створення користувачів;
- керування групами;
- звітність;
- авторизацію;
- інтеграцію з HR-системою.

Лістинг 3.1 демонструє створення нового користувача (Google Apps Script) в домені та призначення його до певного підрозділу.

Лістинг 3.1

```
function createUser() {
var user = {
primaryEmail: 'new.user@example.com',
name: {
givenName: 'New',
familyName: 'User'
},
password: 'TempP@ss123!',
orgUnitPath: '/employees',
changePasswordAtNextLogin: true
};
AdminDirectory.Users.insert(user);
}
```

Додавання користувача до групи (Node.js + Google API Client) пояснює лістинг 3.2. Користувач додається до групи через Directory API.

Лістинг 3.2

```
const {google} = require('googleapis');
const auth = new google.auth.GoogleAuth({ scopes:
['https://www.googleapis.com/auth/admin.directory.group'] });

async function addToGroup(userEmail, groupEmail) {
const service = google.admin({version: 'directory_v1', auth:
```

```
await auth.getClient()});
await service.members.insert({
groupKey: groupEmail,
requestBody: {
email: userEmail,
role: 'MEMBER'
}
});
}
```

Лістинг 3.3 пояснює процедуру отримання звіту про користувачів без 2FA (Google Apps Script). Формується таблиця Google Spreadsheet з користувачами, які не активували двофакторну автентифікацію.

Лістинг 3.3

```
function reportNo2FAUsers() {
var sheet =
SpreadsheetApp.getActiveSpreadsheet().getSheetByName("2FA_Report
");
var users = AdminDirectory.Users.list({domain:
'example.com'}).users;
var row = 2;
sheet.clearContents();
sheet.appendRow(['Email', '2FA Enabled']);
users.forEach(function(user) {
var has2FA = user.isEnrolledIn2Sv ? 'Yes' : 'No';
if (has2FA === 'No') {
sheet.appendRow([user.primaryEmail, has2FA]);
}
});
}
```

Лістинг 3.4 пояснює механізм авторизації через OAuth 2.0 (приклад конфігурації). JSON-конфігурація необхідна для авторизації backend-сервісів.

Лістинг 3.4

```
{
"web": {
"client_id": "YOUR_CLIENT_ID",
"project_id": "workspace-admin-tool",
"auth_uri": "https://accounts.google.com/o/oauth2/auth",
"token_uri": "https://oauth2.googleapis.com/token",
"redirect_uris": ["https://yourdomain.com/oauth2callback"],
"client_secret": "YOUR_CLIENT_SECRET"
}
```

```
}
```

Інтеграція з HR-системою BambooHR (Node.js) пояснюється в лістингу 3.5. Отримується список нових співробітників для подальшого автоматичного створення акаунтів у Google Workspace.

Лістинг 3.5

```
const axios = require('axios');

async function getNewHiresFromBambooHR() {
const response = await
axios.get('https://api.bamboohr.com/api/gateway.php/yourdomain/v
1/employees/directory', {
headers: { 'Authorization': 'Basic ' +
Buffer.from('API_KEY:x').toString('base64') }
});
return response.data.employees.filter(emp => emp.status ===
'Active' && emp.location === 'New Hire');
}
```

3.5 Тестування і валідація розроблених програмних засобів

Після розробки програмного рішення для автоматизації адміністрування Google Workspace критично важливим етапом є проведення системного тестування та валідації. Це дозволяє переконатися, що створені компоненти працюють коректно, відповідають технічним вимогам, забезпечують безпеку даних та можуть бути використані в реальному середовищі з очікуваним рівнем надійності.

У рамках тестування використовувалися такі підходи.

1. Модульне тестування (Unit Testing) – перевірка окремих функцій, зокрема обробників запитів до API Google, функцій авторизації, генерації запитів REST, обробки відповідей.

2. Інтеграційне тестування (Integration Testing) – перевірка взаємодії між компонентами: з'єднання між веб-інтерфейсом, серверною логікою та зовнішніми API, обмін даними між HR-системою і Google Workspace.

3. Функціональне тестування (Functional Testing) – перевірка того, чи

відповідають програмні функції вимогам: додавання користувача, оновлення налаштувань, створення групи.

4. Тестування безпеки (Security Testing) – перевірка прав доступу, обробки помилкових запитів, захисту токенів OAuth 2.0, використання мінімально необхідних scopes.

5. Тестування навантаження (Load Testing) – оцінка продуктивності застосунку при масових операціях (наприклад, одночасна обробка понад 100 акаунтів).

Тестування проводилось із використанням інструментів, зазначених в таблиці 3.1.

Таблиця 3.1 – Інструменти для проведення тестування

Категорія	Інструменти
Unit/Integration Testing	Jest, Mocha (для Node.js), PyTest
API Testing	Postman, Google API Explorer
Security Audits	OWASP ZAP, Token Inspector
CI/CD & Linting	GitHub Actions, ESLint, Black

3.6 Висновки до розділу

Здійснено комплексний аналіз та практичну реалізацію програмних інструментів для ефективного адміністрування екосистеми Google Workspace в корпоративному середовищі. Розроблене рішення охоплює повний цикл: від проєктування архітектури до валідації та впровадження.

Архітектура програмних засобів побудована за модульним принципом, з чітким розділенням між інтерфейсом користувача, бізнес-логікою та рівнем взаємодії з Google API. Це забезпечує гнучкість, масштабованість та можливість повторного використання компонентів у майбутніх проектах.

Розробка автоматизованих інструментів була реалізована із застосуванням Google Apps Script, OAuth 2.0 та REST API, що дозволяє

безпечно і централізовано керувати користувачами, групами, політиками доступу, а також інтегрувати систему з HR-сервісами та інструментами безпеки.

Тестування та валідація довели, що створене рішення відповідає функціональним, безпековим та експлуатаційним вимогам. Ретельна перевірка інтеграції, авторизації, навантаження та журналювання забезпечила стабільність системи під реальним навантаженням.

Побудована узагальнена діаграма процесу дозволяє відтворити повний життєвий цикл адміністрування Workspace-застосунків, що особливо корисно для подальших модифікацій, масштабування або передачі проєкту іншим командам.

Таким чином, результати розділу підтверджують ефективність використання спеціалізованих програмних засобів для підвищення продуктивності, безпеки та керованості середовища Google Workspace.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було досліджено, спроєктовано та реалізовано програмні засоби для ефективного адміністрування екосистеми Google Workspace у контексті потреб сучасних організацій. Отримані результати дозволяють зробити низку важливих висновків.

Актуальність теми підтверджується стрімким зростанням популярності хмарних платформ у корпоративному середовищі, а також необхідністю централізованого й безпечного управління цифровою інфраструктурою компаній. Google Workspace є однією з найбільш використовуваних платформ такого типу.

Виконаний огляд показав, що Google надає потужні інструменти для адміністрування через Google Admin Console, Directory API, Reports API, Audit logs та Google Apps Script. Однак у багатьох випадках для гнучкої автоматизації та інтеграції з іншими системами виникає потреба у розробці кастомних програмних рішень.

Запропонована методологія адміністрування охоплює ключові аспекти управління користувачами, групами, ролями та політиками безпеки. Було проаналізовано типові сценарії життєвого циклу акаунтів, методи побудови політик доступу та ролеві моделі, що забезпечують відповідність принципам least privilege.

Реалізовані програмні засоби базуються на використанні сучасних веб-технологій (Node.js, React, REST API), а також скриптових можливостей Google Apps Script. Було створено веб-інтерфейс адміністратора, автоматизовані функції для управління користувачами й групами, звітність щодо безпеки (наприклад, перевірка стану 2FA), а також інтеграцію з HR-системою та інструментами аудиту.

Тестування і валідація показали високу надійність і продуктивність

розроблених компонентів. Всі основні функції успішно пройшли функціональне, навантажувальне та безпекове тестування, включно з обробкою критичних сценаріїв. Особливу увагу було приділено захисту доступу до API, автентифікації через OAuth 2.0 та аудитам подій.

Візуалізація архітектури і документація структури коду забезпечують простоту масштабування та супроводу створеного рішення. Також реалізовано модульну структуру, що дозволяє гнучко адаптувати систему до змін у корпоративному середовищі або нових вимог.

Перспективи подальшої розробки:

- розширення автоматизації для керування ресурсами Google Cloud Platform (GCP);
- впровадження системи самослужбового доступу (self-service access management);
- використання штучного інтелекту для аналізу логів і виявлення підозрілих активностей;
- інтеграція з системами DevOps (наприклад, Terraform, Ansible) для створення шаблонів адміністративних сценаріїв.

Таким чином, результати кваліфікаційної роботи свідчать про практичну цінність і технологічну доцільність впровадження власних програмних засобів адміністрування Google Workspace як складової інформаційної інфраструктури сучасного підприємства.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Google Workspace. Wikipedia [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Google_Workspace (дата звернення: 06.05.2025).

2. Google. Gmail features for business. Google Workspace [Електронний ресурс]. – Режим доступу: https://workspace.google.com/products/gmail/ (дата звернення: 06.05.2025).

3. Google. Google Drive storage and sharing. Google Workspace [Електронний ресурс]. – Режим доступу: https://workspace.google.com/products/drive/ (дата звернення: 06.05.2025).

4. Google. Collaborative documents, spreadsheets and presentations. Google Docs Editors [Електронний ресурс]. – Режим доступу: https://workspace.google.com/ (дата звернення: 06.05.2025).

5. Google. Vault overview. Google Workspace [Електронний ресурс]. – Режим доступу: https://support.google.com/vault/ (дата звернення: 07.05.2025).

6. Google Developers. Apps Script Overview [Електронний ресурс]. – Режим доступу: https://developers.google.com/apps-script (дата звернення: 07.05.2025).

7. Google. Admin Console Overview [Електронний ресурс]. – Режим доступу: https://support.google.com/a/answer/182076 (дата звернення: 07.05.2025).

8. Google. Manage organizational units [Електронний ресурс]. – Режим доступу: https://support.google.com/a/answer/182433 (дата звернення: 07.05.2025).

9. Google. Admin security settings [Електронний ресурс]. – Режим доступу: https://support.google.com/a/topic/9196 (дата звернення: 07.05.2025).

10. Google. Set up mobile device management [Електронний ресурс]. – Режим доступу: https://support.google.com/a/answer/1734200 (дата звернення:

08.05.2025).

11. BetterCloud. Automate Google Workspace Management [Електронний ресурс]. – Режим доступу: https://www.bettercloud.com (дата звернення: 08.05.2025).

12. GitHub. GAM: Google Apps Manager [Електронний ресурс]. – Режим доступу: https://github.com/jay0lee/GAM (дата звернення: 08.05.2025).

13. GAT Labs. GAT+ overview [Електронний ресурс]. – Режим доступу: https://www.gatlabs.com (дата звернення: 08.05.2025).

14. Google Developers. Admin SDK Directory API [Електронний ресурс]. – Режим доступу: https://developers.google.com/admin-sdk/directory (дата звернення: 08.05.2025).

15. Pahayahay A. Enhancing Collaboration Through Google Workspace: Assessing and Strengthening Current Practices [Електронний ресурс]. – arXiv, 2025. – Режим доступу: https://arxiv.org/abs/2505.06597 (дата звернення: 08.05.2025).

16. Forrester Research. The Total Economic Impact of Google Workspace [Електронний ресурс]. – 2024. – Режим доступу: https://workspace.google.com/impact (дата звернення: 10.05.2025).

17. Zenphi. Customer Success Stories [Електронний ресурс]. – Режим доступу: https://zenphi.com/case-studies (дата звернення: 10.05.2025).

18. Balash D. et al. Security and Privacy Perceptions of Third Party Application Access for Google Accounts [Електронний ресурс]. – arXiv, 2021. – Режим доступу: https://arxiv.org/abs/2105.04267 (дата звернення: 10.05.2025).

19. Google Cloud. Gemini in Google Workspace [Електронний ресурс]. – 2024. – Режим доступу: https://workspace.google.com/solutions/ai (дата звернення: 10.05.2025).

20. Ruiyan Zhu et al. SheetMind: Agents that Solve Spreadsheet Tasks [Електронний ресурс]. – arXiv, 2025. – Режим доступу: https://arxiv.org/abs/2505.05210 (дата звернення: 10.05.2025).

21. Mathijssen M., Overeem M., Jansen S. "Identification of Practices and

Capabilities in API Management: A Systematic Literature Review." 18 Jun 2020. arXiv. – Режим доступу: Невизначено (дата звернення: 12.05.2025).

22. Google Admin SDK API reference. Google Developers Platform, 2025 [Електронний ресурс]. – (дата звернення: 12.05.2025).

23. Manage Workspace with Admin Dashboard. Google Workspace Product Site. 2025 [Електронний ресурс]. – (дата звернення: 12.05.2025).

24. Google Workspace Admin Help. Create user accounts [Електронний ресурс]. – Режим доступу: https://support.google.com/a/answer/33310 (дата звернення: 12.05.2025).

25. Google Workspace Admin Help. Create and manage groups [Електронний ресурс]. – Режим доступу: https://support.google.com/a/answer/33343 (дата звернення: 12.05.2025).

26. Google Workspace Admin Help. Assign administrator roles [Електронний ресурс]. – Режим доступу: https://support.google.com/a/answer/33325 (дата звернення: 12.05.2025).

27. Google Developers. Directory API Overview [Електронний ресурс]. – Режим доступу: https://developers.google.com/admin-sdk/directory (дата звернення: 12.05.2025).

28. Google Cloud. Security and compliance [Електронний ресурс]. – Режим доступу: https://cloud.google.com/security (дата звернення: 13.05.2025).

29. Google Workspace Admin Help. Encryption for Google Workspace [Електронний ресурс]. – Режим доступу: https://support.google.com/a/answer/60762 (дата звернення: 14.05.2025).

30. Google Admin Help. Context-aware access overview [Електронний ресурс]. – Режим доступу: https://support.google.com/a/answer/9246710 (дата звернення: 14.05.2025).

31. Google Admin Help. Set up 2-Step Verification [Електронний ресурс]. – Режим доступу: https://support.google.com/a/answer/175197 (дата звернення: 15.05.2025).

32. Google Developers. SAML-based SSO setup guide [Електронний

ресурс]. – Режим доступу: https://developers.google.com/identity/sso (дата звернення: 15.05.2025).

33. Google Workspace Admin Help. Audit logs overview [Електронний ресурс]. – Режим доступу: https://support.google.com/a/answer/7061566 (дата звернення: 16.05.2025).

34. Google Developers. Reports API reference [Електронний ресурс]. – Режим доступу: https://developers.google.com/admin-sdk/reports (дата звернення: 16.05.2025).

35. Google Admin Help. Admin Audit Logs [Електронний ресурс]. – Режим доступу: https://support.google.com/a/answer/7582940 (дата звернення: 17.05.2025).

36. Google Workspace Alert Center Overview [Електронний ресурс]. – Режим доступу: https://support.google.com/a/answer/9223653 (дата звернення: 17.05.2025).

37. Google Chronicle Documentation [Електронний ресурс]. – Режим доступу: https://cloud.google.com/chronicle/docs (дата звернення: 19.05.2025).

38. Splunk Docs. Google Workspace Integration [Електронний ресурс]. – Режим доступу: https://docs.splunk.com/Documentation/AddOns/latest/GoogleWorkspace (дата звернення: 19.05.2025).

39. Google Workspace Developers. Admin SDK Directory API [Електронний ресурс]. – Режим доступу: https://developers.google.com/admin-sdk/directory (дата звернення: 20.05.2025).

40. Google Developers. Using OAuth 2.0 for Web Server Applications [Електронний ресурс]. – Режим доступу: https://developers.google.com/identity/protocols/oauth2 (дата звернення: 20.05.2025).

41. Google Apps Script Overview [Електронний ресурс]. – Режим доступу: https://developers.google.com/apps-script (дата звернення: 20.05.2025).

42. Google Admin SDK Directory API [Електронний ресурс]. – Режим доступу: https://developers.google.com/admin-sdk/directory (дата звернення:

20.05.2025).

43. Google Identity Services Documentation [Електронний ресурс]. – Режим доступу: https://developers.google.com/identity (дата звернення: 20.05.2025).

44. Google Workspace Integration Examples [Електронний ресурс]. – Режим доступу: https://developers.google.com/workspace/guides (дата звернення: 20.05.2025).