

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології підвищення рівня захищеності інформаційних
ресурсів підприємства в умовах використання хмарних технологій»

Виконав студент 2-го курсу групи Кбм-22-1
спеціальності 125 «Кібербезпека»

 Медведенко А.В.

Керівник доцент кафедри комп'ютерної інженерії
та кібербезпеки, кандидат технічних наук

 Шелуха О.О.

Рецензент професор кафедри комп'ютерної інженерії та
кібербезпеки, доктор технічних наук, доцент

 Воротніков В.В.

Житомир – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри

комп'ютерної інженерії

та кібербезпеки

 Єфіменко А.А.

«13» жовтня 2023 р.

ЗАВДАННЯ

на випускн кваліфікаційну роботу

Студента Медведенка Андрія Віталійовича

Тема роботи: Методи та технології підвищення рівня захищеності інформаційних ресурсів підприємства в умовах використання хмарних технологій

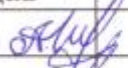
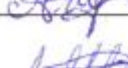
Затверджена Наказом університету від 13 жовтня 2023 р. № 572/с

Термін здачі студентом закінченої роботи 25 грудня 2023 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Розроблені технічні вимоги до проєкту
2. Розроблена функціональна модель проєкту
3. Налагоджено хмарну систему
4. Налагоджено системи безпеки
5. Виконано перехід з однієї системи на іншу

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	О.О. Шелуха	02.09.2023 	02.09.2023 
2	О.О. Шелуха	06.10.2023 	06.10.2023 
3	О.О. Шелуха	04.11.2023 	04.11.2023 

Студент  А.В. Медведенко

Керівник  О.О. Шелуха

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	01.11.2023 – 03.11.2023	Виконано
2	Розробка вимог до проєкту	04.11.2023 – 06.11.2023	Виконано
3	Аналіз хмарних сервісів	10.11.2023 – 13.11.2023	Виконано
4	Вибір хмарного сервісу для організації	15.11.2023 – 17.11.2023	Виконано
5	Дослідження функціонала обраного хмарного сервісу	18.11.2023 – 23.11.2023	Виконано
6	Налагодження хмарного сервісу та систем безпеки	24.11.2023 – 1.12.2023	Виконано
7	Аналіз результатів	3.12.2023 – 4.12.2023	Виконано
8	Написання пояснювальної записки	5.12.2023 – 9.12.2023	Виконано
9	Підготовка презентації	10.12.2023 – 12.12.2023	Виконано
10	Захист	25.12.2023	Виконано

Студент  А.В. Медведенко

Керівник  О.О. Шелуха

АНОТАЦІЯ

Кваліфікаційна робота складається з проєкту підсистеми захисту інформаційних ресурсів підприємства при використанні хмарних технологій та пояснювальної записки до нього. Пояснювальна записка містить 73 сторінки, 35 ілюстрацій та 5 таблиць.

Метою роботи є дослідження методів та технології підвищення рівня захищеності інформаційних ресурсів підприємства в умовах використання хмарних технологій.

Досліджено методи та моделі взаємодії з інформаційними системами підприємства на базі хмарних сервісів. Визначено переваги впровадження хмарних технологій у інфраструктуру підприємства.

Проведено аналіз наступних хмарних сервісів: ClickUp, Wrike, Asana, Google Workspace. Визначено моделі послуг які надаються користувачам та рівень захищеності інформаційних ресурсів який зазначені хмарні сервіси можуть забезпечити.

Розроблено моделі загроз та порушника, визначено методи підвищення захищеності інформаційних ресурсів підприємства. Представлено сценарій розгортання хмарного сервісу та модель налаштування системи безпеки з підвищеним рівнем захищеності.

Проведено аналіз існуючої інфраструктури та визначено недоліки, які дозволяє вирішити застосування системи підвищеної захищеності на базі хмарного сервісу Google Workspace.

Продемонстровано процес розгортання хмарного сервісу Google Workspace, перенесення даних із існуючої системи, та впроваджено налаштування необхідних системи безпеки користувачів.

КЛЮЧОВІ СЛОВА: ХМАРНИЙ СЕРВІС, ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ, GOOGLE WORKSPACE, РІВНІ БЕЗПЕКИ

					КІК.КР.Б – 125 – 15 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Методи та технології підвищення рівня захищеності інформаційних ресурсів підприємства в умовах використання хмарних технологій	Лім.	Арк.	Аркушів
Розроб.		Медведенко А.В.		21.12.23				
Керівник		Шелуха О.О.		21.12.23			4	4
Реценз.		Воротніков В.В.		21.12.23		ФІКТ, Гр. КБм-22-1		
Н. контр.		Воротніков В.В.		21.12.23				
Затверд.		Сфіменко А.А.		21.12.23				

ANNOTATION

The qualification work consists of the information resources protection system project base on cloud technologies and its explanatory note. The explanatory note contains 73 pages, 35 illustrations and 5 tables.

The purpose of the work is to research methods and technologies for increasing the security level of the company's information resources under the conditions of using cloud technologies.

The methods and models of interaction with the information systems of the enterprise based on cloud services were studied. The advantages of introducing cloud technologies into the infrastructure of the enterprise have been determined.

The following cloud services were analyzed: ClickUp, Wrike, Asana, Google Workspace. The models of services provided to users and the level of security of information resources that these cloud services can provide are defined.

Models of threats and violators have been developed, methods of increasing the security of the company's information resources have been determined. The deployment scenario of the cloud service and the configuration model of the security system with an increased level of security are presented.

An analysis of the existing infrastructure was carried out and shortcomings were identified, which can be solved by the application of a system of increased security based on the Google Workspace cloud service.

The process of deploying the Google Workspace cloud service, transferring data from the existing system, and setting up the necessary user security system were demonstrated.

KEY WORDS: CLOUD SERVICE, PROTECTION OF INFORMATION RESOURCES, GOOGLE WORKSPACE, SECURITY LEVELS

		Медведевко А.В.			KIK.KP.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	8
ВСТУП	9
РОЗДІЛ 1. АНАЛІЗ ЗАСТОСУВАННЯ ХМАРНИХ СЕРВІСІВ У ІНФОРМАЦІЙНІЙ ІНФРАСТРУКТУРІ ПІДПРИЄМСТВА	11
1.1 Аналіз актуальності застосування хмарних технологій	11
1.2 Аналіз методів впровадження хмарних технологій в інформаційну інфраструктуру підприємства.....	15
1.3 Аналіз моделей обслуговування із використанням хмарних сервісах.....	18
Висновок до розділу 1	22
РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ	23
2.1 Дослідження можливостей хмарних сервісів	23
2.1.1 Універсальна хмарна платформа ClickUP	23
2.1.2 Платформа управління проєктами Wrike	25
2.1.3 Сервіс керування завданнями Asana	27
2.1.4 Пакет хмарних інструментів Google Workspace	29
2.2 Дослідження можливостей пакету Google Workspace Enterprise	31
2.3 Дослідження рівнів безпеки даних у хмарному сервісі Google Workspace...	35
2.3.1 Безпека на рівні центра обробки даних.....	36
2.3.2 Безпека на рівні користувача	40
2.4 Моделі загроз та порушника.....	46
Висновки до розділу 2	50

РОЗДІЛ 3 РОЗГОРТАННЯ ТА НАЛАШТУВАННЯ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ НА БАЗІ ХМАРНОГО СЕРВІСУ GOOGLE WORKSPACE ...	51
3.1 Дослідження системи захисту існуючої інформаційної інфраструктури.....	51
3.2 Розгортання хмарного сервісу Google Workspace	53
3.3 Впровадження системи безпеки підвищеної захищеності	55
3.4 Перенесення існуючої інфраструктури в Google Workspace	63
Висновки до розділу 3	67
ВИСНОВКИ.....	68
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	70
ДОДАТКИ.....	74

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

NIST – National Institute of Standards and Technology

ЦОД – Центр Обробки даних

CRM – Customer Relationship Management

ERP – Enterprise Resource Planning

VPN – Virtual Private Network

IaaS – Infrastructure as a Service

PaaS – Platform as a Service

SaaS – Software as a Service

MFA – Multi-factor authentication

TLS – Transport Layer Security

IRM – Information Rights Management

DLP – Data Loss Prevention

RBAC – Role Based Access Control

DDoS – Distributed Denial of Service

		Медведевко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Зростання популярності та поширення глобальної мережі Інтернет призвело до того, що обсяги інформації, що циркулює та оброблюється людьми, постійно збільшуються.

Хмарні технології – це основа сучасної інформаційно-телекомунікаційної інфраструктури. Вони дозволяють створювати потужні інформаційні системи з новою архітектурою та можливостями.

Традиційні локальні інформаційні системи потребують значних витрат на експлуатацію та технічне обслуговування. Хмарні технології дозволяють зменшити ці витрати та пришвидшити процес розробки та випуску програмних продуктів. Вони також сприяють підвищенню ефективності праці підприємств шляхом організації прозорого документообігу та спільної праці над проектами.

Хмарні технології є однією з найперспективніших тенденцій у сфері інформаційних технологій. Вони пропонують підприємствам ряд переваг, які можуть суттєво підвищити ефективність їхньої діяльності. Однією з ключових переваг хмарних технологій є можливість масштабування інфраструктури для зберігання даних та динамічного керування потужностями. Це дозволяє підприємствам адаптувати свою інформаційну систему до змінних потреб бізнесу без необхідності вкладати кошти в нове обладнання та програмне забезпечення. Крім того, хмарні технології дозволяють підприємствам скоротити витрати на обслуговування інформаційної системи. Підприємства можуть відмовитися від власного обладнання та програмного забезпечення, що дозволить їм заощадити на витратах на закупівлю, експлуатацію та обслуговування. Нарешті, хмарні технології дозволяють підприємствам швидко розгортати нові філіали. Це дає підприємствам можливість розширювати свою діяльність у нові регіони без необхідності вкладати кошти в закупівлю та встановлення обладнання, саме тому обрана тема є актуальною.

Хмарні технології мають ряд переваг, але процес формування нормативно-правової бази для регулювання взаємодії постачальників хмарних послуг та користувачів досі не завершений.

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

Мета кваліфікаційної роботи. Мета роботи полягає в підвищенні захищеності інформаційних ресурсів підприємства з використанням хмарних технологій.

Для досягнення поставленої мети було сформульовано наступні завдання:

1. Провести аналіз моделей обслуговування на основі хмарних технологій, визначити їх переваги та недоліки.

2. Розробити моделі загроз та порушника в інформаційній інфраструктурі на основі хмарних сервісів.

3. Розробити методи підвищення захищеності інформаційних ресурсів та дослідити можливості щодо їх впровадження у систему безпеки хмарних сервісів.

Об'єктом дослідження є процес розробки, розгортання та захисту інформаційної інфраструктури підприємства з використанням хмарних технологій.

Предметом дослідження є методи та технології підвищення захищеності інформаційних ресурсів підприємства в умовах використання хмарних технологій.

Практичне значення роботи полягає у впровадженні системи підвищеного захисту інформаційних ресурсів підприємства.

		Медведевко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. АНАЛІЗ ЗАСТОСУВАННЯ ХМАРНИХ СЕРВІСІВ У ІНФОРМАЦІЙНІЙ ІНФРАСТРУКТУРІ ПІДПРИЄМСТВА

1.1 Аналіз актуальності застосування хмарних технологій

Обчислювальні хмари - це розподілені системи, які об'єднують тисячі серверів, розташованих у дата-центрах по всьому світу. Вони забезпечують доступ до обчислювальних ресурсів, таких як процесорна потужність, пам'ять, дисковий простір та мережевий трафік, для користувачів і організацій.

Хмарні технології мають ряд переваг перед традиційними моделями обчислювання. Вони дозволяють підприємствам і організаціям масштабувати свої обчислювальні ресурси в залежності від потреб, що може призвести до зниження витрат. Крім того, хмарні технології дозволяють уникнути витрат на придбання та обслуговування власного обладнання.

Хмарні обчислення - це модель надання користувачам доступу до обчислювальних ресурсів, таких як сервери, сховища та бази даних, через Інтернет. Ці ресурси можуть бути налаштовані та надані на вимогу, що дозволяє користувачам масштабувати їх відповідно до своїх потреб. Вони мають ряд переваг перед традиційним способом розміщення обчислювальних ресурсів на власному обладнанні. До них належать:

- Економія витрат: дозволяє користувачам уникати витрат на придбання та обслуговування власного обладнання.
- Зручність: дозволяє користувачам легко масштабувати свої ресурси відповідно до потреб.
- Гнучкість: дозволяє користувачам швидко та легко запускати нові проекти.

Хмарні сервіси надають користувачу свої обчислювальні ресурси у чистому вигляді і користувач може не знати, які комп'ютери обробляють його запити, під керуванням якої операційної системи це відбувається і т.д.

Хмарні обчислення визначаються Національним інститутом стандартів і технологій США (NIST) як «модель для зручного, на вимогу, мережевого доступу

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

до загального сховища даних з налаштованим обчислювальними ресурсами (наприклад, до мереж, серверів, систем зберігання, додатків і послуг), який може бути здійснений швидко, при мінімальній необхідності в управлінні і взаємодії з постачальником послуг » [1].

Часто хмари порівнюють з мейнфреймами, які мають ряд спільних рис. Обидві системи дозволяють користувачам отримувати доступ до обчислювальних ресурсів, які не знаходяться на їхньому власному комп'ютері. Це може бути корисно для підприємств і організацій, які потребують великих обсягів обчислювальних потужностей або зберігання даних. Однак між хмарами та мейнфреймами також є ряд важливих відмінностей. Однією з ключових відмінностей є масштабованість. Хмари теоретично не обмежені за масштабом, що означає, що вони можуть підтримувати необмежену кількість користувачів і завдань. Мейнфрейми, з іншого боку, зазвичай мають обмежену пропускну здатність і продуктивність [2]. Іншою важливою відмінністю є тип доступу до користувачів. Хмари використовують модель "pay-as-you-go", що означає, що користувачі платять лише за ті ресурси, які вони використовують. Мейнфрейми, як правило, використовують модель ліцензування, що означає, що користувачі повинні придбати ліцензію на використання системи.

Серед більш ранніх технологій обробки даних, з'явилися так звані grid-обчислення. Цей напрямок спочатку сприймався як можливість використовувати безкоштовні процесорні ресурси та розвивати систему добровільної оренди обчислювальних потужностей. Низка проєктів довели, що ця модель розрахунку досить ефективна. Ця технологія використовується для вирішення наукових і математичних завдань, які потребують значних обчислювальних ресурсів. Відомо, що grid-обчислення використовують і в комерційних цілях. Наприклад, вони використовуються для виконання трудомістких завдань, пов'язаних з економічним прогнозуванням, аналізом сейсмічних даних, розробкою і дослідженням властивостей вакцин і нових препаратів. Дійсно, grid-обчислення та хмарні обчислення мають багато спільного з точки зору архітектури та принципів. Проте модель хмарних обчислень на сьогоднішній день вважається більш перспективною

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

завдяки своїй набагато більш гнучкій платформі для роботи з віддаленими обчислювальними ресурсами [3].

Великі обчислювальні хмари - це розподілені системи, що складаються з тисяч серверів, розміщених у центрах обробки даних (ЦОД). Ці сервери забезпечують ресурсами десятки тисяч застосунків, які одночасно використовують мільйони користувачів. Це зручний інструмент для невеликих компаній, у яких не вистачає бюджету утримувати власні CRM, ERP, тощо.

Хмарні технології стають все більш популярними, і на це є ряд причин. По-перше, вони дозволяють підприємствам економити на витратах на інфраструктуру, обслуговування та персонал. По-друге, хмарні технології забезпечують доступ до даних і додатків з будь-якого місця, де є доступ до Інтернету. По-третє, хмарні технології дозволяють підприємствам швидко і легко масштабувати свої ресурси відповідно до потреб. Майже всі проблеми повністю перекладаються на провайдера і з'являється змога стандартизувати програмне забезпечення навіть на різних операційних системах.

Одним з головних недоліків є залежність від постачальника послуг. Підприємство, яке використовує хмарні обчислення, стає заручником провайдера, оскільки саме він відповідає за збереження даних і доступ до них. Щоб забезпечити надійність даних, підприємство має докласти чимало зусиль. Наприклад, воно може використовувати кілька дублюючих каналів зв'язку, що дозволить продовжити роботу в разі виходу з ладу одного з них. Крім того, необхідно продумати питання безпеки даних, щоб захистити їх від несанкціонованого доступу. Хмарні обчислення також не підходять для підприємств, які мають справу з державною та військовою таємницею. Такі дані не можуть зберігатися на сторонніх серверах, оскільки це може призвести до їх розголошення.

Національним інститутом стандартів і технологій США було виділено п'ять основних принципів побудови хмарної моделі: самообслуговування за вимогою, універсальність доступу, об'єднання ресурсів, еластичність масштабування, облік споживання [4].

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

Хмарні обчислення дозволяють споживачам отримувати доступ до обчислювальних ресурсів, коли вони потрібні. Ця модель надання послуг ґрунтується на принципах самообслуговування та автоматизації, що дозволяє споживачам самостійно керувати своїми ресурсами. Запит споживача на ресурси автоматично обробляється хмарною інфраструктурою, без необхідності звертатися до постачальника послуг. Це забезпечує швидке та ефективне надання послуг.

Для реалізації самообслуговування постачальник хмарних послуг повинен мати інфраструктуру, яка може обробляти велику кількість запитів у режимі реального часу. Ця інфраструктура зазвичай є віртуальною, що дозволяє використовувати одне й те ж апаратне забезпечення для обслуговування кількох споживачів.

Хмарні обчислення відокремлюють обчислювальні ресурси від споживачів, тому їм не потрібно самостійно їх підтримувати та обслуговувати. Наслідком цього є необхідність доступу за допомогою мережі інтернет до територіально розподілених центрів обробки інформації.

Хмарні обчислення дозволяють об'єднувати обчислювальні ресурси, такі як сервери, пам'ять та обчислювальна потужність, в єдину віртуальну інфраструктуру. Це дозволяє підвищити коефіцієнт використання ресурсів, оскільки ресурси можуть використовуватися декількома користувачами одночасно.

Динамічний перерозподіл обчислювальних потужностей дозволяє ще більше підвищити коефіцієнт використання ресурсів, оскільки ресурси можуть перерозподілятися між користувачами в залежності від їхніх потреб. Це дозволяє заощадити кошти, оскільки хмарні провайдери не повинні купувати та обслуговувати зайві ресурси.

Об'єднання ресурсів на програмному рівні накладає певні обмеження на розробників програмного забезпечення. Розробники повинні передбачити можливість одночасного використання програмного продукту декількома користувачами. Це може призвести до необхідності використання додаткових механізмів безпеки та керування доступом.

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

Хмарні обчислення дають споживачам можливість отримувати обчислювальні ресурси у будь-який час і в будь-якій кількості. Щоб забезпечити безперебійну роботу додатків і систем, хмарна інфраструктура повинна мати можливість швидко масштабуватися вгору або вниз, залежно від потреб.

Масштабування вгору означає додавання нових ресурсів, коли це необхідно, наприклад, під час пікових навантажень. Масштабування вниз означає видалення ресурсів, коли вони не потрібні, наприклад, у міжпікові періоди.

Різні програми і системи мають різні моделі робочого навантаження. Наприклад, веб-сайти можуть мати пікові навантаження в певні години доби, а бази даних можуть мати пікові навантаження в певні дні тижня. Завдяки масштабуванню хмарна інфраструктура може ефективно розподіляти ресурси між різними додатками і системами, що призводить до підвищення коефіцієнта використання ресурсів і зниження витрат.

У загальному випадку, масштабування означає здатність системи збільшувати свою продуктивність пропорційно до збільшення апаратного забезпечення. У хмарі це означає, що можна просто додати нові сервери або інші ресурси, коли це необхідно.

Для оперативного масштабування вгору чи вниз, потрібно постійно аналізувати поточний попит на обчислювальні ресурси хмари, тобто навантаження на центральний процесор, оперативну пам'ять та пропускну здатність мережі, щоб переконатися, що споживачі не відчують вичерпності цих ресурсів.

1.2 Аналіз методів впровадження хмарних технологій в інформаційну інфраструктуру підприємства

На даний час існують три моделі розгортання хмарних технологій: приватні, загальнодоступні та гібридні.

Приватна хмара - фізично ізольована віртуальна інфраструктура з ексклюзивним доступом одного замовника. Її можна підключити до вже існуючої інфраструктури або інтегрувати з публічною хмарию. За своїм функціоналом вона

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

схожа на власний дата-центр. Проте на відміну від ЦОД, який потрібно будувати та обслуговувати, приватну хмару можна взяти в оренду у хмарного оператора.

Вона призначена для великих компаній з безліччю ІТ-сервісів для яких важлива висока інформаційна безпека та здатність витримувати пікові навантаження на ІТ-інфраструктуру. Однією з найбільших переваг є можливість гнучко нарощувати обчислювальні потужності та підвищення рівня безперервності функціонування ІТ-сервісів [5].

Враховуючи те, що підприємство самостійно несе відповідальність за встановлення та обслуговування хмари, вартість і складність впровадження такої хмари може значно перевищувати вартість обслуговування хмар, реалізованих за іншими моделями.

Використовуючи приватну хмару, гарантується високий рівень безпеки, завдяки відсутності прямого доступу до Інтернету та інфраструктурі лише однієї організації. Це чудовий варіант для компаній з високими вимогами до конфіденційності даних, розміщених у хмарі, наприклад для різних фінансових і державних компаній.

У приватній хмарі, як і в публічній чи гібридній, використовується технологія віртуалізації. З її допомогою можна об'єднати обчислювальні ресурси у загальні пули та автоматизовано ініціалізувати їх залежно від потреб компанії. Це дозволяє масштабувати ресурси та використовувати їх найбільш ефективно. У приватному хмарному середовищі ці обчислювальні ресурси належать лише одній компанії. Кожен її працівник отримує доступ до хмари через внутрішню мережу компанії або віртуальну приватну мережу (VPN).

Публічна хмара - це сукупність віртуальних обчислювальних ресурсів, які користувач отримує через інтернет у вигляді віртуальної інфраструктури. За цією моделлю надання послуг стоять високопродуктивні сервери, системи зберігання та канали передачі на стороні хмарних провайдерів. Вони за допомогою спеціального програмного забезпечення (системи віртуалізації) ділять фізичні ресурси на фрагменти. Таким чином, будь-який клієнт провайдера може отримати саме такий набір ресурсів, який необхідний йому для роботи [6].

		Медведченко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

У публічній хмарі фізичні ресурси інфраструктури провайдера діляться між замовниками у програмний спосіб, а виділяються динамічно - у будь-який момент можна запросити у постачальника послуги додаткову процесорну потужність, пам'ять або місце у сховищі. При тому клієнт може побудувати хмару на будь-якій кількості віртуальних машин з обраними конфігураціями ресурсів. Кожна віртуальна машина - це аналог фізичного сервера, на якому можна встановлювати та запускати будь-які ОС та програми на вибір клієнта.

Користувачі публічної хмари не мають можливості керувати чи підтримувати хмару, і вся відповідальність лежить на власнику хмари. Постачальник хмарних послуг бере на себе відповідальність за встановлення, керування, доставку та підтримку програмного забезпечення, інфраструктури додатків або фізичної інфраструктури. Споживачі платять лише за ті ресурси, які вони використовують.

Публічні хмари прості у використанні і не потребують великих витрат, їх легко масштабувати та нею можна керувати віддалено.

Гібридна хмара - це модель хмарної інфраструктури, яка може використовуватися як самостійне рішення, яке забезпечує гнучкість, так і як перехідний етап на шляху до повного експорту в публічну хмару.

Гібридна хмара отримує від публічної гнучкість, а від приватної – найкращий контроль ресурсів та високу безпеку. Таким чином, та частина ІТ-інфраструктури, на яку покладаються найвідповідальніші завдання, розміщується у дата-центрі. Дата-центр, своєю чергою, перебуває під контролем компанії [7].

Менш критичні програми можуть бути розгорнуті на потужностях публічних операторів. Однією з головних особливостей гібридного підходу є те, що вся хмарна інфраструктура працює як цілісна система під загальним централізованим керуванням.

Залежно від виду хмари сервісу, їм можуть володіти і розпоряджатися як провайдер, так і користувач, або і той і інший. Також можуть відрізнятися права доступу до ресурсів (табл. 1.1)

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Управління хмарними ресурсами

Хмара	Доступ	Власник	Розташування	Обслуговування
Приватна	У авторизованого користувача	Користувач або провайдер	У користувача або провайдера	Користувач або провайдер
Публічна	У всіх користувачів	Провайдер	У провайдера	Провайдер
Гібридна	У авторизованих та зовнішніх користувачів	Користувач і провайдер	У користувача і провайдера	Користувач і провайдер

1.3 Аналіз моделей обслуговування із використанням хмарних сервісів

На цей день існує три моделі обслуговування: інфраструктура як послуга (Infrastructure as a Service, скор. IaaS), платформа як послуга (Platform as a service, скор. PaaS) та програмне забезпечення як послуга (software as a service, скор. SaaS).

Інфраструктура як послуга - це модель обслуговування, в межах якої споживачу надається можливість керувати засобами обробки та збереження, комунікаційними мережами, та іншими фундаментальними обчислювальними ресурсами, на базі яких споживач може розгортати та виконувати довільне програмне забезпечення, до складу якого можуть входити операційні системи та прикладні програми. Споживач не керує фізичною та віртуальною інфраструктурою, що лежить в основі хмари, проте він контролює операційні системи, системи збереження, встановлені програми та, можливо, має обмежений контроль над деякими мережевими компонентами (наприклад, мережевими екранами вузлів). За концепцією IaaS споживач купує лише ті обчислювальні потужності, які необхідні йому для виконання конкретних завдань [8].

IaaS працює за принципом віртуалізації. Платформа IaaS дозволяє вибрати тип та конфігурацію необхідної інфраструктури. Потім система автоматично створює цифрову версію базової інфраструктури. Ці віртуалізовані обчислювальні

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

ресурси імітують поведінку фізичних ресурсів. Для вас і ваших програм все працює так само, як і на фізичному пристрої.

Постачальники сервісів IaaS також пропонують додаткові послуги для підтримки управління інфраструктурою. Наприклад, ви можете використовувати сервіси для виконання таких завдань: перегляд системних журналів та моніторинг продуктивності, впровадьте узгоджені заходи безпеки у всій інфраструктурі, налаштування політик, які автоматизують спільні інфраструктурні завдання, такі як резервне копіювання та балансування навантаження.

При використанні хмарних платформ споживач має певний контроль над своїми ресурсами. Наприклад, він може вибирати операційну систему, систему зберігання та застосунки, які будуть запущені в хмарі. Однак, споживач не керує базовою інфраструктурою хмари, яка належить провайдеру хмари. Споживач відповідає за захист своїх застосунків, а провайдер хмари відповідає за захист інфраструктури хмари.

Перевагою є зниження вкладень коштів в апаратне забезпечення. Оскільки в цій моделі зазвичай використовуються методи віртуалізації, економія може бути досягнута за рахунок більш ефективного використання ресурсів. Зниження ризику втрати інвестицій і порогу реалізації, можливість плавного автоматичного масштабування. Недоліками є те, що ефективність і продуктивність бізнесу значною мірою залежать від можливостей постачальника.

Платформа як послуга - це повноцінна середовище розробки та розгортання у хмарі з ресурсами, які дозволяють надавати будь-які хмарні програми – від найпростіших до передових рішень промислового класу. Ви отримуєте у постачальника хмарних служб необхідні ресурси з оплатою в міру використання та підключаєтеся до них за безпечним інтернет-підключенням [9].

Як і у випадку з IaaS, PaaS включає інфраструктуру (сервери, сховище та мережеве обладнання), а також програмне забезпечення проміжної кулі, засоби розробки, бізнес-аналітику, служби системи управління базами даних та інше. PaaS призначена для підтримки повного життєвого циклу веб-програми: розробки, тестування, розгортання, управління та оновлення.

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

РaaS також дозволяє уникнути витрат і труднощів, пов'язаних із придбанням ліцензій на програмне забезпечення, базової інфраструктури додатків, програмного забезпечення проміжного рівня, оркестраторів контейнерів, або засобів розробки та інших ресурсів, а також управління ними. Ви керуєте програмами та службами, які розробляєте, а постачальник хмарних служб зазвичай керує всім іншим.

Засоби розробки РaaS можуть скоротити час, необхідний для програмування нових програм завдяки заздалегідь підготовленим компонентам, вбудованим у платформу (робочим процесам, службам каталогів, компонентам безпеки, засобам пошуку тощо). А деякі постачальники служб надають варіанти розробки для кількох платформ, наприклад комп'ютерів, мобільних пристроїв та браузерів, спрощуючи та прискорюючи таким чином крос-платформну розробку програм.

Перевагою є плавне розгортання версій, а недоліком – вимога до надійних засобів безпеки.

Програмне забезпечення як послуга дозволяє користувачам підключатися до хмарних програм та використовувати їх через Інтернет. Стандартними прикладами можуть бути електронна пошта, календар та офісні засоби.

SaaS надає повноцінний набір програмного забезпечення, який сплачується постачальнику хмарних служб у міру використання. Орендується використання програми для організації, і користувачі підключаються до нього через Інтернет, зазвичай, за допомогою веб-браузера. Вся базова інфраструктура, програмне забезпечення проміжного шару, програмне забезпечення програм і дані програм знаходяться в центрі обробки даних постачальника. Постачальник служб керує обладнанням та програмним забезпеченням на основі відповідної угоди про обслуговування та забезпечує доступність та безпеку додатків та даних. SaaS дозволяє вашій організації швидко запускати програму з мінімальними попередніми витратами [10].

Щоб надати програми SaaS користувачам не потрібно купувати, встановлювати, оновлювати або обслуговувати обладнання, програмне забезпечення проміжного шару або програмне забезпечення.

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

SaaS підвищує мобільність співробітників, оскільки програми та дані SaaS доступні користувачам з будь-якого комп'ютера або мобільного пристрою, підключеного до Інтернету. Не потрібно піклуватися про розробку програм для роботи на різних типах комп'ютерів та пристроїв, тому що постачальник послуг вже зробив це за вас.

Перевагою є зниження вкладень коштів в апаратне забезпечення, а недоліком – вимога до надійних засобів безпеки.

Щоб краще зрозуміти, що включає в себе кожна з моделей обслуговування, розглянемо рисунок 1.1, який ілюструє склад кожної моделі у порівнянні з традиційними рішеннями.



Рисунок 1.1 - Склад моделей обслуговування хмарних технологій у порівнянні з локальним рішенням

Висновок до розділу 1

У цьому розділі розглянуто сучасні хмарно-орієнтовані технології, різні моделі хмарних сервісів, а також визначення хмарних обчислень. Було досліджено, що впровадження хмарних технологій дозволяє відмовитися від застарілого локального інфраструктурного підходу до запуску сервісів у сфері інформаційно-комунікаційних технологій

Також було описано архітектуру хмарних сервісів. Крім того, було виявлено актуальність використання хмарних технологій, а також розглянуто певні загрози, пов'язані з ними.

		Медведевко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

2.1 Дослідження можливостей хмарних сервісів

На сьогоднішній день існує велика кількість хмарних сервісів, які дають користувачам доступ до своїх ресурсів практично з будь-якої точки планети завдяки мережі Інтернет. Прикладом таких сервісів можуть бути: ClickUp, Wrike, Asana та Google Workspace. Далі розглянемо кожен з цих сервісів більш детально.

2.1.1 Універсальна хмарна платформа ClickUP

ClickUp — це універсальна платформа, яка є ідеальним місцем для команд, щоб збиратися разом, проводити мозковий штурм, планувати та співпрацювати над усім, починаючи від документації процесів і закінчуючи дизайном продукту (рис. 2.1). Хоча покладатися на один інструмент для такої кількості випадків використання може здатися наляжним, ClickUp створено для цього [11].

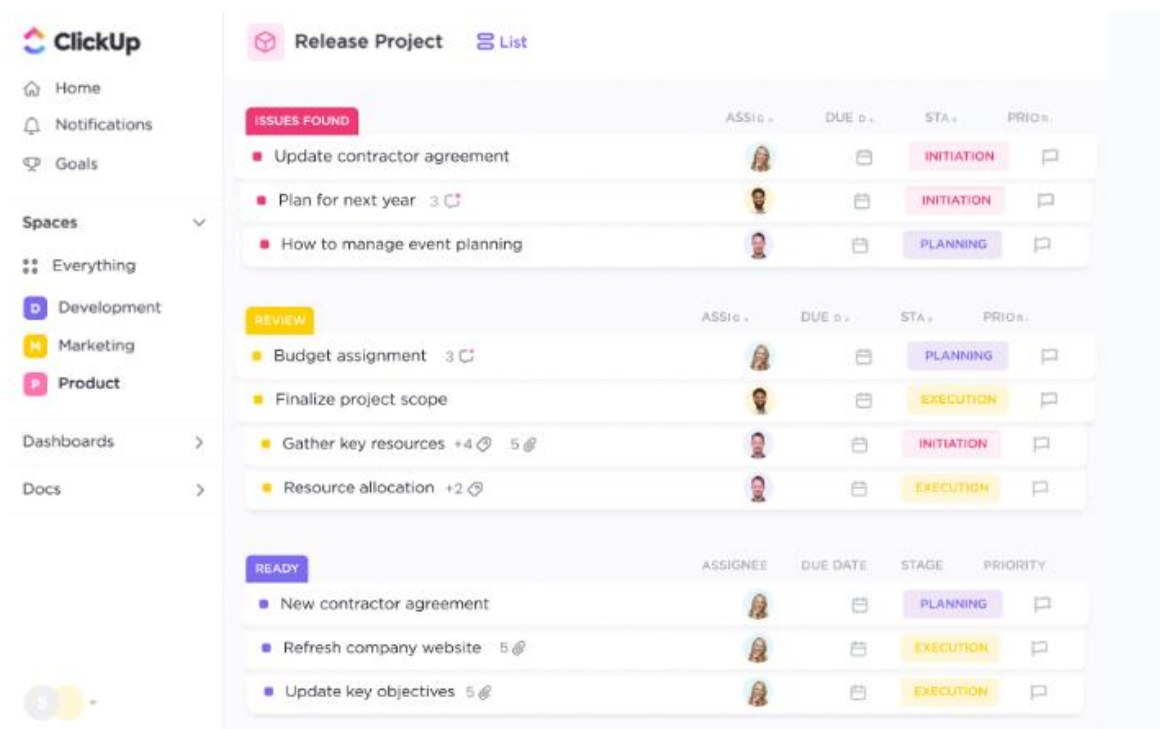


Рисунок 2.1 – Зовнішній вигляд ClickUP

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

ClickUp також має власні інструменти для відстеження KPI проєктів та візуалізації ієрархії проєктів. Користувачі можуть адаптувати програмне забезпечення до своїх конкретних потреб, дозволяючи їм створити систему, яка найкраще відповідає їхнім робочим процесам.

У цього сервіса наявні 4 плани підписки: Безкоштовний, Unlimited, Business, Enterprise (рис. 2.2). Кожен з планів включає в собі різний функціонал наведений на рисунку нижче [12].

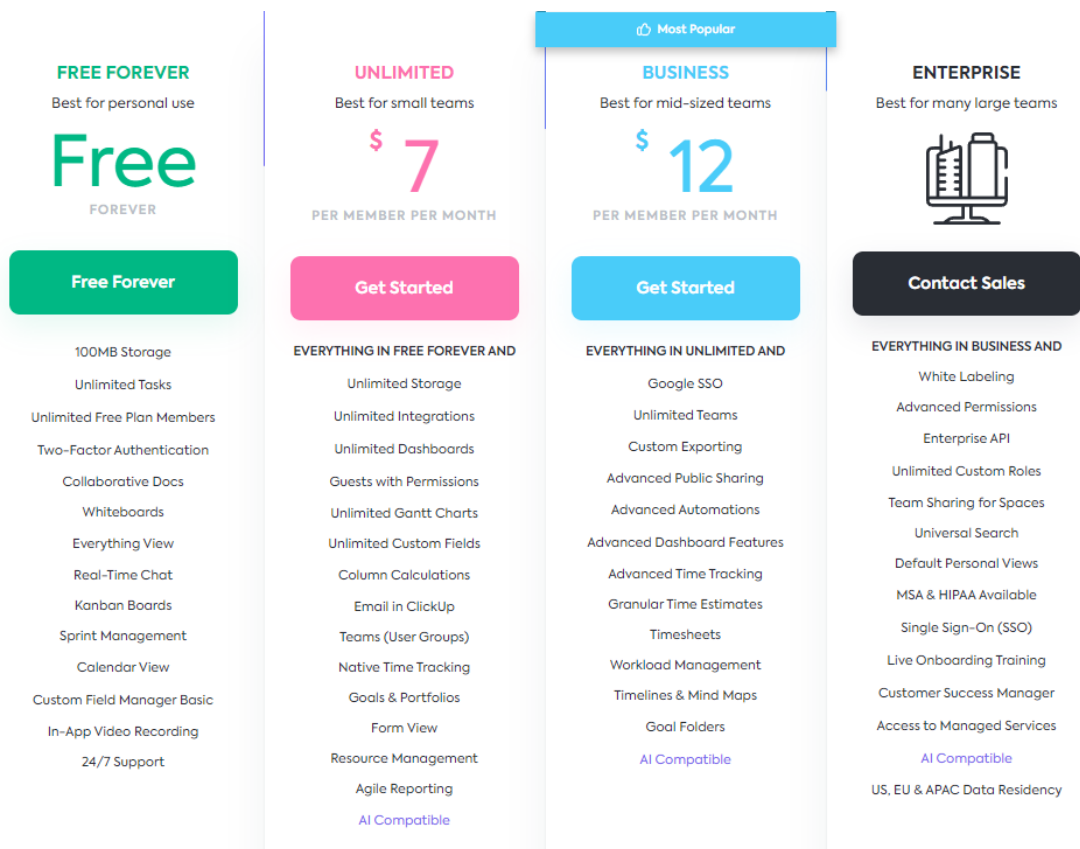


Рисунок 2.2 – Плани підписки ClickUP

Безкоштовна версія ClickUp — це чудовий спосіб для команд випробувати платформу та побачити її потенціал. Крім того, якщо програмне забезпечення вас вразить, ви можете перейти на один із платних планів для більш розширених функцій, таких як графіки проєктів і аналітика.

Основними перевагами сервісу є: функція автоматизації, яка дозволяє користувачам швидко визначати робочі процеси, заощаджуючи багато часу, доступ

до своїх даних будь-де за допомогою хмарної системи ClickUp і синхронізації облікових записів на кількох пристроях. До недоліків можна віднести функціонал та інтерфейс, який може бути незрозумілим та складним для освоєння для більшості нових користувачів, які менше знайомі з програмним забезпеченням для керування проєктами.

ClickUp – це хороший інструмент для управління проєктами та командної співпраці. Він пропонує широкий спектр функцій, які дозволяють користувачам планувати, відстежувати та контролювати прогрес проєктів.

2.1.2 Платформа управління проєктами Wrike

Wrike — це хмарна платформа для управління проєктами, розроблена, щоб допомогти командам працювати разом ефективніше (рис. 2.3). Він містить різноманітні функції, такі як списки завдань, керування ресурсами, відстеження часу та звітування, спеціальні інформаційні панелі, автоматизований робочий процес тощо. Wrike також має мобільний додаток, щоб ви могли отримувати доступ до проєктів на ходу [13].



Рисунок 2.3 – Зовнішній вигляд Wrike

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

На відміну від ClickUp, Wrike має 5 планів підписки: Free, Team, Business, Enterprise, Pinnacle [14] (рис. 2.4).

	★ QUICK START	🔥 MOST POPULAR		⚡ MOST ENHANCED
Free For teams getting started Intelligent task management	Team For growing teams Effective team management	Business For all teams across an organization Customizable platform for any use case	Enterprise For large teams Enterprise-grade security and scalability	Pinnacle For teams with complex work needs Advanced tools and analytics for complex work
\$0 user/ month	\$9.80 user/ month	\$24.80 user/ month	Contact us	Contact us
Get started	Try for free	Try for free	Try for free	Try for free
No credit card required	No credit card required	No credit card required	No credit card required	No credit card required
Key features: ✓ Web, desktop, and mobile apps ✓ Project & task management ✓ AI content generation ✓ Board view ✓ Table view ✓ Active task limitations apply ➤ Compare all features	Key features: ✓ 3-25 users ✓ Unlimited projects ✓ Unlimited tasks & subtasks ✓ Unlimited custom fields ✓ Unlimited request forms ✓ 20 free collaborators ✓ Interactive Gantt charts ✓ Automations (50 actions/user/month) ✓ Custom workflows ✓ Analytics view ✓ Calendar view ✓ Dashboards ✓ Use case templates ✓ Google Sign-In ✓ External requester collaboration ✓ Integrations & open API ✓ 2 GB storage per user ➤ Compare all features	Team plan features plus: ✓ 5-200 users ✓ Folder structure & nested projects ✓ Cross-tagging ✓ Project Blueprints ✓ Custom item types ✓ Automations (200 actions/user/month) ✓ AI risk prediction & work creation ✓ Approvals & guest approvals ✓ File and video proofing (30+ file formats) ✓ Resource management, workloads & time tracking ✓ Reports and Unlimited Dashboards ✓ User groups & permissions ✓ DAM Integrations and Cloud Content Connector ✓ Adobe Creative Cloud Extensions ✓ 5 GB storage per user ➤ Compare all features	Business plan features plus: ✓ 5 to unlimited users ✓ SAML-based SSO ✓ Two-Factor Authentication (2FA) ✓ Password policies ✓ Custom access roles ✓ Customizable user types ✓ Admin permissions ✓ User audit reports ✓ Automations (1000 actions/user/month) ✓ 10 GB storage per user ➤ Compare all features	Enterprise plan features plus: ✓ 5 to unlimited users ✓ Locked Spaces ✓ Advanced reporting & BI ✓ Team utilization and performance dashboard ✓ Job roles ✓ Budgeting and billable hours ✓ Bookings (project-level effort & time planning) ✓ SharePoint and HTML5 proofing and approvals ✓ Automations (1500 actions/user/month) ✓ 15 GB storage per user ➤ Compare all features

Рисунок 2.4 – Плани підписки Wrike

Цікавою є наявність плану під назвою Pinnacle, який включає в собі функціонал всіх попередніх, а також має функцію перевірки HTML, розширене управління ресурсами, бюджетування і закриті простори. Закриті простори — це обмежені, безпечні простори для конфіденційної співпраці, наприклад на рівні правління чи керівників, що є великим плюсом для захисту конфіденційної інформації.

Плюси цього хмарного сервіса: запити, подані через форми, можуть автоматично перетворюватися на завдання, автоматично оновлює кінцеві терміни на діаграмах Ганта, коли змінюються часові рамки проєкту, мобільна сумісність. Мінуси: не дуже інтуїтивно зрозумілий інтерфейс, що може заплутати користувачів, для ефективного використання Wrike може знадобитися деяке навчання, відсутність параметрів налаштування сповіщень електронною поштою про оновлення, часто користувачі відмічають присутність багів у Wrike.

2.1.3 Сервіс керування завданнями Asana

Asana схожа на інше програмне забезпечення для керування завданнями та проєктами, яке дозволяє командам організовувати, співпрацювати, планувати та виконувати завдання (рис. 2.5). Це веб-інструмент керування завданнями та спільної роботи, який усуває безлад електронної пошти та об'єднує всі завдання. Команди можуть використовувати Asana для відстеження всіх завдань, співпраці з іншими членами команди, обміну пов'язаними файлами тощо [15].

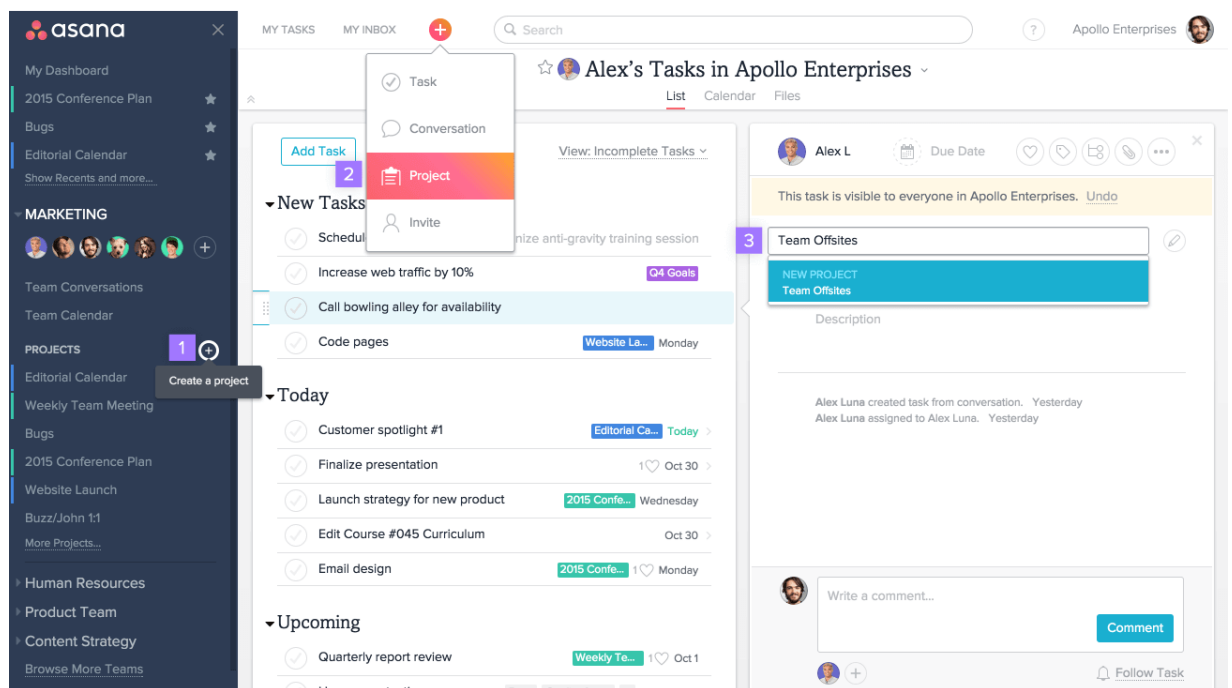


Рисунок 2.5 – Зовнішній вигляд Asana

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

Asana має лише 3 плани підписки: Personal, Starter, Advanced [16] (рис. 2.6).

Personal

For individuals and small teams looking to manage their tasks.

€0

Free forever

Get started

Manage tasks and personal to-dos:

✓ Collaborate with up to 10 teammates

✓ [Unlimited tasks](#)

✓ Unlimited projects

✓ Unlimited messages

✓ Unlimited activity log

✓ Unlimited file storage (100MB per file)

✓ Unlimited assignee and due dates

✓ [List view projects](#)

✓ Board view projects

✓ [Calendar view](#)

✓ Basic search filters

✓ Status updates

✓ iOS and Android mobile apps

✓ Time tracking with integrations - [See time tracking apps](#)

✓ 100+ free integrations with your favorite apps - [Learn more](#)

Starter

For growing teams that need to track their projects' progress and hit deadlines.

€10.99

Per user, per month billed annually
€ 13.49 billed monthly

Get started

[Purchase now](#)

Everything in Personal, plus:

✓ Collaborate with up to 500 teammates

✓ [Timeline view](#)

✓ Gantt view

✓ Asana Intelligence **NEW**

✓ [Workflow Builder](#)

✓ Project dashboards

✓ [Advanced search](#)

✓ [Global custom fields](#)

✓ [Forms](#)

✓ 250 Automations per month

✓ Start dates and times

✓ Custom project templates

✓ Admin Console

✓ Private teams & projects

✓ Unlimited free guests

Advanced

For companies that need to manage a portfolio of work and goals across departments.

€24.99

Per user, per month billed annually
€ 30.49 billed monthly

Get started

[Purchase now](#)

Everything in Starter, plus:

✓ Collaborate with up to 500 teammates

✓ [Goals](#)

✓ [20 Portfolios](#)

✓ Asana Intelligence **NEW**

✓ [Workload](#)

✓ 25,000 Automations per month

✓ [Forms branching & customization](#)

✓ [Approvals](#)

✓ Proofing

✓ Lock custom fields

✓ [Advanced reporting](#)

✓ [Time tracking](#)

✓ Scaled security

Рисунок 2.6 – Плани підписки Wrike

Asana дозволяє делегувати завдання, призначати терміни виконання та визначати пріоритетність робочих процесів за допомогою можливостей перетягування, миттєво переглядати залежності завдань у формі моделі даних Work Graph і діаграм Ганта, має інтеграцію з іншими службами, як Dropbox, SurveyMonkey, Google Drive і понад 1000 сторонніх програм. Asana використовується командами для організації та відстеження внутрішніх проєктів,

для співпраці з зовнішніми стейкхолдерами та одноосібними підприємцями для організації та відстеження своєї роботи.

Asana має ряд переваг, які роблять її популярним вибором для команд, які хочуть поліпшити свою ефективність управління проектами. Ось деякі з цих переваг: Asana має простий у використанні інтерфейс, який легко освоїти, пропонує широкий спектр функцій. Але також є і мінуси: важко використовувати, якщо користувачі не знайомі з програмним забезпеченням для управління проектами, відсутність гнучкості в постановці повторюваних завдань.

2.1.4 Пакет хмарних інструментів Google Workspace

Google Workspace — це пакет спеціалізованого хмарного програмного забезпечення й інструментів для спільної роботи від компанії Google, доступний за передплатою (рис. 2.7). Він включає в себе такі веб-застосунки, як Gmail, Контакти, Календар, Meet та Chat для спілкування; Документи, Таблиці, Презентації, Форми та Сайт для спільної роботи над документами, таблицями, презентаціями, опитуваннями та веб-сайтами.

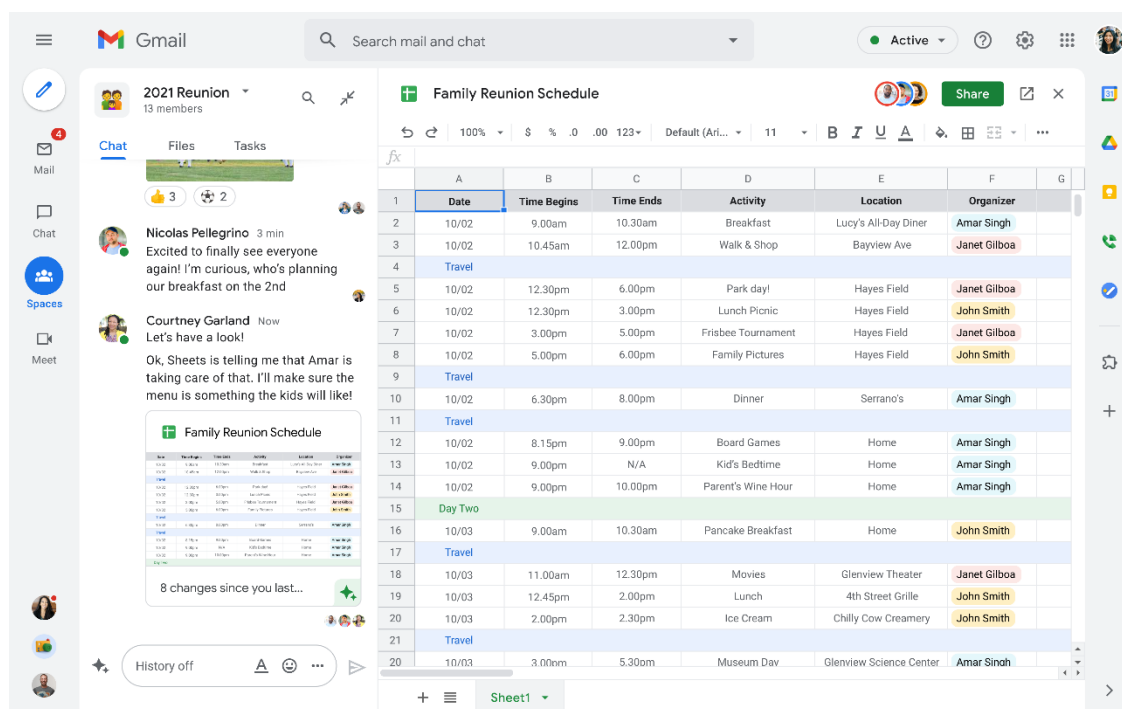


Рисунок 2.7 – Зовнішній вигляд Google Workspace

Google Workspace не має безкоштовної версії, а включає в себе тільки Business Starter, Business Standard, Business Plus та Enterprise версії [17] (рис. 2.8).

THE MOST POPULAR			
Business Starter \$5.40 USD \$6 * per user per month with an annual contract Start using ✓ Secure corporate email with addresses in your own domain ✓ Video meetings with up to 100 participants ✓ 30 GB per user combined storage* ✓ Management tools and security features ✓ Standard support	Business Standard \$10.80 USD \$12 * per user per month with an annual contract Start using ✓ Secure corporate email with addresses in your own domain ✓ Video meetings with up to 150 participants with recording function ✓ 2 TB per user in pooled storage* ✓ Management tools and security features ✓ Standard support (with the option of a paid upgrade to advanced support)	Business Plus \$ 18USD per user per month with an annual contract Start using ✓ Secure corporate email with your own address, as well as functions for providing and storing electronic documents ✓ Video meetings for up to 500 participants with recording and participation tracking features ✓ 5 TB per user in pooled storage* ✓ Improved management and security features, including Google Vault and advanced endpoint management ✓ Standard support (with the option of a paid upgrade to advanced support)	Enterprise Contact sales for prices Contact sales department ✓ Secure corporate email with your own address, as well as functions for providing electronic documents, storage and S/MIME encryption ✓ Video meetings with up to 1,000 participants, plus video meeting recording, participation tracking, noise reduction, and live streaming for domain users ✓ 5 TB per user pooled storage (more can be requested)* ✓ Advanced management tools, security and compliance features including Google Vault, DLP, storage regions, and enterprise endpoint management ✓ Extended support (with the option of paid upgrade to premium support)

Рисунок 2.8 – Плани підписки Google Workspace

Google Workspace можна використовувати для будь-якого виду діяльності, яка вимагає спілкування та спільної роботи. Він ідеально підходить для малого та середнього бізнесу, шкіл, некомерційних організацій та окремих користувачів.

Gmail можна використовувати для надсилання та отримання електронних листів, а також для створення та управління контактами. Календар можна використовувати для планування зустрічей та подій. Meet можна використовувати для проведення відеоконференцій. Chat можна використовувати для чату в реальному часі з іншими користувачами.

Документи, Таблиці та Презентації можна використовувати для створення та редагування документів, таблиць та презентацій у співпраці з іншими користувачами. Форми можна використовувати для створення опитувань і форм. Сайт можна використовувати для створення веб-сайтів.

		Медведенко А.В.			KIK.KP.B – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

Ось деякі з переваг використання Google Workspace: доступний з будь-якого пристрою з доступом до Інтернету, пропонує широкий спектр функцій, які можуть допомогти поліпшити продуктивність та ефективність, використовує сучасні технології безпеки для захисту даних користувачів. Мінуси: не завжди повністю інтегрується з іншими програмами.

2.2 Дослідження можливостей пакету Google Workspace Enterprise

Якщо обирати один з вищезазначених сервісів, то кращим вибором буде Google Workspace і на це є ряд причин. Він простий у використанні та не вимагає спеціальної підготовки. Це робить його хорошим вибором для організацій будь-якого розміру. Google Workspace відповідає найвищим стандартам безпеки. Він шифрує дані використовуючи стандарти AES-256 та TLS 1.2, має багатофакторну аутентифікацію та контроль доступу. Google Workspace має систему відновлення в разі несправності, яка захищає ваші дані від втрати. Ця система зберігає копії ваших даних на кількох серверах, що дозволяє відновити дані, якщо один із серверів вийде з ладу.

Google Workspace Enterprise — це найвищий рівень передплати на пакет хмарних програмних продуктів та інструментів для спільної роботи Google Workspace. Він пропонує широкий спектр функцій і переваг, які призначені для задоволення потреб великих організацій.

- Доступ до сучасних інформаційних технологій без необхідності вкладатися у власну інфраструктуру і розгортати складне програмне забезпечення;
- Переклад функції резервного копіювання, безпеки та управління на Google, що дозволяє організаціям зосередитися на власних стратегічних завданнях;
- Платіж за принципом оренди, що дозволяє організаціям переносити витрати на програмне забезпечення з капітальних в операційні;
- Швидке розгортання системи;
- Зниження витрат на навчання співробітників, тому що всі інструменти знайомі і легкі у використанні;

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

- Передова система забезпечення безпеки та приватності даних, яка включає в себе вбудовані антивірус і антиспам, відповідність стандарту ISO/IEC 27001, ISO/IEC 27017 та ISO/IEC 27018 і вимогам Європейського Союзу в галузі безпеки;
 - Постійне оновлення програмного забезпечення до найновіших версій;
- У порівнянні з іншими планами, Enterprise включає в себе найбільшу кількість можливостей (табл. 2.1).

Таблиця 2.1

Можливості планів

Business Starter	Business Standard	Business Plus	Enterprise
Захищена електронна пошта з корпоративними адресами	Захищена електронна пошта з корпоративними адресами	Захищена електронна пошта з корпоративними адресами + збереження електронних документів для юридичних цілей	Захищена електронна пошта з корпоративними адресами + збереження персональних даних і електронних документів для юридичних цілей, шифрування S/MIME
Відеозустрічі на 100 учасників	Відеозустрічі на 150 учасників із можливістю запису	Відеозустрічі на 500 учасників + записування відеозустрічей, відстеження відвідуваності	Відеозустрічі на 1000 учасників + записування відеозустрічей, відстеження відвідуваності, заглушення шумів, прямі трансляції для користувачів із корпоративного домену
30 ГБ об'єднаного сховища на користувача	2 ТБ об'єднаного сховища на користувача	5 ТБ об'єднаного сховища на користувача	5 ТБ об'єднаного сховища на користувача (можна надіслати запит на збільшення обсягу)

Функції безпеки й керування	Функції безпеки й керування	Додаткові функції безпеки й керування, зокрема Сейф і розширене керування кінцевими точками	Додаткові функції захисту, адміністрування та забезпечення відповідності вимогам, зокрема Сейф, DLP, регіони збереження даних і керування корпоративними кінцевими точками
Стандартна підтримка	Стандартна підтримка (доступний платний перехід на розширену підтримку)	Стандартна підтримка (доступний платний перехід на розширену підтримку)	Розширена підтримка (доступний платний перехід на преміум-підтримку)

Компанія Google надає можливість використовувати власні сервіси (рис. 2.9).

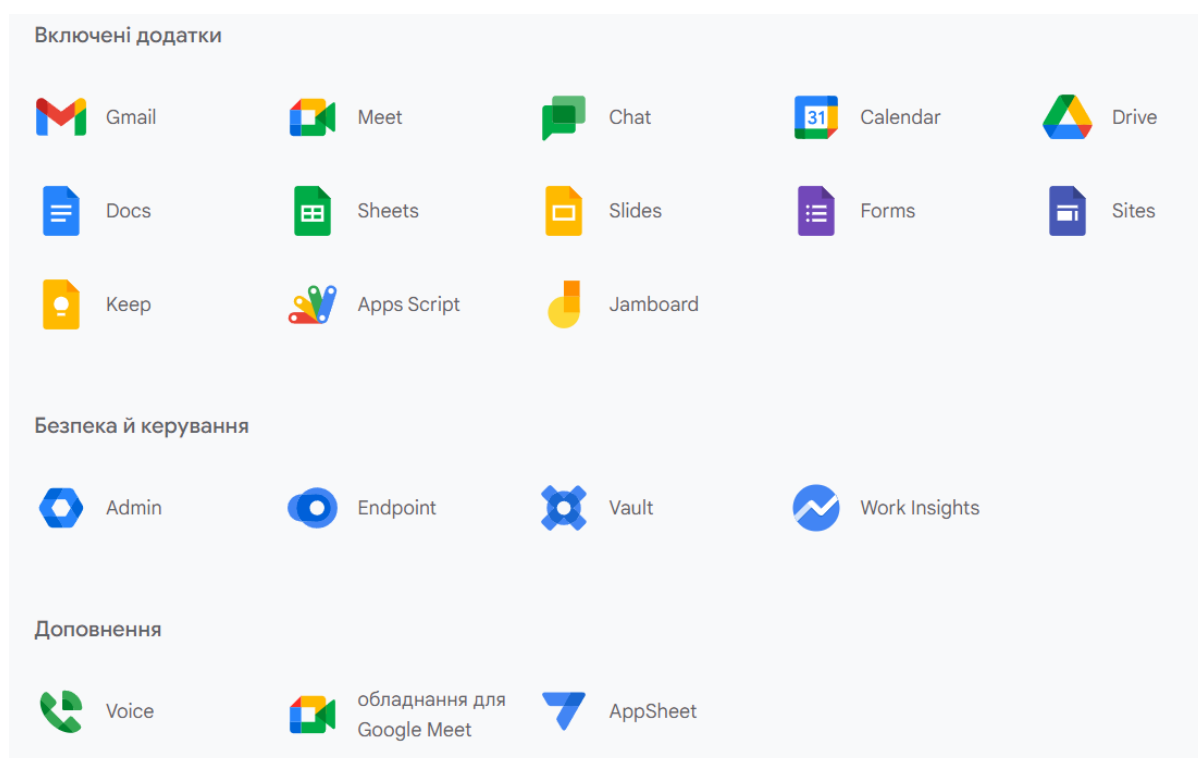


Рисунок 2.9 – Сервіси Google

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				33
Змн.	Арк.	№ докум.	Підпис	Дата		

Сьогодні хмарні сервіси все частіше використовуються організаціями для зберігання та обробки даних. Однак, незважаючи на те, що провайдери хмарних сервісів пропонують широкий спектр функцій безпеки, організації все частіше прагнуть до того, щоб самостійно налаштовувати та контролювати ці функції.

Існує кілька причин такої тенденції. По-перше, організації хочуть бути впевнені, що їхні дані захищені відповідно до їхніх власних вимог. По-друге, організації хочуть мати можливість адаптувати функції безпеки до своїх конкретних потреб. По-третє, організації хочуть мати контроль над тим, як їхні дані використовуються.

Крім того, організації повинні враховувати ризик компрометації конфіденційної інформації. Це може статися в результаті випадкової втрати пристрою або через дії зловмисника. Щоб захистити свої дані, організації повинні використовувати хмарну службу з надійними вбудованими засобами безпеки. Розширення функцій віддаленого доступу для підтримки передових практик забезпечення безпеки може бути складним і дорогим завданням.

Через це перед провайдером стоїть складна задача як забезпечити безпеку інформації. Компанії Google використовує свої методики щоб захистити Google Workspace.

Користувач має повний контроль над своїми даними, а працівники та інженери Google не мають до них постійного доступу. Тому ці дані ізольовані і компанія не може їх використовувати для своїх цілей. Навіть якщо компанії потрібен доступ, то його потрібно спочатку ухвалити з користувачем.

Багатофакторна аутентифікація (MFA) є одним з найефективніших способів захисту від несанкціонованого доступу до даних [18]. MFA вимагає від користувачів ввести не менше двох факторів автентифікації для входу в систему. Google Workspace підтримує MFA, що дозволяє організаціям підвищити рівень безпеки своїх даних. MFA в Google Workspace можна налаштувати за допомогою таких параметрів: код з мобільного пристрою, безконтактний ключ, другий пристрій. Налаштування параметрів MFA дозволяє забезпечити належний захист

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

своїх даних. Наприклад, організації можуть обмежити доступ до даних з загальнодоступних комп'ютерів або з використанням відкритої мережі Wi-Fi.

Всі дані шифруються на серверах Google, а при передачі даних від користувача до серверів використовується TLS Шифрування [19].

Google Workspace записує події активності користувачів і адміністраторів у своїх службах. Журнали також відстежують усі дії, які виконує інженер служби підтримки Google [20]. Усі журнали зберігаються централізовано та доступні протягом 90 днів.

Google застосовує суворі процедури безпеки у своїх центрах обробки даних, які важко зламати. Центри обробки даних Google мають кілька рівнів фізичної безпеки, які запобігають несанкціонованому доступу до фізичних серверів. Безпека починається з багатофакторної автентифікації, цілодобового моніторингу та включає біометричне сканування для доступу до центру обробки даних. А від атак хакерів використовується сервіси захисту від спаму, фішингу та інших загроз за допомогою технологій IRM и DLP.

Google адаптує Google Workspace відповідно до галузі використання та регіону користувача, щоб допомогти споживачам відповідати вимогам, зазначеним в ISO/IEC 27001 [21], ISO/IEC 27017, ISO/IEC 27018.

2.3 Дослідження рівнів безпеки даних у хмарному сервісі Google Workspace

Google Workspace використовує багаторівневу систему безпеки, яка включає в себе фізичні, логічні, дані рівня та розгорнута за моделлю SaaS. На фізичному рівні дані захищені від несанкціонованого доступу за допомогою фізичних заходів безпеки, таких як охорона, відеоспостереження та контроль доступу. На логічному рівні дані захищені за допомогою криптографії, автентифікації та авторизації. На рівні даних дані захищені за допомогою політики доступу та управління доступом на основі ролей (RBAC).

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

2.3.1 Безпека на рівні центра обробки даних

Центри обробки даних Google – це великі об’єкти центрів обробки даних, які Google використовує для надання своїх послуг, які об’єднують великі диски, комп’ютерні вузли, організовані в рядах стійок, внутрішні та зовнішні мережі, засоби контролю навколишнього середовища та операційне програмне забезпечення. Офіційних даних про кількість серверів у центрах обробки даних Google немає, але Gartner оцінив у звіті від липня 2016 року, що Google на той час мав 2,5 мільйона серверів. Ця цифра змінюється, оскільки компанія розширює потужності та оновлює апаратне забезпечення. [22]. Вибір основного центра даних залежить від регіону який вказав користувач при початковій установці. Всі дані реплікуються мінімум у двох центрах обробки даних, а їх розташування показано на рисунку 2.10 [22]. Якщо через якусь причину один з центрів перестане працювати, то дані не втраяться тому що вони доступні в інших центрах обробки даних.

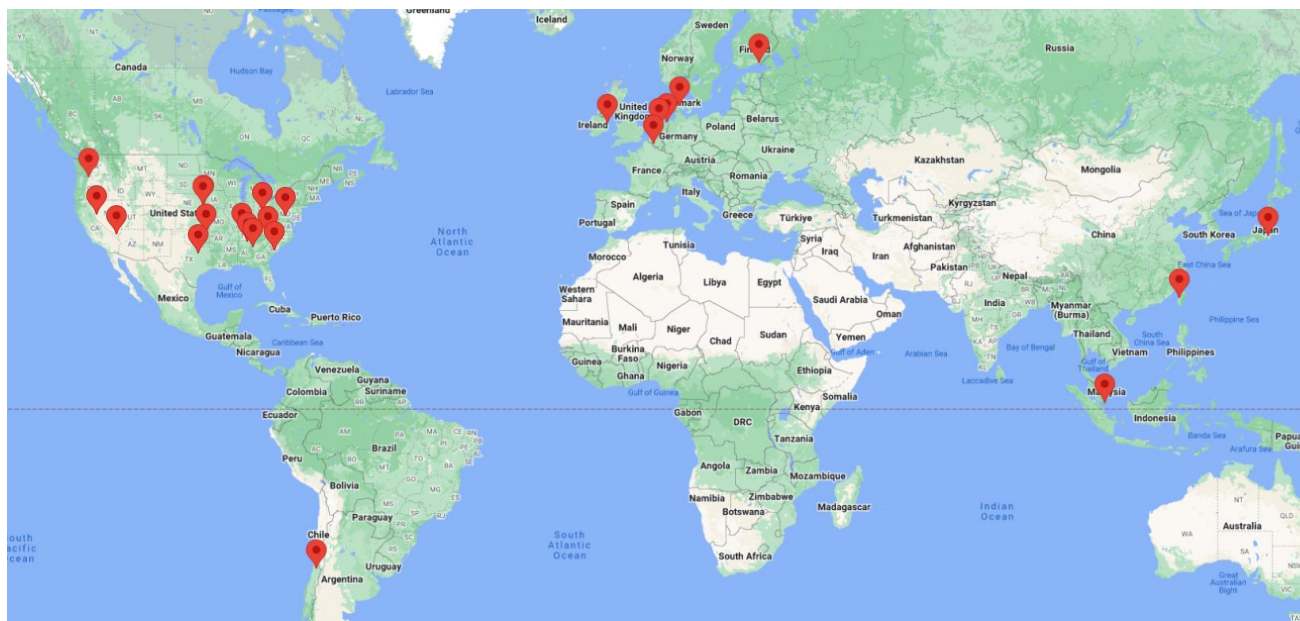


Рисунок 2.10 – Розташування центрів обробки даних

Для деяких служб усунення несправностей може не призвести до збою служби. Клієнти повинні припускати, що в будь-який момент часу їхні дані можуть оброблятися в одному або кількох центрах обробки даних у регіоні.

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

Дані Google Workspace зберігаються в мережі центрів обробки даних компанії Google, які знаходяться під управлінням служби Google Cloud Platform Services. Google Cloud Platform Services - постачальник загальнодоступних хмар, який пропонує набір обчислювальних послуг для виконання будь-яких завдань: від керування даними до доставки Інтернету та відео через Інтернет до штучного інтелекту та інструментів машинного навчання [23].

Ці центри обробки даних забезпечують надання послуг і захист інформації від стихійних лих або несанкціонованого доступу. Співробітники мають цілодобовий доступ до центрів обробки даних лише для виконання пов'язаних із роботою завдань. Реалізовано розподіл ролей, завдяки якому персонал, який має фізичний доступ до місця зберігання даних, жодним чином не може визначити місцезнаходження конкретних даних клієнта. Контроль фізичного доступу здійснюється за допомогою численних процедур автентифікації та безпеки. Центри обробки даних оснащені датчиками руху, системами відеоспостереження та сигналізації. Безпека даних у разі стихійних лих забезпечуються сейсмостійкими шафами, а також автоматичним протипожежним захистом і системою пожежогасіння.

Політика Google заснована на принципах управління доступом на основі ролей (RBAC) і мінімальних привілеїв. RBAC дозволяє визначати набори дозволів, які надаються певним ролям. Мінімальні привілеї гарантують, що співробітники мають доступ лише до тих даних, які їм необхідні для виконання своїх робочих завдань і відповідають необхідним вимогам, що охоплюють в тому числі перевірку благонадійності, контроль відбитків пальців, обов'язкове навчання заходам безпеки і утвердження прав доступу.

У центрах обробки даних Google використовується система контролю доступу з подвійною автентифікацією, яка пов'язана із системною сигналізацією. Несанкціонована діяльність і невдалі спроби доступу реєструються системою контролю доступу та досліджуються відповідно. Авторизований доступ до всіх бізнес-операцій і центрів обробки даних обмежено залежно від зон і посадових обов'язків особи. Google має та підтримує політику безпеки для свого персоналу та

		Медведев А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

вимагає навчання з безпеки як частину навчального пакету для свого персоналу. Персонал із безпеки інфраструктури Google відповідає за постійний моніторинг інфраструктури безпеки Google, перегляд Послуг і реагування на інциденти безпеки [24].

Адміністратори баз даних Google мають доступ до всіх ресурсів у базі даних, у тому числі до даних клієнтів. Однак вони можуть використовувати ці дані лише для надання послуг клієнтам. Google має сувору політику захисту даних клієнтів. Ця політика забороняє адміністраторам баз даних використовувати дані клієнтів для будь-яких інших цілей, крім надання послуг. В рамках надання послуг адміністратори баз даних можуть звертатися до даних клієнтів для виконання таких дій, як: налаштування бази даних, перенесення клієнтів з однієї бази даних в іншу, рішення технічних проблем.

Дані клієнта - це будь-яка інформація, яка може бути використана для ідентифікації або зв'язку з фізичною особою, дані з веб-сайтів, додатків, звичайних магазинів та інші відомості [25]. Дані клієнта не включають в себе дані адміністраторів, дані про платежі і оперативну інформацію про служби. Контент – це підмножина даних клієнта, яка зазвичай є конфіденційною інформацією та зазвичай не передається незашифрованою. Рівень доступу адміністратора до даних описано у таблиці 2.2.

Таблиця 2.2

Рівень доступу адміністратора до даних

Адміністратор	Дані клієнта	Контент
Оперативна група	При необхідності	Так, як виняток
Організація, що забезпечує підтримку	При необхідності у відповідь на запит в службу підтримки	Ні
Інженери	Немає прямого доступу. Дані можуть передаватися в ході усунення неполадок.	Ні
Партнери	З дозволу клієнта	З дозволу клієнта
Співробітники Google	Ні	Ні

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

Мережі в центрах обробки даних (ЦОД) розділені на сегменти, що дозволяє ізолювати критично важливі внутрішні сервери та пристрої зберігання даних від загальнодоступних інтерфейсів. Це допомагає захистити ці ресурси від несанкціонованого доступу, використання або розкриття і виявляти спроби вторгнення і ознаки уразливості системи [26].

Використання служб Google Workspace передбачає передачу даних між комп'ютером або мобільним пристроєм, серверами Google і, іноді, іншими користувачами. Google за умовчанням вмикає шифрування під час передачі між пристроєм і центрами обробки даних і використовує протокол безпеки транспортного рівня (TLS) для шифрування запитів перед передачею за межі Google. Це допомагає запобігти третім особам від використання вразливостей у підключеннях до Інтернету для доступу до конфіденційних даних [27].

Протокол TLS гарантує безпечне підключення клієнтів до сервера, конфіденційність і цілісність даних, що пересилаються між комп'ютером користувача і центром обробки даних.

Статичні дані в екосистемі Google підписуються спеціальним криптографічним ключем. За замовчуванням Compute Engine шифрує клієнтський вміст у стані спокою. Compute Engine обробляє та керує цим шифруванням за користувача без будь-яких додаткових дій з його боку. Цей параметр називається шифруванням, керованим Google.

Однією з причин масштабованості та низької вартості Google Workspace є те, що послуга доступна багатьом користувачам, тобто декілька різних клієнтів розміщені на одних і тих самих апаратних ресурсах. А для того щоб окремо контролювати дані кожного клієнта використовується Google Directory. Він відокремлює клієнтів один від одного використовуючи зони безпеки.

Протягом останніх кількох років компанія Google спостерігала, що розподілені атаки типу «відмова в обслуговуванні» (DDoS) частішають і збільшуються в геометричній прогресії. Сучасні робочі навантаження, пов'язані з Інтернетом, знаходяться під постійним ризиком атак із наслідками, починаючи від погіршення продуктивності та досвіду користувача для законних користувачів, до

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

збільшення операційних витрат і витрат на хостинг, до повної недоступності критично важливих робочих навантажень. Клієнти Google Cloud можуть використовувати Cloud Armor, щоб використовувати глобальний масштаб і потужність межі мережі Google, щоб захистити своє середовище від найбільших DDoS-атак. Адаптивний захист Cloud Armor може виявляти й аналізувати трафік на ранніх етапах життєвого циклу атаки [28].

Google продовжує розробляти високоефективні автоматичні системи виправлення, які вирішують проблеми, виявлені системами моніторингу, без втручання людини. Це значно підвищує рівень безпеки та гнучкості сервісу. Google Workspace проводить тестування на захист від несанкціонованого доступу, щоб постійно вдосконалювати процедури реагування на інциденти. Результати цих тестів дають професіоналам із безпеки можливість створювати систематичні, повторювані та оптимізовані покрокові процеси реагування на інциденти та автоматизувати ці процеси.

2.3.2 Безпека на рівні користувача

Усі служби Google Workspace пропонують індивідуальні функції безпеки, якими клієнт може керувати. Ці функції дозволяють забезпечити відповідність нормативним вимогам, надати співробітникам доступ до служб і контенту, захистити від спаму та шкідливого програмного забезпечення, а також шифрувати дані. Адміністратори можуть контролювати, які елементи шифруються, і використовувати різні алгоритми шифрування для різних цілей.

Користувач може налаштувати розміщені захищені/багатоцільові розширення Інтернет-пошти (S/MIME) на консолі адміністратора Google, щоб допомогти захистити своїх співробітників у організації від фішингу, шкідливих вкладень та інших загроз електронної пошти. S/MIME покращує безпеку електронної пошти шляхом шифрування та додавання цифрового підпису до повідомлень. Повідомлення розшифровуються за допомогою комбінації відкритого та закритого ключів. Коли S/MIME розміщено, організація, яка

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

використовує S/MIME для шифрування, зберігає закритий ключ. Шифрування на стороні клієнта (CSE) Google Workspace також дозволяє користувачам надсилати й отримувати зашифровані повідомлення S/MIME. Але з CSE особистими ключами керує зовнішня служба ключів для підвищення конфіденційності та захисту даних [29].

Служба Google Message Encryption забезпечує шифрування повідомлень на вимогу для організації, щоб безпечно спілкуватися з діловими партнерами та клієнтами відповідно до політики безпеки або на основі «за потреби». Без складності та витрат, пов'язаних із застарілими локальними технологіями шифрування, служба Google Message Encryption робить шифрування електронних повідомлень простим і доступним.

Служба Google Message Encryption захищає вихідну електронну пошту до центру обробки даних за допомогою безпечного зашифрованого з'єднання SSL/TLS. У центрі обробки даних повідомлення перевіряються на наявність вірусів і відповідність політиці обміну повідомленнями. На основі централізовано керованих політик повідомлення шифруються для кожного одержувача. Зашифровані повідомлення доставляються безпосередньо до вхідних повідомлень одержувачів або зберігаються на веб-порталі для безпечного отримання. Рисунок 2.11 наглядно демонструє цей цикл [30].

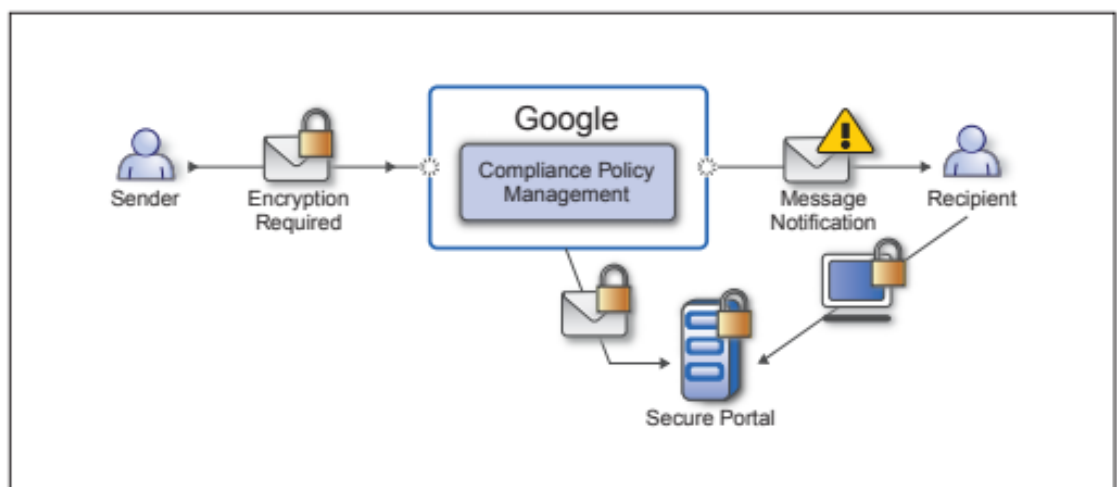


Рисунок 2.11 – Робота Google Message Encryption

Адміністратори можуть створювати додаткові механізми аутентифікації, такі як двофакторна перевірка автентичності або контроль доступу на основі ролей.

Google пропонує різні види двофакторної автентифікації. Окрім традиційного пароля, користувачі можуть ввести одноразовий код безпеки, який вони отримують за допомогою текстового чи голосового дзвінка або створюють у додатку Google Authenticator, який працює на Android та iOS. Користувачі також можуть надати список надійних пристроїв у своєму обліковому записі Google. Якщо користувач спробує увійти з пристрою, якого немає в списку, він отримає попередження безпеки від Google [31].

Google Workspace пропонує ряд функцій відповідності: запобігання втраті даних (DLP), виявлення електронних даних (eDiscovery), а також інструменти аудиту та звітності. Все більше користувачів використовують ці функції, оскільки вони прості та не впливають на продуктивність.

Використовуючи функцію захисту від втрати даних (DLP), ви можете створювати та застосовувати правила, які контролюють вміст файлів, якими співробітники можуть ділитися із зовнішніми користувачами (рис. 2.12). Ця функція дозволяє вказувати, до яких документів та файлів користувачі можуть надавати доступ, а також запобігати ненавмисному розкриттю конфіденційної інформації, наприклад даних кредитних карток або ідентифікаційних номерів.



Рисунок 2.12 – Приклад роботи DLP

Правила DLP запускають сканування файлів на наявність конфіденційного вмісту та за необхідності блокують надання до нього загального доступу. У правилах визначено типи інцидентів DLP, у відповідь на які запускаються дії, наприклад, блокування певного контенту [32].

		Медведенко А.В.			KIK.KP.B – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

DLP дозволяє виконувати такі дії:

- Перевірити використання конфіденційного вмісту на Диску, до якого користувачі вже могли надати доступ, з метою збирання даних про додані ними конфіденційні файли.
- Попереджати кінцевих користувачів про те, що заборонено ділитися конфіденційним вмістом за межами домену.
- Захищати конфіденційні дані (наприклад, номери банківських карток) від доступу зовнішніх користувачів.
- Повідомляти адміністраторів та інших осіб про порушення правил або інцидентів DLP.
- Аналізувати інциденти, використовуючи дані щодо порушення правил.

Захист конфіденційних даних включає різні типи методів, які можна використовувати для перевірки чи перетворення ваших даних. Використовуючи ці різні методи, ви можете перевіряти дані як у Google Cloud, так і поза ним, а також оптимізувати поведінку захисту конфіденційних даних для різних типів робочих навантажень. Захист конфіденційних даних надає такі типи методів: методи змісту, методи зберігання, гібридні методи [33].

Методи змісту є синхронними методами без стану. Дані, які потрібно перевірити або трансформувати, надсилаються безпосередньо в запиті до DLP API. Результати інспекції захисту конфіденційних даних або трансформовані дані повертаються у відповідь API. Дані запиту шифруються під час передавання та не зберігаються (рис. 2.13).

Методи зберігання призначені для перевірки даних, що зберігаються в Google Cloud у режимі Datastore. Щоб увімкнути перевірку сховища, створюється завдання захисту конфіденційних даних за допомогою ресурсу `dlpJobs`. Кожне завдання виконується як керована служба для перевірки даних, а потім виконання дій захисту конфіденційних даних, таких як збереження або публікація результатів. На додаток до цих додаткових дій, захист конфіденційних даних створює та зберігає відомості про завдання, включаючи статус завдання, скановані байти та зведені

		Медведев А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

результати для кожного типу інформації. Користувач може керувати завданнями за допомогою DLP API або захисту конфіденційних даних у консолі Google Cloud (рис. 2.14).

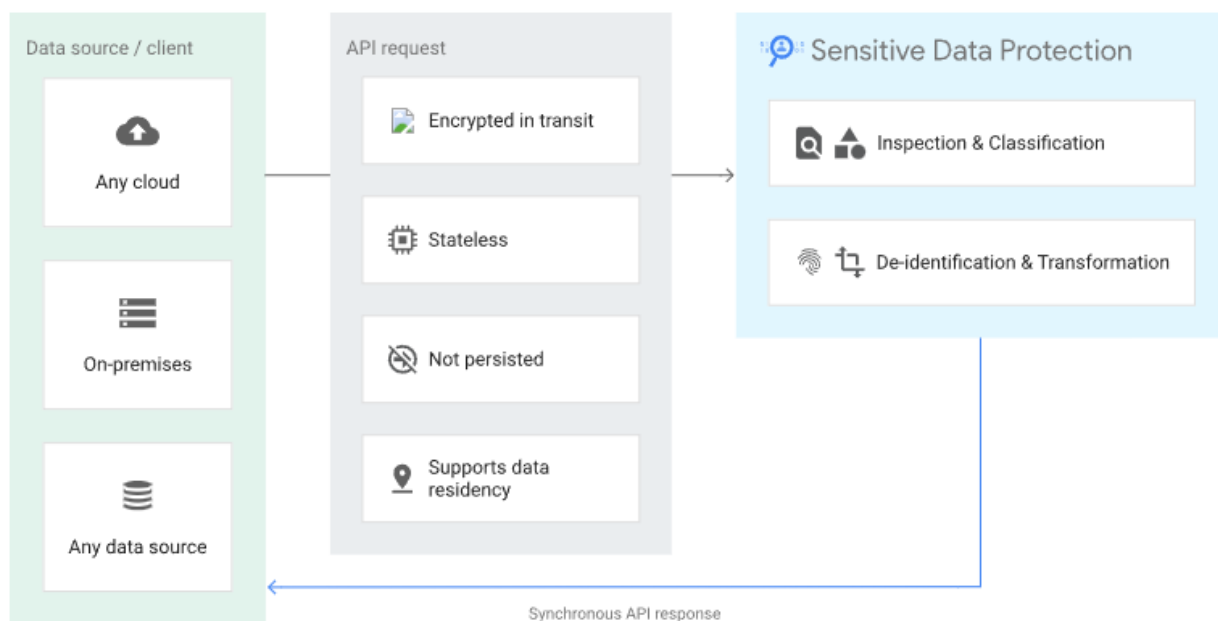


Рисунок 2.13 – Приклад роботи методу змісту

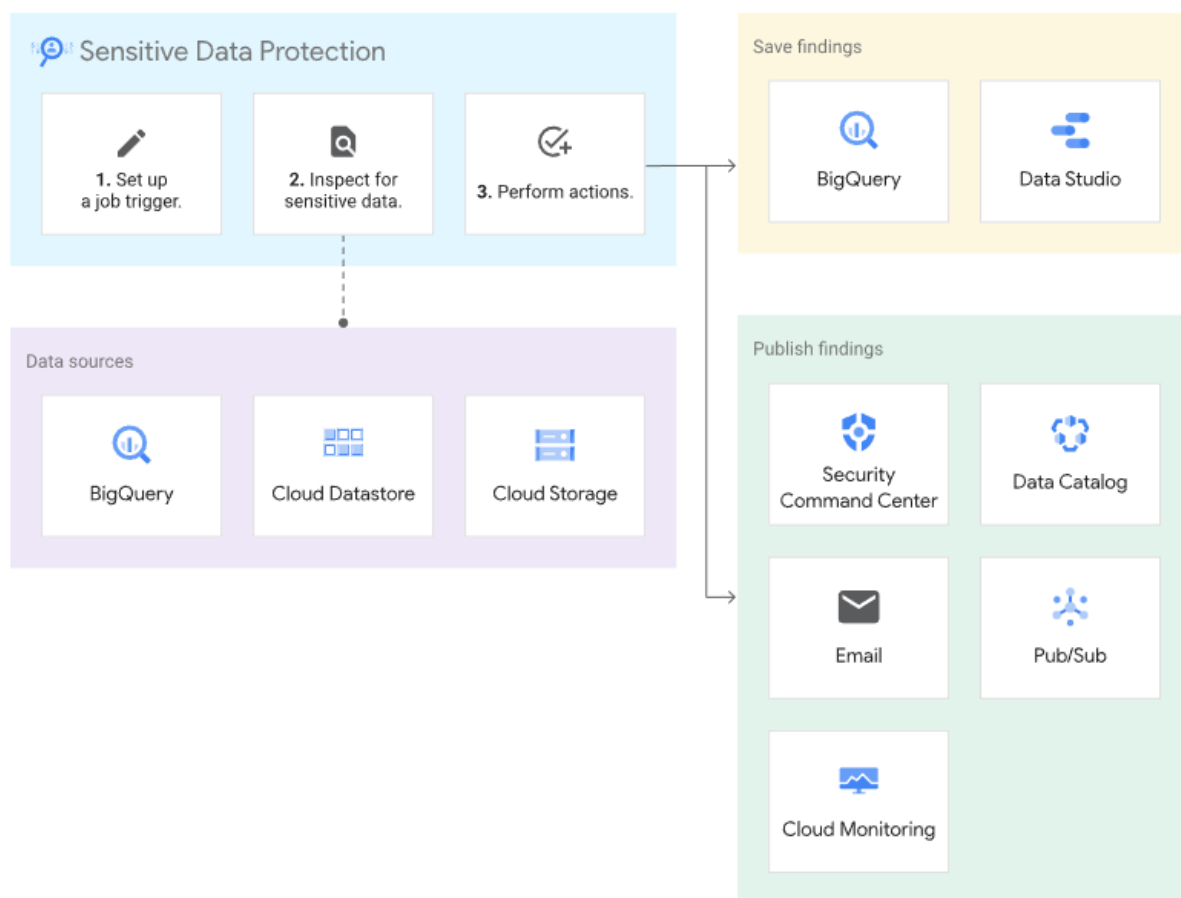


Рисунок 2.14 – Приклад роботи методу зберігання

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

Гібридні методи – це набір асинхронних методів API, які дозволяють сканувати корисні дані, надіслані практично з будь-якого джерела, на предмет конфіденційної інформації та зберігати результати в Google Cloud. Гібридні методи подібні до методів вмісту тим, що дані, які ви хочете перевірити, включені в один або кілька запитів на перевірку; однак, на відміну від методів вмісту, гібридні методи не повертають результати перевірки у відповідь API. Натомість результати перевірки обробляються на стороні сервера асинхронно, а результати зводяться в таблицю та зберігаються у спосіб, подібний до методів зберігання (рис. 2.15).

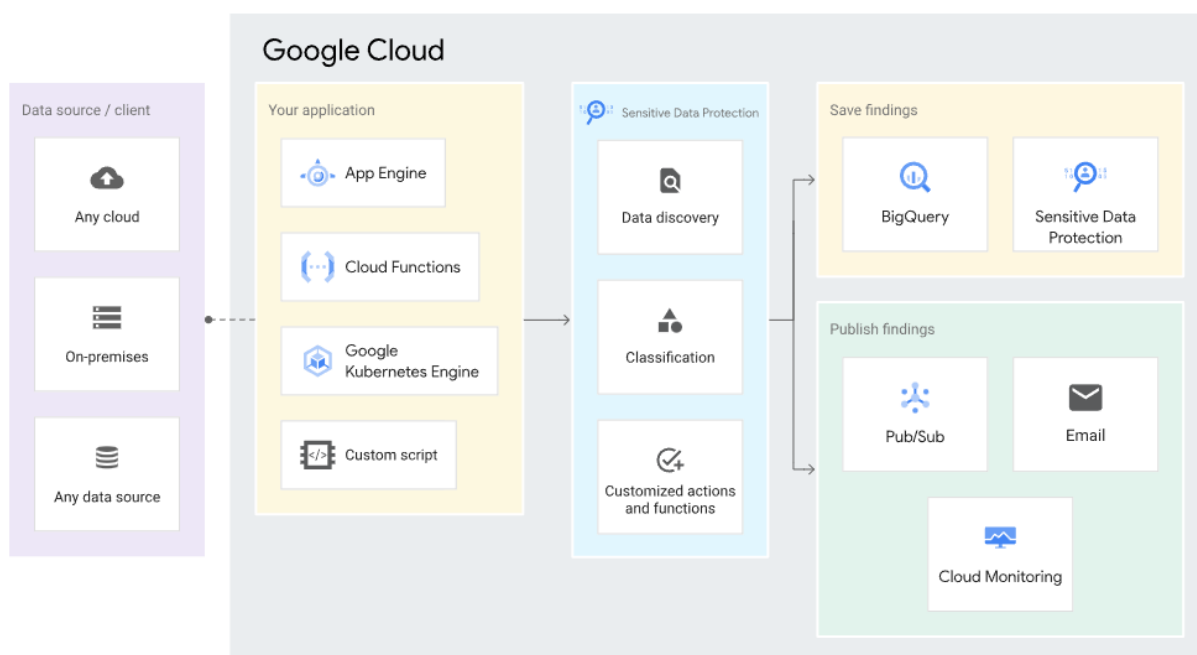


Рисунок 2.15 – Приклад роботи гібридного методу

На консолі адміністратора Google можна використовувати сторінку аудиту та дослідження, щоб переглянути дії користувачів і адміністраторів у організації. Можна використовувати інформацію для відстеження користувачів і адміністраторів, а також з метою безпеки. Можна сортувати, фільтрувати й аналізувати дані для визначення користувачів, які отримали доступ до сайтів, списки, бібліотеки, типи вмісту, елементи списків і файлів бібліотеки в колекції сайтів. Наприклад, можна визначити, який вміст видалено. Інформація про те, хто виконував певні дії з вмістом колекції сайтів, може мати вирішальне значення для

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

виконання організаційних вимог, таких як відповідність законодавству та керування записами.

Підприємству може бути потрібно зберігати або архівувати вміст, включаючи повідомлення електронної пошти, вкладення і документи, протягом певного періоду часу. Для цього може використовуватися Google Vault. Vault – це інструмент керування інформацією для Google Workspace. За допомогою Vault можна зберігати, шукати та експортувати дані користувачів Google Workspace.

2.4 Моделі загроз та порушника

Загрози можуть мати об'єктивну природу або суб'єктивну. Загрози, що мають суб'єктивну природу, можуть бути випадковими або навмисними. Необхідно визначити основні загрози безпеки інформації та врахувати їх у моделі загроз:

- Природні катастрофи, такі як землетруси, повені, пожежі та інші непередбачувані події;
- Непередбачувані ситуації, які можуть призвести до неправильної роботи обладнання та технічних систем автоматизованої системи;
- Технічні недоліки у компонентах системи, таких як технічні засоби, технології обробки інформації, програмне забезпечення, засоби захисту, структури даних тощо;
- Людські помилки, які можуть виникнути під час використання автоматизованої системи;
- Людські помилки, які можуть виникнути під час використання автоматизованої системи.

Випадкові загрози суб'єктивної природи, що виникають внаслідок недбалості, неуважності або незнання, і не мають на меті навмисного завдання шкоди є [34]:

- Дії, що можуть спричинити відмову автоматизованої системи;
- Ненавмисне пошкодження носіїв інформації;
- Неправомірна зміна режимів роботи автоматизованої системи;

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

- Неумисне зараження програмного забезпечення комп'ютерними вірусами;
- Невиконання вимог організаційних заходів захисту документів системи;
- Помилки введення та виведення даних;
- Дії, що можуть призвести до розголошення конфіденційних відомостей;
- Неправомірне використання забороненого програмного забезпечення;
- Наслідки некомпетентного застосування засобів захисту;
- Інші випадкові дії, що можуть впливати на безпеку інформації в системі.

Умисними загрозами суб'єктивного характеру, спрямованими на розгромлення автоматизованої системи або нанесення їй шкоди, а також на отримання несанкціонованого доступу до ресурсів є:

- Порушення фізичної цілісності системи;
- Втручання у режими функціонування системи життєзабезпечення;
- Порушення режимів функціонування системи;
- Використання комп'ютерних вірусів та інших засобів;
- Використання засобів перехоплення електромагнітних випромінювань;
- Зловживання персоналом системи з корисливою метою;
- Крадіжки носіїв інформації та виробничих відходів;
- Несанкціоноване копіювання інформації;
- Неправомірне підключення та перехоплення даних;
- Використання забороненого програмного забезпечення.

У таблиці А.1 (додаток А) визначено перелік можливих загроз і проведено класифікацію впливу загроз на інформацію, а саме визначено вид загрози, її ймовірність, що саме вона порушує, який рівень шкоди має кожна загроза та її джерело. Ця класифікація є важливою для розуміння того, які саме загрози можуть виникнути і як вони можуть вплинути на інформацію.

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

Така класифікація є основою для розробки заходів щодо захисту інформації від загроз, тому що кожна загроза може призвести до витоку, порушення цілісності або блокування інформації.

У кожному конкретному випадку, виходячи з технології обробки інформації, необхідно розробити модель порушника. Модель порушника – абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апіорні знання, час та місце дії та інші [35]. Порушники можуть бути внутрішніми (співробітники, користувачі) або зовнішні (сторонні особи).

Модель порушника має визначати: категорії осіб, з числа яких може бути порушник, рівень можливостей порушника, припущення про кваліфікацію та можливий рівень знань порушника, методи і способи, що використовуються при здійсненні порушень, можливу мету порушника, можливі місця здійснення порушень, припущення про характер його дій. Можливою метою порушника може бути здійснення спроб несанкціонованого доступу до ресурсів, установка програмних та фізичних засобів для модифікації даних або їх викрадення, установка програмних засобів (програмних закладок чи вірусів) для модифікації, зміна режимів функціонування системи, тощо.

Порушники діляться на чотири категорії за рівнем своїх можливостей. Перший рівень – можливість запуску фіксованого набору завдань, що реалізують заздалегідь передбачені функції обробки інформації. Другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації. Третій рівень визначається можливістю управління функціонуванням системи, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування. Четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів.

Також потрібно розглянути профілі захищеності, що реалізують різні компоненти Google Workspace Enterprise. Поділ критерій оцінки інформації наведено на рисунку 2.16 [36].

		Медведев А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

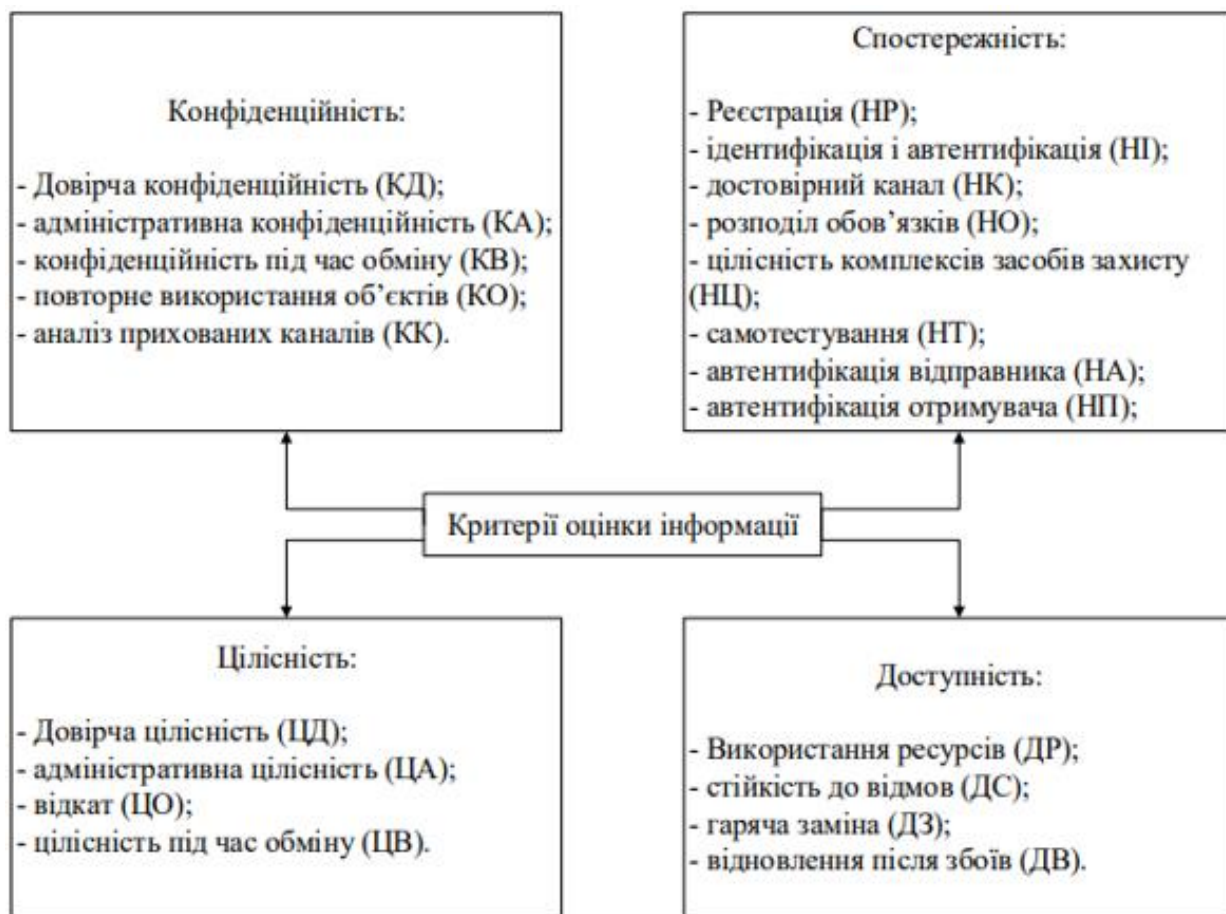


Рисунок 2.16 - Критерії оцінки інформації

Таблиця 2.3

Профілі захищеності, що реалізують різні компоненти Google Workspace Enterprise

Компоненти	Критерії конфіденційності
Gmail	КД-2, КА-2, КВ-2, ЦД-1, ЦО-2, ДР-2, ДС-2, ДВ-2, НР-3, НИ-3, НО-2, НЦ-1
Google Sites	КД-2, КА-2, КВ-2, ЦД-1, ЦА-1, ЦО-2, ДР-2, ДС-2, ДВ-2, НР-2, НИ-3, НО-3, НЦ-1
Google Диск	КД-2, КА-2, КВ-2, ЦД-1, ЦА-1, ЦО-2, ДР-2, ДС-2, ДВ-2, НР-1, НИ-3, НО-2, НЦ-1
Google Документи	КД-2, КА-2, КВ-2, ЦО-1, ДЗ-1, ДВ-2, НР-2, НИ-3, НО-1, НЦ-1
Google Meet	КД-2, КА-2, КВ-2, ЦД-1, ДС-2, ДВ-2, НР-1, НИ-3, НО-2, НЦ-1, НВ1
Google Chat	КД-2, КА-2, КВ-2, ЦД-1, ДС-2, ДВ-2, НР-1, НИ-3, НО-2, НЦ-1, НВ1

Висновки до розділу 2

У цьому розділі було досліджено такі хмарні сервіси як ClickUp, Wrike, Asana, Google Workspace, визначено переваги і недоліки кожного з них та обрано найкращий варіант.

Було досліджено які сервіси та послуги надає користувачам Google Workspace. Було розглянуто безпеку даних Google на рівні користувача та на рівні центру обробки даних.

Побудовано модель загроз підприємства та модель загроз порушника. Було розглянуто профілі захищеності, що реалізують різні компоненти Google Workspace Enterprise.

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 РОЗГОРТАННЯ ТА НАЛАШТУВАННЯ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ НА БАЗІ ХМАРНОГО СЕРВІСУ GOOGLE WORKSPACE

3.1 Дослідження системи захисту існуючої інформаційної інфраструктури

Розглянута при виконанні дипломної роботи організація використовувала хмарний сервіс під назвою Zoho Workplace. Це комплексне рішення для бізнесу, яке включає в себе різноманітні інструменти для спільної роботи, електронної пошти, керування проектами, відеоконференцій та інше.

Проте вказаний сервіс має і ряд недоліків:

1. Вузкий набір додатків та розширень.

Хоча Zoho і пропонує ряд інструментів в ньому значно менше додатків та інтеграцій для певних продуктів. А через відсутність широкої екосистеми важко знайти адекватне поєднання з іншими платформами та інструментами.

2. Низька частота оновлень.

Оновлення та нові функції у Zoho випускаються менш часто у порівнянні з іншими конкурентами, що сильно впливає на доступність новітніх можливостей.

3. Недоліки безпеки.

Якщо вищезгадані недоліки не такі критичні, то найважливішими є недоліки систем безпеки:

- У Zoho Workplace відсутня двофакторна аутентифікація для всіх користувачів. Тобто Zoho Workplace надає 2FA для деяких користувачів, але вона не є обов'язковою для всіх. Це означає, що користувачі можуть увійти в систему, просто ввівши свій пароль, і це є серйозний недоліком безпеки, оскільки робить облікові записи користувачів більш уразливими для хакерських атак. Відомі непоодинокі випадки, коли зловмисники раз отримували доступ до облікового запису користувача-співробітника організації, який не використовував 2FA і, відповідно, частина була скомпрометована та/або знищена чутлива інформація, така як фінансові звіти, плани маркетингу та конфіденційна інформація про контрагентів/клієнтів компанії. Також є інформація випадок, коли порушник

		Медведев А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

використав незахищений обліковий запис користувача та поширив у мережі шкідливе програмне забезпечення. Це призвело до збою операційних систем деяких користувачів, які не змогли працювати та втратили частину своїх конфіденційних даних, включаючи імена, адреси, номери телефонів та електронні адреси. Відповідно організацією було витрачено значні кошти на відновлення даних та заходи з очищення мережі від шкідливого ПЗ.

- У Zoho Workplace відсутній захист від витоку даних. Так один з працівників випадково оприлюднив конфіденційний документ у загальнодоступному каталозі через свою помилку, так як нічого цьому не завадило. Документ містив інформацію про рахунки компанії, і хоча цей інцидент було швидко виявлено та вирішено, дані вже потрапили до порушників які викрали певну суму з рахунку компанії. Через це компанія була змушена провести аудит своїх політик безпеки, що призвело до непланових витрат.

- Часто зустрічається проблема з некоректним контролем доступу до інформації при використанні Zoho Workplace. При звільненні нелояльний працівник не повернув ноутбук компанії. За допомогою контролю доступом у нього забрали всі уповноваження та доступи. Але ця система дала збій і він все ще мав доступ до усіх ресурсів. Він викрадав особисті дані співробітників компанії, включаючи їхні імена, адреси, номери телефонів та електронні адреси, які згодом передав третім особам, що призвело до загрози іншим співробітникам.

Отже, хоча хмарний сервіс Zoho Workplace і надає базовий захист від зловмисного програмного забезпечення, який включає в себе фільтрацію вмісту, виявлення шкідливих посилань та блокування шкідливих файлів, цей захист не є достатнім для захисту від сучасних загроз, таких як фішинг, зловмисні додатки та розширені стійкі загрози. Тому керівництвом компанії було вирішено змінити Zoho Workplace на інший хмарний сервіс. В результаті аналізу, наведеного у розділі 2, було обрано сервіс Google Workspace.

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

3.2 Розгортання хмарного сервісу Google Workspace

Розглянемо, які кроки потрібно виконати, щоб налаштувати Google Workspace. Щоб почати потрібно створити власний обліковий запис Google Workspace. Це запустить майстер налаштування облікового запису, який запропонує надати інформацію про назву, кількість працівників та країну (рис.3.1).

Google Workspace

Почнімо!

Назва компанії
Medvedenko

Кількість співробітників, включно з вами

☐ Лише ви

☐ 2–9

☐ 10–99

☐ 100–299

☐ 300+

Регіон*
Україна

Далі

Працюйте віддалено з максимальною ефективністю

З Google Meet можна проводити безпечні відеозустрічі у високій якості просто з поштової скриньки або календаря

Робіть більше з Google Workspace

- ✓ Персоналізована електронна адреса з вашим доменним ім'ям
- ✓ Робота в хмарі без необхідності встановлювати додаткове ПЗ
- ✓ Розширені функції адміністрування й безпеки
- ✓ Цілодобова підтримка без вихідних
- ✓ Безкоштовне користування протягом 14 днів; потім плата стягуватиметься щомісяця

Рисунок 3.1 – Базова інформація

Наступним кроком потрібно буде ввести інформацію про свій обліковий запис адміністратора Google Workspace (рис.3.2).

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

Укажіть контактну інформацію

Коли ви створюєте обліковий запис Google Workspace, то автоматично стаєте його адміністратором. ?

Ім'я

Андрій

Прізвище

Медведенко

Поточна електронна адреса

medvedenko.andrii3@gmail.com

Далі

Рисунок 3.2 – Інформацію про обліковий запис адміністратора

Після того як ми ввели інформацію про обліковий запис адміністратора, потрібно вказати, чи має компанія вже доменне ім'я. Якщо уже є веб-сайт, то потрібно вибрати «Так, у мене є один, яким я можу скористатися» (рис.3.3).

У вашої компанії є домен?

Щоб налаштувати для компанії електронну адресу й обліковий запис Google Workspace, потрібно мати домен на зразок *example.com*. ?

Так, у мене є домен, який можна використовувати

Ні, мені потрібен домен

Використати цей домен, щоб налаштувати обліковий запис?

med.ua Ваш домен

Це не вплине на листи, надіслані в домен **med.ua**, доки ви не налаштуєте електронну пошту для цього облікового запису.

Далі

Я хочу придбати новий домен

Рисунок 3.3 – Інформацію про домен

Потім потрібно ввести ім'я користувача та пароль, які використовуватимуться для входу в Google Workspace (рис.3.4). За замовчуванням

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

ім'я користувача буде корпоративною адресою електронної пошти (тобто username@yourdomain.com), тому потрібно мати це на увазі, вибираючи, яке ім'я користувача використовувати.

Як увійти в систему

За допомогою імені користувача ви зможете увійти в обліковий запис Google Workspace і створити корпоративну електронну адресу. ?

Ім'я користувача

andrii.medvedenko

@med.ua

17 / 64

Пароль

.....

👁

14 / 100

Ми здогадуємося, що ви не робот, але маємо запитати.
Ви робот?



Натискаючи **Прийняти та продовжити**, ви погоджуєтеся виконувати такі правила: [Google Workspace Agreement](#) і [Supplemental Terms and Conditions for Google Workspace Free Trial Agreement](#).

Прийняти та продовжити

Рисунок 3.4 – Інформацію про користувача

На цьому етапі розгортання хмарного сервісу Google Workspace завершується і можна переходити до налаштування необхідних служб та розширених систем безпеки.

3.3 Впровадження системи безпеки підвищеної захищеності

Google пропонує власні елементи керування безпекою в Google Workspace і вмикає деякі рекомендовані параметри безпеки за умовчанням, але працює за моделлю спільної відповідальності. Це означає, що користувач несе

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

відповідальність за впровадження політик і процедур, таких як контроль доступу та дозволи. Google Workspace має вбудовані надійні функції безпеки, які надають адміністраторам контроль і видимість, необхідні для прийняття обґрунтованих і відповідних рішень для організації.

Потрібно увімкнути багатофакторну автентифікацію (MFA). MFA — це захід безпеки, який вимагає від користувачів надавати більше, ніж просто пароль для доступу до своїх облікових записів. Це може бути у формі маркера безпеки, відбитка пальця або іншої форми підтвердження. Увімкнення MFA може допомогти запобігти несанкціонованому доступу до даних організації. Щоб увімкнути MFA у Google Workspace, треба перейти до панелі двоетапної перевірки на панелі адміністратора Google Workspace і встановити прапорець «Дозволити користувачам увімкнути двоетапну перевірку». У розділі Enforcement потрібно вибрати «On» або «On from <Date>» відповідно. У розділі «Методи» обираємо варіант, який підходить (рис.3.5).

Рисунок 3.5 – Встановлення двоетапної перевірки

Це дозволить організації захистити акаунти своїх співробітників, щоб зловмисники не змогли отримати доступ до незахищених облікових записів і конфіденційних даних.

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

Увімкнути захист від втрати даних (DLP) DLP — це засіб безпеки, який допомагає запобігти випадковому чи навмисному витоку конфіденційних даних. Google Workspace містить функцію DLP, за допомогою якої можна ідентифікувати та захищати конфіденційні дані. Щоб увімкнути DLP у Google Workspace потрібно увійти до консолі адміністратора Google ввімкнути параметр Сканування даних і звітування (рис.3.6).

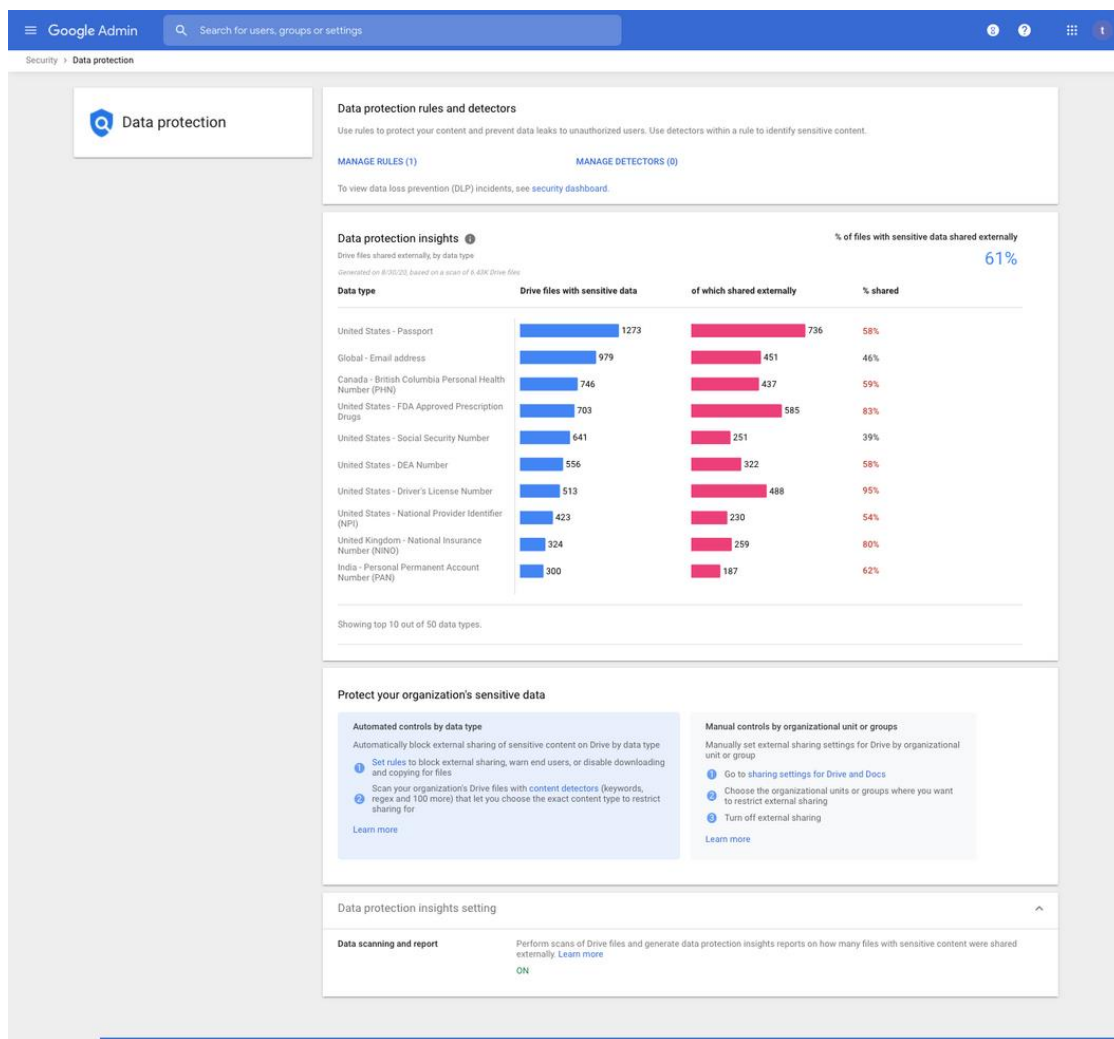


Рисунок 3.6 – Сканування даних і звітування

Далі потрібно створити власні правила, визначити область сканування, тригери подій, встановити умови і визначити відповідні дії. Розглянемо один з прикладів створення правила. Потрібно увійти у консоль адміністратора та натиснути “Створити нове правило” (рис.3.7).

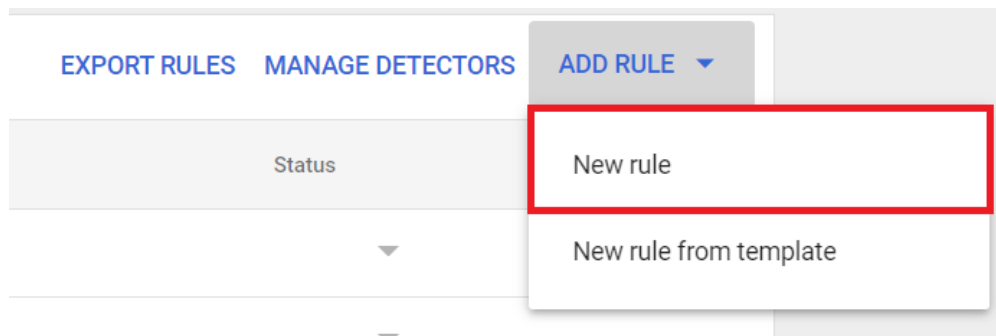


Рисунок 3.7 – Створення правила

Наступною дією потрібно додати назву, опис та вибрати область дії правила (рис.3.8).

Name Your rule name will appear in your policies.

Name*

Credit card numbers

Description

Block external sharing

Scope Choose your rule's scope.

☒ Apply to all [Tricent Security Group]

☐ Apply to organizational units and/or groups

Include organizational units +

Exclude organizational units +

Include groups +

Exclude groups +

Рисунок 3.8 – Назва, опис та область дії правила

Після того як усе буде обрано потрібно поставити прапорець у полі “File modified”, вибрати весь контент та обрати “Global - Credit card number” (рис.3.9).

Triggers Select the events that trigger your rule.

Google Drive

☒ File modified

Conditions
Set conditions to define sensitive content.

All content

Matches default dete ...

Minimum match count
1

ADD CONDITION

Global - Credit card number

Global - Date

Global - Date of Birth

Global - Domain Name

Global - Email Address

Minimum unique matches
1

Рисунок 3.9 – Налаштування правила

Коли всі потрібно дані будуть заповнені, потрібно зробити правило активним, активувавши відповідний прапорець (рис.3.10).

Create rule

Select the status for your rule. You can change this anytime.

☒ **Active**
Selected actions (if any) will be enforced, and logs will be collected when the rule is triggered.

☐ **Inactive**
Selected actions won't be enforced, and logs won't be collected.

CANCEL COMPLETE

Рисунок 3.10 – Активація правила

Якщо працівник навіть випадково спробує оприлюднити конфіденційні дані, то система Google Workspace просто не дасть цього зробити і просто заблокує цю спробу, тим самим захистивши дані.

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

Також не буде зайвим увімкнути елементи контролю доступу. Контроль доступу – це заходи безпеки, які визначають, хто має доступ до певних ресурсів у вашій організації. Google Workspace містить низку елементів керування доступом, за допомогою яких можна обмежити доступ до конфіденційних даних. Щоб увімкнути керування доступом у Google Workspace потрібно перейти у вкладку “Керування доступом” та створити нову роль (рис.3.11).

Рисунок 3.11 – Створення нової ролі

Наступним кроком потрібно надати їй привілеї які потрібні для цієї ролі (рис.3.12).

Рисунок 3.12 – Надання привілеїв

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

Функція DLP надасть змогу контролювати повноваження кожного користувача. І навіть якщо співробітник забере корпоративний ноутбук з собою після звільнення, він не зможе отримати доступ ні до яких даних. Так як Google використовує нові системи безпеки і завжди оновлюється, шанс на те що трапиться майже відсутній.

Також необхідно увімкнути розширений захист від зловмисного програмного забезпечення: завдяки моделям машинного навчання Google постійно вдосконалює здатність виявляти фішингові та інші атаки зловмисного програмного забезпечення та реагувати на них. Розширений захист від зловмисного програмного забезпечення забезпечує додаткові функції безпеки, такі як сканування зображень у посиланнях для захисту від зловмисного програмного забезпечення та визначення посилань за короткими URL-адресами для захисту від фішингу. Так як ця система базується на машинному навчанні, то зможе розпізнати навіть найновіші види загроз та попередити про них. Це стосується навіть нових загроз про які ще ніхто не знає.

Важливим пунктом є обмеження параметрів спільного доступу. Це збереже спільний доступ до файлів у своїх доменах, щоб запобігти витоку даних і викраданню. Також можна вимкнути спільний доступ за посиланням для нових файлів і попередити користувачів, коли вони збираються поділитися файлом за межами вашого домену.

Необхідно встановити розширення Password Alert. Google пропонує розширення для веб-переглядача Chrome, яке може допомогти захистити паролі. Розширення Password Alert розроблено, щоб запобігти фішингу/підробці. По суті, розширення надішле сповіщення, якщо користувач спробує використати пароль свого облікового запису Google на веб-сайті, що не належить Google. Так паролі будуть ще більш надійно захищені і навіть неуважний співробітник не віддасть свій пароль до рук зловмисників.

І також на даному етапі увімкнемо функцію Mobile Management Solution. Ця функція дозволяє адміністраторам налаштовувати елементи керування безпекою для будь-яких пристроїв, які мають доступ до їхнього середовища, не потребуючи, щоб їхні працівники встановлювали додаткові програми на свої пристрої. Щоб її

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

активувати потрібно перейти в панель адміністратора та ввімкнути “Advanced” (рис.3.13).

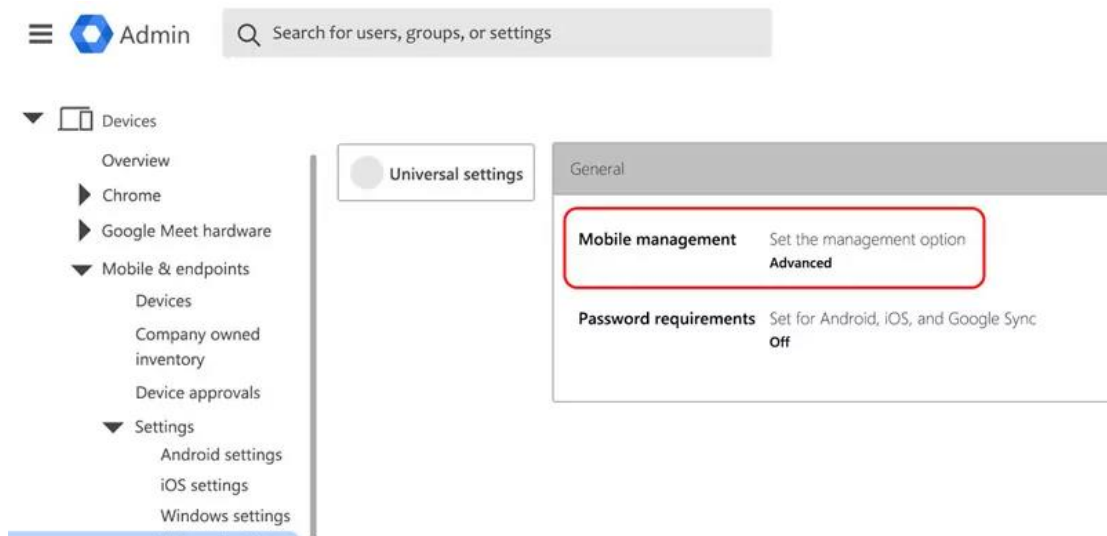


Рисунок 3.13 – Активація Mobile Management Solution

Коли ми ввімкнули опцію “Advanced” потрібно зареєструвати пристрої. Це дасть можливість переглядати деталі пристрою, типи та користувачів пристрою. Потрібно ввести всі дані про пристрій та імпортувати його (рис.3.14).

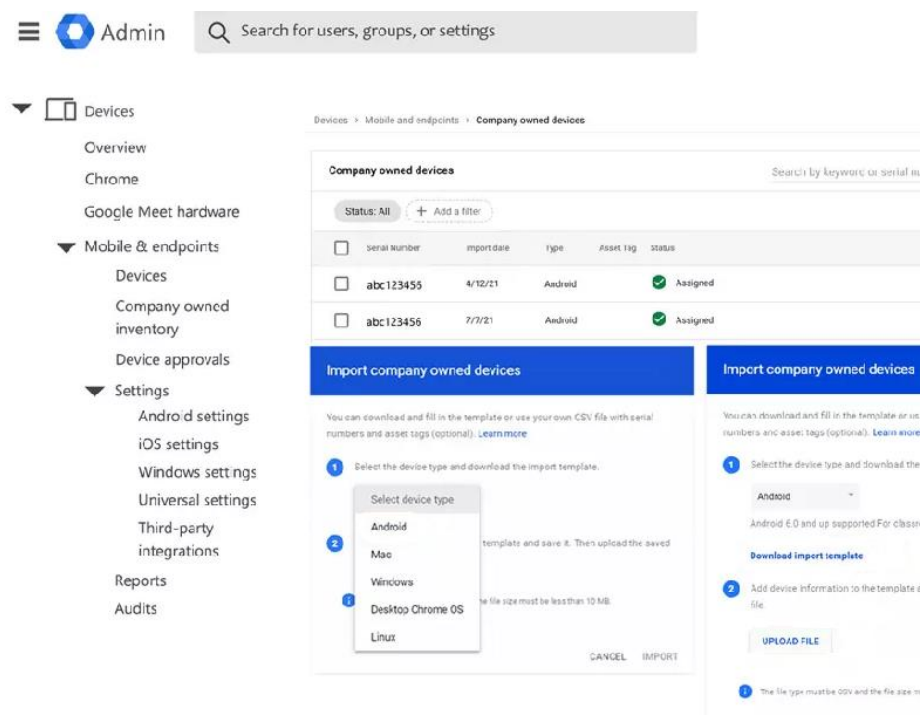


Рисунок 3.14 – Реєстрація нового пристрою

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

За допомогою цього можна слідкувати щоб недоброчесні співробітники не віддали конфіденційні дані та хакери не отримали до них доступ. Або просто захистити пристрої працівників від хакерських атак, а у разі чого одразу їх відключити.

На цьому етапі було завершено налаштування підвищеної захищеності хмарного сервісу Google Workspace, і можна переходити до процесу перенесення даних з Zoho Workplace.

3.4 Перенесення існуючої інфраструктури в Google Workspace

За допомогою Google Workspace Migrate можна перенести великий обсяг даних до домену Google Workspace. Цей інструмент дозволяє централізовано керувати масштабними перенесеннями даних до основних сервісів Google Workspace.

Google Workspace Migrate є простим у використанні інструментом, який не вимагає від адміністраторів ІТ-систем спеціальних знань або навичок, дає можливість мігрувати дані швидко та ефективно, мінімізуючи час простою для організації та використовує сучасні технології безпеки для захисту даних під час міграції.

Запустити Google Workspace Migrate можна як у хмарному, так і локальному середовищі. Цей інструмент працює окремо на базі керованого програмного забезпечення, і адміністратори можуть контролювати, коли і куди виконати перенесення.

Всі дані залишаються у мережі організації. Зберігається за собою право власності на дані, що перенесені в Google Workspace. Google Workspace Migrate – рішення для корпоративних клієнтів, яке підходить для роботи з великими обсягами даних та складною інфраструктурою. Перенести корпоративні дані можна з джерел наведених у таблиці 3.1.

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

Джерела з яких можна імпортувати дані

Обліковий запис	Дані, які можна перенести	Примітки
Exchange Online (Microsoft 365) Exchange 2016 Exchange 2013 Exchange 2010 Exchange 2007	Електронна пошта Контакти Заходи календаря Ресурси календаря	За одну операцію можна перенести електронну пошту, контакти чи календарі, але не кілька типів даних одночасно. Їх потрібно переносити лише окремо.
Exchange 2003 або раніше Поштові служби IMAP, такі як 1&1 IONOS, AOL, Apple iCloud, Bluehost, Yahoo! або Zoho Інший обліковий запис Google Workspace Особистий обліковий запис Gmail (@gmail.com) Інші IMAP-сервери	Електронна пошта	
Сервер HCL (раніше IBM) Domino	Електронна пошта	Сервіс перенесення даних дозволяє перенести дані електронної пошти з HCL Notes у Google Workspace

В першу чергу потрібно обирати пункт “Data migration” на панелі адміністратора (рис.3.15).

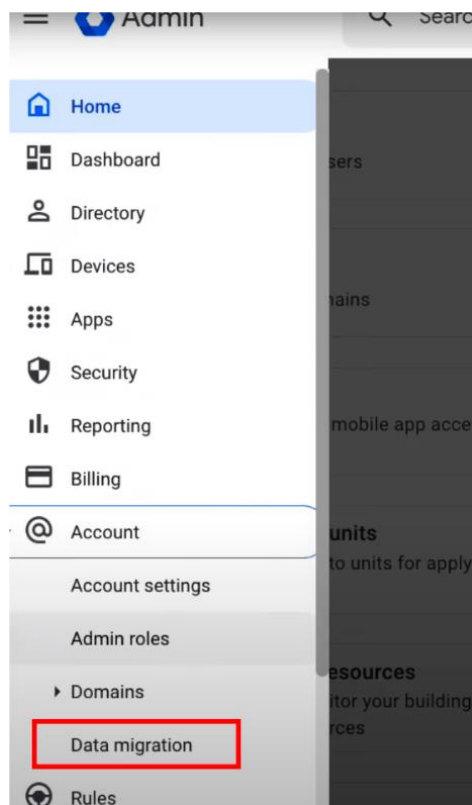


Рисунок 3.15 – Data migration

Після чого з'являється вікно з налаштуваннями переносу даних, де потрібно обрати джерело звідки дані будуть переноситися та сам тип даних (рис.3.16).

 A screenshot of a configuration window titled 'Configure Data Migration Service'. It has two tabs: '1 Source Connection Settings' (active) and '2 Additional Migration Settings'. The main content area is titled 'Configure your source connection settings. Learn More'. It contains three sections: 'Migration Source' with a dropdown menu 'Select a Migration Source*', 'Select the type of items to migrate from your source server.' with a dropdown menu 'Select a Data Type*', and 'Connection Protocol' with a dropdown menu 'Auto Select (Recommended)'.

Рисунок 3.16 – Налаштування переносу

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

Коли джерело звідки дані будуть переноситися та сам тип даних обрано, переходимо до наступного кроку, де потрібно обрати за який проміжок переносити дані та додаткові опції, такі як видалені листи наприклад (рис.3.17).

Рисунок 3.17 – Вибір дати та додаткові налаштування

Наступною дією потрібно обрати користувачів, чиї дані будуть переноситися. Для цього потрібно ввести електронну пошту користувача з якої буде відбуватися перенос, його пароль та безпосередньо саму пошту Google Workspace (рис.3.18).

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

Start a Migration

1. Enter the resource name of the resource to migrate data from.
2. Select the resource to migrate to.
3. Click START to start the migration.

Source Email

Password

Google Workspace Email

CANCEL START

Рисунок 3.18 – Додавання користувача

Після того як усі попередні кроки будуть виконані, автоматично розпочнеться процес переносу даних.

На цьому процес переходу на хмарний сервіс Google Workspace завершено.

Висновки до розділу 3

У цьому розділі було описано чому компанія вирішила перейти з хмарного сервіса Zoho Workplace на Google Workspace.

Покроково показано як налаштовувати Google Workspace для нових користувачів.

Розглянуто та налаштовано необхідні системи безпеки для захисту інформації, щоб захистити всі конфіденційні дані від витоку.

Показано як переносити дані користувачів з інших хмарних сервісів до Google Workspace.

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

В ході виконання кваліфікаційної роботи було розглянуто сучасні хмарно-орієнтовані технології, різні моделі хмарних сервісів, досліджено принципи роботи хмарних сервісів, їх переваги та недоліки.

Досліджено, що впровадження хмарних технологій дозволяє відмовитися від застарілого локального інфраструктурного підходу до запуску сервісів у сфері інформаційно-комунікаційних технологій, який занадто дорогий та складний в обслуговуванні для не таких великих організацій.

Описано архітектуру хмарних сервісів, виявлено актуальність використання хмарних технологій, а також розглянуто певні загрози, пов'язані з ними.

Досліджено такі хмарні сервіси як ClickUp, Wrike, Asana, Google Workspace, визначено функціонал, переваги і недоліки кожного з них. За допомогою отриманої інформації та проведених досліджень було обрано систему Google Workspace, через її перевагу над іншими.

В ході дослідження було описано які сервіси та послуги надає користувачам Google Workspace. Було розглянуто безпеку даних Google на рівні користувача та на рівні центру обробки даних. Детально розібрано наявні системи безпеки які забезпечать захист організації, користувачів та даних.

Побудовано модель загроз підприємства та модель загроз порушника, які є потенційно небезпечними для організацій. Було розглянуто профілі захищеності, що реалізують різні компоненти Google Workspace Enterprise.

Детально описано всі недоліки попередньої хмарної системи, які потрібно усунути. Визначено які елементи безпеки були найбільш вразливими, щоб майбутня система могла їх усунути.

Покроково показано як налаштовувати Google Workspace для нових користувачів.

Налаштовано необхідні системи безпеки для захисту інформації, щоб захистити всі конфіденційні дані від витоку, такі як: багатофакторна автентифікація, захист від втрати даних, елементи контролю доступу, розширений захист від зловмисного програмного забезпечення, налаштовано параметри

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

спільного доступу, ввімкнено розширення Password Alert та функцію Mobile Management Solution.

Перенесено всі дані користувачів з Zoho Workplace до Google Workspace з використанням Google Migrate, через що процес пройшов швидко і без можливості втратити дані при перенесенні.

В результаті виконаних маніпуляцій отримали систему, яка буде захищена від атак зловмисників, буде коректно функціонувати, буде швидко отримувати найновіші оновлення та буде простою і інтуїтивно зрозумілою у використанні.

Зважаючи на все вище сказане, можна вважати мету кваліфікаційної роботи успішно досягнутою.

		Медведев А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Integrity Systems. (2020). Приватне хмарне рішення. [Електронний ресурс]. Режим доступу: <http://integritysys.com.ua/solutions/pricatecloud-solution/> – Дата звернення: 12.11.2023
2. Microsoft. (2023, 12, 16). Архітектура мейнфреймів та середньорозмірних систем в Azure. [Електронний ресурс]. Режим доступу: <https://learn.microsoft.com/ru-ru/azure/architecture/mainframe/mainframe-midrange-architecture>: <https://learn.microsoft.com/ru-ru/azure/architecture/mainframe/mainframe-midrange-architecture> – Дата звернення: 10.11.2023
3. Грід обчислення. [Електронний ресурс]. – Режим доступу: https://wiki.cuspu.edu.ua/index.php/%D0%93%D1%80%D1%96%D0%B4_%D0%BE%D0%B1%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F. – Дата звернення: 1.12.2023
4. Хмарні обчислення. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Хмарні_обчислення: https://uk.wikipedia.org/wiki/Хмарні_обчислення. – Дата звернення: 15.11.2023
5. Що таке приватна хмара та в чому її відмінність від публічної. [Електронний ресурс]. – Режим доступу: <https://gigacloud.ua/blog/navchannja/scho-take-privatna-hmara-ta-v-chomu-ii-vidminnist-vid-publichnoi>: – Дата звернення: 18.11.2023.
6. Публічна хмара: що це таке і чим вона відрізняється від приватної та гібридної / Колобридж Україна // Blog.colobridge.net. - Київ, 2023. - Електронний ресурс. - URL: <https://blog.colobridge.net/uk/2023/09/public-cloud-ua/>. - 2023-09-20
7. Що таке хмарна технологія і навіщо вони потрібні. [Електронний ресурс]. – Режим доступу: <https://edin.ua/shho-take-xmarni-texnologi%D1%97-i-navishho-voni-potribni/> : – Дата звернення: 17.11.2023.
8. Азізова Н. Інфраструктура як послуга (IaaS) [Електронний ресурс] // Wikidata.uk-ua.nina.az. – 2023. – Режим доступу: <https://www.wikidata.uk-ua.nina.az/IaaS.html>. – Дата звернення: 29.11.2023.

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

9. Що таке SaaS та PaaS: основні принципи та відмінності. [Електронний ресурс]. – Режим доступу: <https://igrm.org.ua/shho-take-saas-ta-paas-osnovni-principi-ta-vidminnosti.html>: – Дата звернення: 17.11.2023

10. Компанія "Бізнес-Технології Онлайн". Що таке SaaS? [Електронний ресурс]. – Режим доступу: <https://cbto.com.ua/library/saas>. – Дата звернення: 25.11.2023

11. Що таке ClickUp і для чого він використовується? [Електронний ресурс]. – Режим доступу: <https://clickup.com/blog/what-is-clickup-used-for/#:~:text=ClickUp%20is%20an%20all%2Din,ClickUp%20was%20built%20for%20this> – Дата звернення: 21.11.2023

12. ClickUp Pricing. [Електронний ресурс]. – Режим доступу: <https://clickup.com/pricing> – Дата звернення: 21.11.2023

13. Wrike. [Електронний ресурс]. – Режим доступу: <https://www.wrike.com/> – Дата звернення: 22.11.2023

14. Wrike Price. [Електронний ресурс]. – Режим доступу: <https://www.wrike.com/price/> – Дата звернення: 22.11.2023

15. Що таке Asana як інструмент управління проєктами? Все, що вам потрібно знати [Електронний ресурс]. – Режим доступу: <https://www.simplilearn.com/tutorials/asana-tutorial/what-is-asana-project-management-tool>: <https://www.simplilearn.com/tutorials/asana-tutorial/what-is-asana-project-management-tool> – Дата звернення: 23.11.2023

16. Asana Price. [Електронний ресурс]. – Режим доступу: <https://asana.com/pricing> – Дата звернення: 23.11.2023

17. Google. Ціни на Google Workspace. 2023-12-16. [Електронний ресурс]. Режим доступу: <https://workspace.google.com/pricing.html> – Дата звернення: 24.11.2023

18. Що таке MFA: багатофакторна аутентифікація [Електронний ресурс]. Режим доступу: <https://datami.ua/shho-take-mfa-bagatofaktorna-autentifikatsiya/> – Дата звернення: 02.12.2023

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

19. Require a secure connection for email. [Електронний ресурс]. Режим доступу: <https://support.google.com/a/answer/2520500?hl=en> – Дата звернення: 05.12.2023
20. User log events. [Електронний ресурс]. Режим доступу: <https://support.google.com/a/answer/4580120?hl=en> – Дата звернення: 05.12.2023
21. Google Cloud. (2023). Безпека та відповідність вимогам ISO 27001. [Електронний ресурс]. Режим доступу: <https://cloud.google.com/security/compliance/iso-27001> - Дата звернення: 05.12.2023
22. Google data centers [Електронний ресурс] / Google. Режим доступу: https://en.wikipedia.org/wiki/Google_data_centers. Дата звернення: 05.12.2023
23. What is Google Cloud Platform. [Електронний ресурс]. Режим доступу: <https://www.pluralsight.com/resources/blog/cloud/what-is-google-cloud-platform-gcp> - Дата звернення: 06.12.2023
24. Google Cloud Platform. Terms of Service. [Електронний ресурс] / Google LLC. – Google Cloud Platform. – 2023. – 08. [15]. – URL: <https://cloud.google.com/terms/data-processing-addendum/index-20230815>
25. Дані клієнта (визначення). [Електронний ресурс]. Режим доступу: <https://support.google.com/google-ads/answer/9004362?hl=uk> - Дата звернення: 07.12.2023
26. Google. Архітектура та фреймворк безпеки Google Cloud [Електронний ресурс] / Google. – Google Cloud. – 2022. – Режим доступу: <https://cloud.google.com/architecture/framework/security/network-security>
27. Довіра в G Suite [Електронний ресурс] / [Google]. – Режим доступу: <https://cloud.google.com/files/gsuite-trust-whitepaper.pdf>. – Дата звернення: 07.12.2023
28. Google Cloud. Як Google Cloud заблокував найбільший DDoS-атаку на рівні 7 із 46 мільйонів RPS. [Електронний ресурс]. Режим доступу: <https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps> - Дата звернення: 08.12.2023

		Медведенко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

29. Turn on hosted S/MIME for message encryption. [Електронний ресурс]. Режим доступу: <https://support.google.com/a/answer/6374496?hl=en> - Дата звернення: 08.12.2023

30. Google Message Encryption. [Електронний ресурс]. Режим доступу: https://static.googleusercontent.com/media/www.google.com/ru//a/help/intl/en/security/pdf/message_encryption.pdf - Дата звернення: 08.12.2023

31. Two-factor authentication can help users to better protect themselves online. [Електронний ресурс]. Режим доступу: <https://about.google/stories/passwort/> - Дата звернення: 09.12.2023

32. Use Workspace DLP to prevent data loss. [Електронний ресурс]. Режим доступу: <https://support.google.com/a/answer/9646351?hl=en> - Дата звернення: 09.12.2023

33. Google Cloud. (2023, 12, 16). Концепції та типи методів. [Електронний ресурс]. Режим доступу: <https://cloud.google.com/dlp/docs/concepts-method-types>

34. Рекомендації щодо структури та змісту Плану захисту інформації в автоматизованій системі. [Електронний ресурс]. Режим доступу: https://wiki.tntu.edu.ua/Рекомендації_щодо_структури_та_змісту_Плану_захисту_інформації_в_автоматизованій_системі - Дата звернення: 09.12.2023

35. Новий алгоритм сортування. [Електронний ресурс]. - Режим доступу: https://ela.kpi.ua/bitstream/123456789/11427/1/10_p35.pdf. - Дата звернення: 10.12.2023.

36. Критеріальний Аналіз Профілю Захищеності Інформації На Підприємстві. [Електронний ресурс]. - Режим доступу: <https://ir.kneu.edu.ua/server/api/core/bitstreams/f886c3e7-a1e7-40a7-8a0a-c28ed160f9b7/content> - Дата звернення: 10.12.2023.

		Медведевко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Медведевко А.В.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Шелуха О.О.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

Характеристика загроз

Вид загрози	Ймовірність	Що порушує	Рівень шкоди	Джерело
Навмисні загрози (з боку зловмисників)				
Порушення фізичної цілісності	висока	к, ц, д, с	неприпустимо високий	внут. зовн.
Доступ до даних з порушенням встановлених правил розмежування доступу	низька	к, ц, д, с	неприпустимо високий	внут. зовн.
Модифікація інформаційних ресурсів, в тому числі програмного забезпечення	низька	ц, д, с	неприпустимо високий	внут. зовн.
Несанкціоноване змінювання повноваження інших користувачів	низька	к, ц, д, с	неприпустимо високий	внут. зовн.
Видавання власних несанкціонованих запитів за запити операційної системи	середня	к, ц, д, с	середній	внут.
Отримання захищених даних за допомогою спеціально організованої серії санкціонованих запитів	середня	к, ц, д, с	середній	внут. зовн.

Читання залишкової інформації з оперативної та зовнішньої пам'яті ЕОМ	низька	к	високий	внут.
Одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача, незаконне розширювання своїх повноважень, видавання себе за зареєстрованого користувача, вивчання права доступу інших користувачів	низька	к, ц, д, с	неприпустимо високий	внут. зовн
Маскування захищених даних під незахищені	Дуже висока	к	високий	внут.
Впровадження і використання забороненого політикою безпеки ПЗ	висока	к, ц, д, с	високий	внут. зовн.
Несанкціоноване копіювання носіїв інформації	висока	к	високий	внут.
Крадіжки носіїв інформації, виробничих відходів (роздруківок, записів тощо)	низька	к	середній	внут.
Фальсифікація фактів формування та видачі даних	висока	ц	високий	внут.

Підтвердження отримання від деякого користувача даних, сформованих самим порушником	висока	ц	високий	внут.
Підтвердження передачі якому–небудь користувачеві даних, які не передавалися	висока	ц	середній	внут.
Фальсифікація фактів отримання даних	висока	ц	середній	внут.
Розкриття змісту даних у каналах зв'язку	висока	к	високий	внут.
Виконання аналізу потоку даних (трафіку)	висока	д, с	низький	внут. зовн
Змінювання потоку даних, наприклад шляхом генерації несправжніх повідомлень для перевантаження системи	висока	ц, д, с	високий	внут. зовн
Переривання передачі потоку даних	дуже висока	ц, д	Неприпустимо високий	внут. зовн
Виконання ініціації фіктивного з'єднання	середня	ц, д	високий	внут.

Випадкові загрози				
Дії, що призводять до відмови АС чи окремих її елементів, руйнування апаратурних ресурсів та обладнання	низька	к, ц, д, с	неприпустимо високий	внут.
Ненавмисне пошкодження носіїв інформації чи інформації, яка зберігається на цих носіях	низька	к, ц	низький	внут.
Неправомірна зміна режимів роботи АС	низька	к, ц, д, с	неприпустимо високий	внут.
Невмисне зараження програмних засобів комп'ютерними вірусами	значна	к, ц, д, с	неприпустимо високий	внут.
Невиконання організаційних заходів щодо порядку і правил експлуатації чи використання ресурсів	низька	к, ц, д, с	неприпустимо високий	внут.
Помилки при введенні даних в систему, видачі даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо	низька	к, ц, д, с	високий	внут.

		Медведенко А.В.		
		Шелуха О.О.		
Змн.	Арк.	№ докум.	Підпис	Дата

КІК.КР.Б – 125 – 15 – ПЗ

Арк.

78

Неправомірне впровадження і використання забороненого політикою безпеки програмного забезпечення	низька	к, ц, д, с	низький	внут.
Некомпетентне застосування засобів захисту	висока	к, ц, д, с	високий	внут.
Наслідки викривлень під час проектування та розробки компонентів	низька	к, ц, д, с	неприпустимо високий	внут.
Впливи природних факторів				
Зміна умов фізичного середовища (стихійні лиха, як землетрус, повінь, пожежа і аварії або інші випадкові події)	низька	ц, д, с	неприпустимо високий	зовн.
Збої та відмови у роботі обладнання та технічних засобів, аварійне відключення живлення та т.п.	низька	ц, д, с	неприпустимо високий	внут.
Впливи природних завад (грозіві розряди, іскріння в електромережах, під час електрозварювання та т.п.	низька	ц, д, с	неприпустимо високий	зовн.