МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

Кафедра комп'ютерних технологій та інформаційної безпеки

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент
_____ С.М. Нужний
«18» 06 2025 р.

Кваліфікаційна робота
на правах рукопису

КВАЛІФІКАЦІЙНА РОБОТА

ОРГАНІЗАЦІЯ ЗАХИСТУ БАЗИ ЗНАНЬ ПРИ РОБОТІ З ХМАРНИМ СХОВИЩЕМ

Ступінь вищої освіти: БАКАЛАВР
Галузь знань: 12 «Інформаційні технології»
Спеціальність: 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

Виконала: студентка 4 курсу групи 4381
Письменюк Варвара Андріївна

Кваліфікаційна робота містить результати самостійного виконання навчального завдання. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Письменюк В.А.

Керівник: доцент кафедри комп'ютерних технологій та інформаційної безпеки к.т.н., доцент **Сірівчук Андрій Сергійович** _____

Миколаїв – 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

ЗАТВЕРДЖУЮ
Гарант освітньої програми, к.т.н., доцент, завідувач кафедри КТІБ
_____ С.М. Нужний
«18» 06 2025 р.

ЗАВДАННЯ

на кваліфікаційну роботу

Студент: Письменюк Варвара Андріївна

Курс:4

Група: 4381

Ступінь вищої освіти: бакалавр

Галузь знань: 12 Інформаційні технології

Спеціальність: 125 «Кібербезпека та захист інформації»

Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

1. Тема роботи: «Організація захисту бази знань при роботі з хмарним сховищем »

затверджена наказом НУК від «_23__» квітня 2025 р. № УЧ- 343

2. Вихідні дані до роботи: розмеження доступу до ресурсів, подвійний захист даних, що зберігаються, об'єкт база знань Obsidian.

3. Перелік питань, які необхідно розробити: аналіз загроз використання хмарних середовищ для зберігання даних; визначення вимог до безпечного зберігання та передачі даних; розробка системи захисту.

4. Терміни виконання завдання:
термін видачі завдання: «_03_» лютого 2025 р.
термін подання роботи: «18» червня 2025 р.

6. План-графік виконання кваліфікаційної роботи

№ п/п	Заходи	Дата		Готовність	Відмітка про виконання
		Навч. тиждень	Контрольна дата		
19.	Організаційні збори.	23	03.02.2025	Вибір теми, визначення мети, завдань, об'єкта та предмета дослідження	вик
20.	Організаційні збори	25	20.02.2025	Попередній варіант оглядових розділів, підбір і опрацювання списку використаних джерел	вик
21.	Рубіжний контроль	31	03.04.2025	Попередній варіант повної КР.	вик
22.	Рубіжний контроль	33	20.04.2025	Попередній варіант презентації.	вик
23.	ЄДКІ на рівень «бакалавр»	34	29.04.2025	Здавання ЄДКІ зі спеціальності на ступінь бакалавра	вик
24.	Перевірка на плагіат	42	14.06.2025	1. Електронний варіант кваліфікаційної роботи; 2. Подання КР на перевірку на плагіат.	вик
25.	Кафедральний захист	43	18.06.2025	1. Оформлена КР (в форматі pdf) (передається студентом на кафедрі для внутрішньої рецензії, висновок керівника). У разі отримання позитивної внутрішньої рецензії, КР подається на зовнішню рецензію. 2. Оформлена презентація (в форматі pdf).	вик
26.	Подання документів на захист	44	24.06.2025	1. Подання щодо захисту КР 2. Зовнішня рецензія (окремо від КР). Резюме на КР. 3. Висновок кафедри про КР, допуск до захисту; 4. Електронний варіант та роздрукована презентація в кількості 5 примірників. 5. Електронний варіант КР на диску	вик
27.	Захист КР	44	25.06.2025	1. Приєднання студента до засідання кваліфікаційної комісії (конференції) у встановлений час для проведення процедури дистанційного захисту 2. Процедура захисту КР.	вик

ПРИМІТКА: Завдання додається до виконаної роботи та подається до атестаційної комісії.

Керівник
Доцент кафедри комп'ютерних технологій
та інформаційної безпеки, к.т.н., доцент _____ А.С. Сірівчук

Студент _____ В.А. Письменюк

АНОТАЦІЯ

Письменюк В. А. Організація захисту бази знань при роботі з хмарним сховищем. – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття ступеня вищої освіти «бакалавр» за спеціальністю 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології», освітньо-професійна програма «Системи технічного захисту інформації, автоматизація її обробки». – Національний університет кораблебудування імені адмірала Макарова, Миколаїв, 2025.

Пояснювальна записка: 63 с., 26 рис., 20 джерел.

Кваліфікаційна робота присвячена актуальній темі – підвищенню рівня захисту в хмарних середовищах.

Метою даної роботи є організація захисту бази знань в хмарному середовищі. В роботі проведено аналіз проблем використання хмарних середовищ, розглянуто основні загрози витоку інформації та сучасні методи захисту даних у хмарних системах. Особливу увагу приділено механізмам забезпечення конфіденційності та контролю доступу.

В роботі також представлений аналіз вимог до системи захисту даних у хмарних сховищах. Проведено дослідження нормативно-правової бази захисту даних та формалізовано основні завдання безпеки при використанні таких технологій.

Також було розроблено систему захисту даних у хмарному середовищі, проведено налаштування програмних засобів та розглянуто їхню інтеграцію з персональним комп’ютером. Виконано тестування запропонованого рішення для оцінки його ефективності. Результатом дипломної роботи є розробка підходу, який поєднує використання хмарних сервісів із засобами локального шифрування даних. Зокрема, було обґрунтовано доцільність використання програми Cryptomator для забезпечення додаткового рівня безпеки конфіденційних даних користувача.

Ключові слова: хмарні сховища, безпека даних, шифрування, захист інформації, Cryptomator.

ANNOTATION

Pysmeniuk V. A. Organization of knowledge base protection when working with cloud storage. – Qualification work in the form of a manuscript.

Qualification work for the degree of higher education "Bachelor" in the specialty 125 "Cybersecurity and information protection" of the field of knowledge 12 "Information technologies", educational and professional program "Systems of technical information protection, automation of its processing". – Admiral Makarov National University of Shipbuilding, Mykolaiv, 2025.

Explanatory note: 63 p., 26 fig., 20 sources.

The qualification work is devoted to a topical topic - increasing the level of protection in cloud environments.

The purpose of this work is to organize the protection of the knowledge base in a cloud environment. The work analyzes the problems of using cloud environments, considers the main threats of information leakage and modern methods of data protection in cloud systems. Particular attention is paid to mechanisms for ensuring confidentiality and access control.

The paper also presents an analysis of the requirements for a data protection system in cloud storage. A study of the regulatory framework for data protection was conducted and the main security tasks when using such technologies were formalized.

A data protection system in a cloud environment was also developed, software settings were performed and their integration with a personal computer was considered. The proposed solution was tested to assess its effectiveness. The result of the thesis is the development of an approach that combines the use of cloud services with local data encryption tools. In particular, the feasibility of using the Cryptomator program to provide an additional level of security for confidential user data was substantiated.

Keywords: cloud storage, data security, encryption, information protection, Cryptomator.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ARP – Address Resolution Protocol

CSE – Client-Side Encryption

DLP – Data Loss Prevention

DNS – Domain Name System

ICMP – Internet Control Message Protocol

RAT – Remote Access Trojan

БФА – багатофакторна автентифікація

КС – комп’ютерна система

НСД – несанкціонований доступ

ПЗ – програмний застосунок

ПК – персональний комп’ютер

ХСЗД – хмарні середовища зберігання даних

ВСТУП

У сучасному світі технології хмарних обчислень стали невід'ємною частиною інформаційного середовища. Використання хмарних сховищ дозволяє значно спростити управління даними, забезпечуючи доступ до інформації з будь-якого пристрою та місця. Проте, зростання обсягів конфіденційної інформації, яка зберігається в хмарних середовищах, спричиняє збільшення кількості загроз безпеці.

Зокрема, серед основних ризиків слід виділити несанкціонований доступ, витоки даних, атакуючі дії з боку кіберзлочинців, ненадійність методів шифрування, а також можливі вразливості у політиках доступу. У зв’язку з цим актуальним стає завдання створення надійної системи захисту, яка забезпечувала б високий рівень безпеки передачі та зберігання даних, а також контроль за доступом до них.

Забезпечення конфіденційності, цілісності та доступності інформації у хмарному середовищі є критично важливим питанням як для корпоративних користувачів, так і для окремих осіб. Таким чином, дослідження проблеми захисту даних у хмарних сховищах та розробка відповідних механізмів безпеки є надзвичайно актуальним.

Метою кваліфікаційної роботи є налаштування системи захисту бази знань, що знаходиться в хмарному середовищі.

Об’єктом кваліфікаційної роботи розробка системи захисту файлів, що зберігаються в хмарному середовищі.

Предметом кваліфікаційної роботи є реалізація безпечної мережі, аналіз загроз безпеці та розробку системи безпеки, яка забезпечує належний захист конфіденційної інформації.

Для вирішення поставленої мети вирішено наступні завдання:

– аналіз сучасних загроз, пов’язаних із використанням хмарних середовищ для зберігання даних;

– дослідження існуючих методів і технологій захисту інформації у хмарних сховищах;

– визначення ключових вимог до безпечного зберігання та передачі даних;

– розробка системи захисту конфіденційної інформації у хмарному середовищі;

– тестування розробленої системи та оцінка її ефективності.

Результати роботи частково опубліковані в наступному джерелі:

Письменюк В. А., Ферцович М.С. Організація захисту бази знань при роботі з хмарним сховищем / Наук. керівник А.С. Сірівчук // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XII всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв: НУК, 2024.

Дана кваліфікаційна робота може бути використана для підвищення рівня безпеки інформації у хмарних сервісах та застосована у реальних умовах для захисту даних як у корпоративному, так і в особистому використанні.

1 АНАЛІЗ ПРОБЛЕМИ ВИКОРИСТАННЯ ХМАРНИХ СЕРЕДОВИЩ

1.1 Аналіз загроз витоку інформації

Незважаючи на досягнення технологій кібербезпеки постачальниками хмарних послуг, безпека ресурсів хмарних сховищ залишається проблемою. Проблеми з безпекою хмарного сховища, такі як неналежне керування та моніторинг, можуть призвести до того, що конфіденційні дані стануть доступними для неавторизованих сторін. Загрози для хмарних сервісів можуть бути як технічно-програмні заходи так і некомпетентність користувачів [1,2,3].

1.1.1 Злом облікових даних

Взлом облікових даних є однією з найпоширеніших кіберзагроз, яка може привести до витоку конфіденційної інформації та компрометації особистих даних. Зловмисники використовують різноманітні методи, від фішингу до перебору паролів, аби отримати несанкціонований доступ до облікових записів.

Найчастішими причинами взлому облікових даних користувачів є:

– використання слабких паролів: короткі, очевидні або поширенні паролі, котрі легко зламати через перебір чи використовуючи бази даних, що були оприлюднені;

– відсутність багатофакторної аутентифікації (БФА): якщо людина не використовує додатковий рівень захисту (наприклад, код підтвердження, що висилають *SMS* повідомленням на телефон, дзвінок для вводу коду або відповідь на секретне питання), зловмиснику буде достатньо легко обійти базовий захист;

– людський фактор: нерідко користувачі бувають неуважні та переходять за посиланнями або завантажують файли з підозрілих листів, не приділяють увагу *URL*-адресам сайтів, що можуть мати незначну відмінність від оригіналу, та вводять там власні данні;

– використання одного пароля для різних сервісів: якщо один з сервісів зазнає злому, усі інші облікові записи даного користувача з тим самим паролем стають уразливими та є потенційними цілями зловмисника;

– ігнорування оновлень програмного забезпечення: вразливості в застарілих версіях програм можуть бути використані хакерами;

– ненадійні мережі: використання неперевірених, незахищених публічних *Wi-Fi* без *VPN* створює ризик перехоплення даних та робить інформацію незахищеною від стороннього втручання.

1.1.2 Перехоплення даних при їх передачі.

Перехоплення передачі даних становить серйозну загрозу для безпеки хмарних середовищ, оскільки зловмисники можуть отримати несанкціонований доступ до конфіденційної інформації під час її передачі між клієнтом і хмарним сервісом. Існує кілька методів перехоплення даних, які можна класифікувати за різними рівнями атаки:

1) Перехоплення у *Wi-Fi* мережах. Зловмисники можуть створювати підроблені *Wi-Fi* мережі, відомі як «*Evil Twin*», які імітують легітимні мережі, або підключатися до тієї ж мережі, що й жертва. Використовуючи інструменти для аналізу мережевого трафіку, такі як *Wireshark*, вони можуть перехоплювати незашифровані дані, що передаються між користувачем і хмарним сервісом. Відсутність шифрування або використання слабких протоколів робить ці атаки особливо ефективними.

Механізм роботи такої атаки виглядає наступним чином:

– створюється точка доступу *«Evil Twin»*: зловмисник запускає точку доступу *Wi-Fi* з тим самим ідентифікатором *SSID*, що й легітимна мережа. Це часто робиться за допомогою спеціалізованого обладнання, наприклад, *Wi-Fi* – адаптерів у режимі моніторингу або програм, таких як *Airbase-ng* із набору інструментів *Aircrack-ng*. Пристрої користувачів автоматично підключаються до підробленої точки, якщо вона має сильніший сигнал або налаштована як "відкрита" (без пароля);

– аналізується незашифрований трафік: після підключення зловмисник використовує програми-аналізатори, такі як *Wireshark*, для збору даних, що передаються між пристроєм жертви та мережею. Якщо з'єднання не використовує *HTTPS* або інші форми шифрування (*TLS/SSL*), ці дані можна

переглянути у вигляді відкритого тексту. Це можуть бути облікові записи, паролі, файли тощо;

– далі використовується вразливість до *Man-in-the-Middle* (*MITM*): зловмисник може діяти як посередник між клієнтом і сервером, перенаправляючи весь трафік через свій пристрій. Для цього часто використовується інструмент *Ettercap*, який дозволяє автоматично модифікувати чи переглядати дані, що передаються.

2) Спуфінг *ARP*. *ARP* (*Address Resolution Protocol*) використовується для перетворення *IP*-адрес на *MAC*-адреси в локальних мережах. Оскільки *ARP* не має вбудованого механізму аутентифікації, його можна обдурити.

Механізм роботи такої атаки наступний:

– зловмисник надсилає підроблені *ARP*-відповіді до мережі. У цих повідомленнях зазначається, що *IP*-адреса, наприклад, маршрутизатора або іншого легітимного пристрою, асоціюється з *MAC*-адресою пристрою зловмисника;

– далі виконується так зване “отруєння” таблиці *ARP*: таблиці *ARP* пристроїв у мережі оновлюються на основі отриманих повідомлень. У результаті, всі пристрої починають надсилати дані, призначені для маршрутизатора, через пристрій зловмисника;

– після того, як трафік перенаправлено через пристрій зловмисника, він може бути: збережений для подальшого аналізу; змінений перед пересиланням до кінцевого пункту; заблокований, що призводить до відмови в обслуговуванні.

Для виконання даної атаки зловмисники використовують утиліти, такі як *Arpspoof, Bettercap,* або *Ettercap*. Вони автоматизують процес надсилання фальшивих *ARP*-відповідей.

3) *DNS*-спуфінг. *DNS* (*Domain Name System*) відповідає за перетворення доменних імен (наприклад, *google.com*) у відповідні *IP*-адреси. Якщо *DNS*-запити або записи компрометуються, жертва може бути перенаправлена до підроблених ресурсів.

Механізм роботи атаки:

– зміна локального кешу *DNS*: зловмисник може внести фальшиві записи в локальний кеш *DNS* пристрою жертви. Це робиться за допомогою скриптів, які змінюють файл хостів (наприклад, *hosts* у *Windows* чи *Linux*), або через маніпуляції в операційній системі;

– підміна *DNS*-відповідей: якщо зловмисник перебуває в одній мережі з жертвою, він може перехоплювати *DNS*-запити та надсилати підроблені відповіді. Це досягається шляхом використання таких інструментів, як *dnsspoof* або *Bettercap*;

– «отруєння» *DNS*-сервера: зловмисник змінює записи *DNS* на сервері, до якого підключаються клієнти. Наприклад, запис для домену *bank.com* змінюється на *IP*-адресу сервера зловмисника. Сервер може розташовувати фішингову копію справжнього вебсайту. Підроблений сервер може завантажувати шкідливі файли замість легітимних;

– атака з використанням *MITM*: зловмисник може поєднувати *DNS* - спуфінг із *MITM*-атаками, щоб змінювати вміст трафіку в реальному часі.

4) Хибна маршрутизація. *ICMP* (*Internet Control Message Protocol*) використовується в мережах для обміну службовими повідомленнями, наприклад, для повідомлення про помилки або оптимізацію маршрутів. Повідомлення *ICMP Redirect* дозволяють пристроям оновлювати свої маршрути до певного хоста.

Атака методом хибної маршрутизації використовує фальшиві повідомлення *ICMP Redirect* аби змінювати маршрутизації даних між пристроями в мережі.

Принцип дії даної атаки наступний:

– зловмисник надсилає фальшиве повідомлення *ICMP Redirect*, у якому вказується, що для доступу до певного *IP*-адреса найкращий маршрут проходить через пристрій зловмисника. Наприклад, повідомлення може виглядати так, ніби воно надійшло від маршрутизатора;

– пристрій жертви приймає фальшиве повідомлення та змінює свою таблицю маршрутизації. Усі дані, що мають бути передані на певний *IP*-адрес, тепер перенаправляються через пристрій зловмисника;

– далі відбувається перехоплення та модифікація даних: зловмисник може зберігати всі дані, що проходять через його пристрій, використовуючи програмне забезпечення для аналізу трафіку; змінювати вміст даних перед передачею до кінцевого отримувача; здійснювати інші атаки, такі як впровадження шкідливого ПЗ у переданий трафік.

Для виконання таких атак хакери використовують утиліти, як-от *Nemesis* або спеціалізовані бібліотеки в *Python*, що дозволяють створювати кастомні *ICMP*-повідомлення.

5) Перехоплення *TCP*-з’єднання

Зловмисник може перехопити активне *TCP*-з'єднання між клієнтом і сервером, використовуючи методи, такі як захоплення сеансу (*session hijacking*). Це дозволяє йому отримати доступ до переданих даних або виконувати дії від імені жертви.

TCP (*Transmission Control Protocol*) — це протокол, який забезпечує надійну передачу даних між клієнтом і сервером. З'єднання встановлюється через «триетапний рукостиск» (*three-way handshake*):

– *SYN* (запит на встановлення з'єднання);

– *SYN-ACK* (підтвердження сервера);

– *ACK* (підтвердження клієнта).

Суть атаки полягає в тому, що зловмисник перехоплює вже активне *TCP*-з'єднання, використовуючи метод захоплення сеансу (*session hijacking*). Після захоплення з'єднання він отримує доступ до поточної сесії жертви, зберігаючи активність і автентифікацію.

Механізм роботи атаки полягає в наступному:

– зловмисник перехоплює пакети *TCP* між клієнтом і сервером за допомогою інструментів, таких як *Ettercap* або *MITMf* (*Man-in-the-Middle Framework*);

– потім він аналізує ці пакети, щоб отримати номер поточної *TCP*-сесії (наприклад, *Session ID*);

– після чого хакер підробляє свій пристрій під клієнта або сервер, підставляючи правильний номер сесії. Це дозволяє продовжити сеанс без обриву з'єднання.

Для виконання даної атаки використовують як вищезгаданий *Ettercap* та *Wireshark*, так і *Hunt* - спеціалізований інструмент для захоплення сесій *TCP* у реальному часі.

1.1.3 Доступ до комп’ютера зі встановленим клієнтом хмарним сховищем

Однією з найсерйозніших загроз безпеці даних у хмарних середовищах є фізичний або віддалений доступ зловмисника до комп’ютера, на якому встановлено клієнт хмарного сховища. Такий сценарій може призвести до крадіжки, компрометації або повного видалення даних. Зловмисник може отримати доступ до комп’ютера користувача наступними способами:

1) Фізичний доступ до пристрою:

– несанкціонований вхід до системи: якщо комп’ютер користувача не захищений паролем або пароль є слабким, зловмисник може отримати повний доступ до системи та до синхронізованих файлів у хмарному сховищі.

– клонування носіїв даних: зловмисник може фізично скопіювати диск пристрою, на якому зберігаються синхронізовані файли або кешовані дані хмарного клієнта.

2) Використання шкідливого програмного забезпечення:

– віддалений контроль пристрою: зловмисник може встановити програми віддаленого доступу (наприклад, *RAT – Remote Access Trojan*) через фішингові атаки, заражені файли або вразливості в програмному забезпеченні;

– кейлогери та шпигунське ПЗ: кейлогери записують введені паролі, а шпигунське ПЗ може зчитувати локальні файли або дані з кешу клієнта хмарного сховища.

1.2 Аналіз захисту в системах хмарного зберігання даних

Сучасні системи хмарного зберігання даних стали важливим інструментом для збереження, доступу та спільної роботи з інформацією. Завдяки таким платформам, як *Google Drive*, *Dropbox*, *Microsoft OneDrive* та *Mega*, користувачі отримують можливість зберігати файли у віддалених серверах і отримувати до них доступ із будь-якого пристрою, підключеного до Інтернету.

Проаналізуємо можливості та функціонал популярних хмарних платформ, таких як *Google Drive* (у безкоштовній і платній версіях), *Dropbox*, *Microsoft OneDrive* і *Mega*, з акцентом на їхню безпеку.

Основна мета аналізу – визначити переваги та недоліки кожної з платформ з точки зору захисту інформації та сформувати уявлення про те, які рішення можуть бути найкращими для забезпечення безпеки даних у різних сценаріях використання.

1.2.1 *Google Drive*

Google Drive [4] – це хмарний сервіс зберігання, який дозволяє користувачам зберігати та отримувати доступ до файлів онлайн. Сервіс синхронізує збережені документи, фотографії та багато іншого на всіх пристроях користувача, включаючи мобільні пристрої, планшети та ПК.

Використовуючи безкоштовну версію *Google Drive* кожен користувач отримує 15 ГБ безкоштовного хмарного сховища, котре розподіляється між *Google Drive*, *Gmail* та *Google* Фото. Цей обсяг підходить для зберігання документів, фотографій та інших файлів. Безкоштовна версія також надає доступ до офісних додатків *Google*, таких як Документи, Таблиці та Презентації, що дозволяє створювати та редагувати файли онлайн з можливістю спільної роботи в реальному часі.

Платна версія даного застосунку дозволяє використовувати більший обсяг пом’яті хмарного середовища: від 100 ГБ до кількох терабайт в залежності від обраного плану. Крім того, користувач отримує доступ до експертів *Google*, розширенні можливості резервного копіювання (автоматичне резервне

копіювання даних з мобільного пристрою на *Google* Диск, що забезпечує додатковий рівень захисту інформації), розширені можливості користування *Meet* та всі функції *Workspace Individual*, при використанні тарифу *AI Premium* користувач отримує доступ до всіх можливостей *Gemini Advanced*.

Розмежування прав доступу в платному та безкоштовному тарифах працює однаково. *Google Drive* надає наступні права доступу до файлів:

– власник: має повний контроль над файлом або папкою, може редагувати видаляти, надавати доступ іншим користувачам та змінювати їхні права;

– редактор: може вносити зміни до файлу або папки, задавати доступ іншим користувачам, але не може змінювати права власника;

– коментатор: може переглядати файл або папку та додавати коментарі, не може вносити зміни до вмісту;

– читач: може лише переглядати файл або папку, не може вносити зміни або додавати коментарі.

Спільний доступ користувачам надається за електронною адресою або за посиланням.

Для забезпечення безпеки даних *Google Drive* застововує такі методи як 128-бітові та 256-бітові ключі *AES* (залежно від типу носія) та протокол *TLS*.

Під час завантаження файлів на *Google Drive* вони розміщуються у захищених дата-центрах *Google*. Для збережених даних, а також для інформації, що передається, використовується шифрування. *Google* застосовує 128-бітові або 256-бітові ключі *AES* (залежно від типу носія) для захисту файлів, що допомагає забезпечити їх конфіденційність.

Однак *Google* володіє ключами шифрування, що потенційно дозволяє компанії розшифровувати файли за потреби. Дані, що зберігаються, розбиваються на менші частини, кожна з яких зашифрована окремим ключем. Це ускладнює роботу зловмисникам, оскільки їм довелося б зламати кілька ключів для доступу до інформації.

Для даних, що передаються, *Google* використовує протокол *TLS*, який захищає з'єднання від перехоплення та атак типу «зловмисник у середині». Проте

після надання спільного доступу файли можуть стати вразливими. Ризик витоку особливо високий, коли користувачі створюють загальнодоступні посилання з повними правами, що дозволяють будь-кому переглядати, змінювати чи копіювати файл.

Незважаючи на рівень безпеки, *Google* зберігає ключі шифрування для всіх файлів на *Google Drive*, що може створити потенційні вразливості. Оскільки саме *Google* контролює ці ключі, існує ризик несанкціонованого доступу. Як і у випадку з іншими хмарними сервісами, найбільші загрози пов'язані не стільки з інфраструктурою безпеки, скільки з самим користувачем і його діями.

1.2.2 *Dropbox*

Dropbox [5] – це популярний сервіс хмарного зберігання та спільної роботи, який допомагає користувачам організовувати, зберігати та ділитися файлами з будь-якого пристрою.

Оскільки *Dropbox* не має власного офісного пакета або поштового клієнта він співпрацює з файлами як *Microsoft*, так і *Google*. Якщо користувач хочете переключатися між послугами, *Dropbox* робить це легко. Замість того, щоб вибирати, якому сервісу користувач надаєте перевагу, *Dropbox* дозволяє використовувати обидва.

Основні функції *Dropbox*:

– хмарне зберігання та синхронізація: *Dropbox* дозволяє зберігати файли в хмарі та синхронізувати їх між різними пристроями, забезпечуючи доступ до актуальних версій документів у будь-який час;

– обмін файлами та папками: користувачі можуть легко ділитися файлами та папками з іншими, надаючи доступ через посилання або запрошення, а також встановлювати права доступу та захист паролем для додаткової безпеки;

– резервне копіювання та відновлення файлів: сервіс автоматично створює резервні копії файлів і дозволяє відновлювати видалені або попередні версії документів протягом певного періоду часу.

– спільна робота в реальному часі: Функції, такі як коментування та анотування файлів, дозволяють командам ефективно співпрацювати та обмінюватися відгуками безпосередньо в *Dropbox*.

Dropbox надає можливість керувати правами доступу до файлів і папок, забезпечуючи зручність і безпеку спільної роботи. Доступні рівні дозволяють користувачам визначати, хто і які дії може виконувати з файлами та папками.

Власник – це користувач, який створив спільну папку або кому передали повне право володіння. Він має наступні можливості:

– переглядати, редагувати та видаляти файли у папці; додавати та видаляти учасників зі спільної папки;

– змінювати рівень доступу інших учасників (наприклад, робити редакторів читачами);

– передавати права власності іншому користувачеві; видаляти спільну папку для всіх учасників;

– контролювати посилання для спільного доступу (хто може бачити та редагувати файли через них).

Редактор – це користувач, який отримує можливість не тільки переглядати, але й змінювати вміст папки. Можливості редактора включають:

– переглядати та відкривати файли;

– додавати нові файли та змінювати наявні;

– видаляти файли та папки у межах спільної папки;

– коментувати файли (за умови, що ця функція увімкнена);

– завантажувати та зберігати локальні копії файлів;

– додавати нових користувачів (якщо власник дозволив);

– ділитися файлами через посилання (якщо власник дозволив).

Читач – це користувач, який може переглядати, але не змінювати вміст папки. Можливості читача:

– переглядати та відкривати файли та папки;

– завантажувати копії файлів для локального використання; коментувати файли (якщо власник це дозволив);

– ділитися файлами через посилання (якщо власник дозволив).

Розширена версія прав Читача, яка дозволяє залишати коментарі у файлах. Можливості читача з коментуванням:

– переглядати файли;

– залишати коментарі в документах без можливості змінювати вміст;

– завантажувати файли.

Крім того, даний застосунок дозволяє власникам обмежувати можливість поширення файлів. Власник може відключити можливість пересилання посилань, що не дозволить користувачам поділитись доступом без його (власника) дозволу та обмежити завантаження файлів, завдяки чому учасники не зможуть завантажити файли на свій пристрій.

Також *Dropbox* дозволяє захистити посилання паролем та встановити дати припинення строку дії для надання тимчасового доступу.

Для забезпечення безпеки користувачів дане хмарне сховище використовує ті ж методи шифрування, що й *Google Drive*, тобто: метод 256-бітне шифрування *AES* для даних, що зберігаються на сховищі та протокол *SSL/TLS* для даних, що пересилаються. Однак, *Dropbox* за всю історію свого існування мав доволі багато епізодів порушення безпеки, останнє з яких відбулось в 2018 році, що змушує сумніватись в його надійності.

1.2.3 *Microsoft OneDrive*

Microsoft OneDrive [6] – це хмарний сервіс зберігання даних, який забезпечує зручний доступ до файлів, їх резервне копіювання, редагування та спільне використання на різних пристроях. Він інтегрований з *Microsoft 365*, що забезпечує безшовну роботу з такими додатками, як *Word, Excel* та *PowerPoint*.

Основні функції *OneDrive* включають:

– зберігання та синхронізація файлів: *OneDrive* надає можливість зберігати файли в хмарі та синхронізувати їх на різних пристроях, включаючи ПК, ноутбуки, планшети та смартфони;

– *Personal Vault*: спеціальна захищена область для зберігання найбільш конфіденційних файлів. Доступ до цієї області захищений додатковими

методами автентифікації, такими як біометрія або двофакторна автентифікація, що забезпечує підвищений рівень безпеки для важливих документів;

– спільна робота: користувачі можуть надавати доступ до файлів іншим особам та спільно працювати над документами в реальному часі;

– інтеграція з *Microsoft* 365: *OneDrive* тісно інтегрований з іншими сервісами *Microsoft* 365, що дозволяє легко створювати, редагувати та зберігати документи безпосередньо в хмарі. Крім того, дане хмарне сховище інтегроване у *Windows* 10 та *Windows* 11;

– відновлення файлів: *OneDrive* дозволяє відновлювати попередні версії файлів протягом останніх 30 днів, що є корисним у випадку випадкового видалення або пошкодження даних;

– пошук та організація: додаток пропонує покращений пошук з новими фільтрами та більш детальними результатами, а також підтримку кольорових папок у Провіднику файлів *Windows*.

У *Microsoft OneDrive* користувачі можуть керувати доступом до файлів і папок, надаючи різні рівні дозволів іншим особам. Це забезпечує гнучкість у спільній роботі та контроль над вмістом. Система має два основні рівні доступу: доступ із можливістю редагування та доступ лише для перегляду

Доступ із можливістю редагування – користувачі з цим рівнем доступу можуть переглядати, редагувати, видаляти та додавати нові файли або папки. Можливості, що надаються:

– зміна наявних файлів та створення нових;

– видалення або перейменовування файлів та папок;

– обмін файлами з іншими користувачами.

Доступ лише для перегляду – користувачі можуть переглядати та читати файли, але не можуть їх змінювати або видаляти. Можливості:

– перегляд та завантаження файлів;

– коментування файлів, якщо ця функція доступна;

– не можна змінювати або видаляти вміст.

Крім того, також є додаткові параметри спільного доступу: створення посилання, яке дозволяє будь-кому з ним переглядати або редагувати файл, навіть без облікового запису *Microsoft* та обмеження завершення дії посилання або встановлення пароля. Також адміністратори можуть обмежити доступ до вмісту *OneDrive* для певних груп користувачів, використовуючи групи безпеки *Microsoft Entra ID*.

Для забезпечення безпеки *OneDrive* використовує 256-бітне шифрування *AES* для даних, що перебувають на сховищі та з'єднання *SSL/TLS* для даних, що пересилаються. Для особистих облікових записів дані шифруються при передачі і "в стані спокою", але *Microsoft* не надає інформації, який саме метод шифрування застосовується.

OneDrive має вбудовані механізми виявлення шкідливих програм-вимагачів (*ransomware*). Якщо система виявляє підозрілу активність, користувач отримує сповіщення та може відновити файли до попередньої версії.

Даних хмарний застосунок також дозволяє відновлювати попередні версії файлів, що допомагає у випадку випадкових змін, видалень або атак зловмисників. Для бізнес-версій передбачено розширене керування версіями.

1.2.4 *Mega*

MEGA [7] – це хмарний сервіс зберігання даних, відомий своїм акцентом на безпеці та конфіденційності користувачів. З моменту свого запуску в 2013 році він надає широкий спектр функцій для ефективного управління файлами та спільної роботи.

Основні функції *MEGA* включають:

– хмарне зберігання та синхронізація: *MEGA* пропонує безкоштовний обліковий запис з 20 ГБ простору для зберігання, що є одним із найбільших обсягів серед безкоштовних планів. Доступні клієнти для *Windows, macOS, Linux,* а також мобільні додатки для *iOS* та *Android*, що забезпечує синхронізацію файлів між різними пристроями;

– спільна робота та обмін файлами: можливість ділитися файлами та папками з іншими користувачами через посилання з налаштуванням прав

доступу. Платні користувачі можуть встановлювати паролі та дати завершення дії для спільних посилань, підвищуючи безпеку при обміні даними;

– резервне копіювання та версіонування: функція *MEGA Backup* забезпечує автоматичне резервне копіювання вибраних папок з комп'ютера до хмари, з можливістю відновлення попередніх версій файлів та відстеження видалених елементів;

– *MEGA VPN*: у 2024 році *MEGA* запустила власний *VPN*-сервіс для захисту онлайн-активності користувачів, доступний на платформах *iOS, macOS, Windows* та *Android*;

– *MEGA S*4 (*Simple Secure Storage Service*): у грудні 2024 року *MEGA* представила *S*4 – об'єктне сховище з підтримкою *S*3-сумісного *API*, орієнтоване на фрілансерів, стартапи та індивідуальних розробників.

MEGA не надає вбудованого офісного пакету або поштового сервісу. Однак, користувачі можуть інтегрувати *MEGA* з іншими додатками для управління електронною поштою та офісними документами. Наприклад, за допомогою програмного забезпечення для управління електронною поштою, яке інтегрується з обліковими записами *IMAP* та *Exchange Web Services* (*EWS*), можна керувати кількома обліковими записами електронної пошти та додатками, включаючи *MEGA*.

В даному хмарному сховищі передбачені наступні рівні прав доступу для користувачів:

– публічний доступ: створення загальнодоступного посилання, яке дозволяє будь-кому переглядати або завантажувати файл;

– приватний доступ: створення посилання з паролем або обмеженням за часом дії для підвищення безпеки (лише для платної версії).

Однак, можливості одночасної спільної роботи над одним файлом у *MEGA* обмежені. Користувачі можуть ділитися файлами та папками, але функціонал реального часу спільного редагування, як у деяких інших хмарних сервісах, не підтримується.

Даний хмарний застосунок приділяє особливу увагу безпеці та конфіденційності користувачів. З усіх представлених хмарних сховищ, лише *MEGA* має наскрізне шифрування (*End-to-End Encryption*), тобто: усі файли шифруються на пристрої користувача перед завантаженням на сервери *MEGA*. Це означає, що лише користувач володіє ключами дешифрування, і навіть *MEGA* не має доступу до вмісту файлів. Однак хоча вміст файлів шифрується, деякі метадані, такі як імена файлів і структура папок, можуть залишатися видимими. Застосунок мінімізує обсяг зібраних метаданих, зберігаючи лише необхідну інформацію для забезпечення функціональності сервісу.

Для шифрування даних, що перебувають в «хмарі» та пересилаються використовуються вищеописані методи шифрування: 128-бітне шифрування *AES* та *TLS* відповідно.

При виборі хмарного сховища важливо враховувати як функціонал, так і рівень безпеки, що забезпечує платформа [8]. Деякі сервіси орієнтовані на зручність спільної роботи, тоді як інші роблять акцент на конфіденційності та наскрізному шифруванні. В таблиці 1.1 представлено порівняльну характеристику можливостей *Google Drive* (платна та безкоштовна версія), *Dropbox*, *Microsoft OneDrive* і *MEGA* за ключовими характеристиками, включаючи доступні функції та заходи захисту даних.

Таблиця 1.1 – Порівняльна характеристика ХСЗД

Функція / Безпека	*Google Drive* (*Free*)	*Google Drive* (платна)	*Dropbox*	*OneDrive*	*MEGA*
Обсяг сховища	15 ГБ	до 30 ТБ	2 ГБ (*Free*), 2 ТБ (*Plus*)	5 ГБ (*Free*), до 6 ТБ (платно)	20 ГБ (*Free*), до 16 ТБ (платно)
Наскрізне шифрування	Ні	Ні	Ні	Ні	Так
Шифрування даних на сервері	*AES*-256	*AES*-256	*AES*-256	*AES*-256	*AES*-128
Шифрування під час передачі	*TLS*	*TLS*	*SSL/TLS*	*SSL/TLS*	*TLS*
Двофакторна автентифікація	Так	Так	Так	Так	Так
Zero-Knowledge Encryption (повна приватність)	Ключі зберігаються на сервері				лише користувач має ключ
Спільна робота над файлами	Підтримується				редагування лише після завантаження
Версійний контроль файлів	30 днів	до 100 днів	до 180 днів у *Dropbox Business*	до 30 днів *Free*, 93-365 днів платно	обмежене зберігання попередніх версій
Обмін файлами	Доступ за посиланням або електронною поштою		Доступ за посиланням підтримка паролю доступу		
Режим конфіденційності	*Google Workspace* має розширені налаштування		*Dropbox Vault* у платній версії	*OneDrive Personal Vault*	шифрування на рівні користувача
Відкритий вихідний код	Ні				доступний код на *GitHub*

Отже, можемо зробити наступні висновки стосовно користування даними застосунаками та для яких цілей вони підходять:

– *Google Drive*: найкращий для спільної роботи над документами, але не підтримує наскрізне шифрування, також має розширені налаштування прав доступу;

– *Dropbox*: хороший варіант для бізнес-користувачів, але також не підтримує наскрізне шифрування та є сумніви щодо забезпечення безпеки, через успішні хакерські, наслідком яких є злив даних користувачів у мережу;

– *OneDrive*: добре інтегрований з *Microsoft* 365, підтримує *Personal Vault,* але *Microsoft* має доступ до файлів, але не підтримує наскрізне шифрування та не розкриває яким методом шифруються дані особистих облікових записів при передачі і “в стані спокою”;

– *MEGA*: найкращий варіант для користувачів, які цінують конфіденційність і безпеку, але не підтримує спільне редагування файлів онлайн, що є досить важливим при груповій роботі.

1.3 Захист даних на локальному комп’ютері

Захист даних на локальному пристрої є важливим елементом загальної кібербезпеки, оскільки компрометація фізичного пристрою може призвести до втрати або витоку конфіденційної інформації.

Методи забезпечення безпеки даних, включаючи фізичний захист пристрою, захист облікових записів, протидію шкідливому програмному забезпеченню, резервне копіювання та шифрування. Дані методи захисту передбачають наступні параметри:

– фізичний захист пристрою: використання надійного пароля або біометричної аутентифікації (де можливо), увімкнення автоматичного блокування екрану після періоду бездіяльності, зберігання пристрою у безпечному місці, особливо під час роботи у публічних місцях;

– захист облікових записів: використання унікальних та складних паролів для кожного сервісу, увімкнення БФА для облікових записів, використання складних паролів та вимкнення їхнього автоматичного збереження;

– захист від шкідливого програмного забезпечення: встановлення та регулярне оновлення антивірусного програмного забезпечення та системи виявлення вторгнень (*IDS/IPS*), використання брандмауерів для контролю мережевого трафіку та уникання встановлення програм з ненадійних джерел;

– шифрування даних: використання вбудованих засобів операційної системи для шифрування дисків (*BitLocker* у *Windows, FileVault* у *macOS, LUKS* у *Linux*), використання апаратних токенів для зберігання ключів шифрування.

– контроль доступу та журналювання подій: використання засобів моніторингу активності системи (*SIEM*-системи, журналювання подій *Windows/Linux*), встановлення політик обмеженого доступу для важливих файлів та додатків, аудит безпеки та регулярний аналіз логів на предмет підозрілих дій.

Окрім описаних вище методів захисту, варто також звернути увагу на додаткові інструменти шифрування.

Якщо під час роботи використовується хмарне середовище, важливо забезпечити надійне шифрування даних незалежно від можливостей, що надають самі сервіси. Одним із ефективних рішень є безкоштовний програмний застосунок *Cryptomator*, який забезпечує клієнтське шифрування файлів перед їхнім завантаженням у хмару або збереженням на локальному диску.

Cryptomator [9] використовується для забезпечення конфіденційності даних при їх збереженні у хмарних сховищах. Його основна перевага – це зменшення ризику доступу до файлів сторонніми особами, включаючи постачальника хмарних послуг. Для розшифрування даних потрібен ключ шифрування, який невідомий жодній третій стороні.

Cryptomator створює віртуальний диск під назвою *Vault* («підземне сховище»), який можна використовувати як звичайний жорсткий диск або *USB*-накопичувач. Усі файли, що додаються до *Vault*, шифруються автоматично та захищені паролем. Ці сховища можна зберігати на локальному диску, у

хмарному середовищі (наприклад, *Google Drive* або *Dropbox*), а доступ до них можливий з будь-якого пристрою через настільний або мобільний клієнт *Cryptomator*.

Основні особливості *Cryptomator*:

– наскрізне шифрування: файли шифруються перед збереженням, що унеможливлює доступ до їхнього змісту без відповідного ключа;

– прозорість для користувача: програма працює у вигляді віртуального диска, що дозволяє взаємодіяти з файлами так само, як і зі звичайними папками;

– відкритий вихідний код: дозволяє незалежним експертам перевіряти безпеку програми;

– шифрування за алгоритмом *AES*-256: високий рівень безпеки, який забезпечує конфіденційність інформації.

– окреме шифрування кожного файлу: змінюється лише оновлений файл, що оптимізує роботу з хмарними сховищами.

Хоча *Cryptomator* є ефективним засобом для захисту файлів у хмарних сховищах, слід пам’ятати, що він має деякі обмеження: не захищає файли, які зберігаються на локальному комп’ютері без завантаження у *Vault*; не забезпечує захист, якщо програми створюють резервні копії незашифрованих файлів у процесі роботи; не може гарантувати безпеку даних, якщо локальний комп’ютер заражений шкідливим програмним забезпеченням, яке зчитує введені паролі або вміст файлів. Крім того, вона (програма) не є повною заміною іншим інструментам шифрування, оскільки не шифрує мета-інформацію, зокрема: час доступу, зміни або створення файлів; кількість файлів у сховищі; розмір файлів.

Комплексний підхід до безпеки локальних даних включає не тільки стандартні заходи захисту, а й використання додаткових інструментів, таких як *Cryptomator*. Завдяки клієнтському шифруванню та відкритому коду цей застосунок є ефективним способом захисту файлів у хмарних середовищах. Однак, для повного захисту даних слід також враховувати інші методи, зокрема шифрування локального сховища, резервне копіювання, багатофакторну автентифікацію та антивірусний захист. Лише поєднання цих заходів

забезпечить максимальний рівень безпеки даних і захистить їх від потенційних загроз.

Висновок по розділу

У сучасних умовах безпека даних є критично важливим аспектом, особливо в хмарних середовищах, де існує значна кількість потенційних загроз витоку інформації. Використання надійних засобів збереження та захисту даних є необхідністю для зниження ризиків та забезпечення конфіденційності.

Одним із перспективних рішень для роботи в хмарному середовищі є *Google Drive*, що обраний з огляду на його популярність серед користувачів в Україні, зокрема серед освітніх і робочих колективів. Він забезпечує зручний доступ до файлів, спільну роботу та інтеграцію з іншими сервісами *Google*.

2 АНАЛЗ ВИМОГ ДО СИСТЕМИ ЗАХИСТУ

2.1 Аналіз нормативно-правової бази захисту даних в хмарних середовищах

Захист даних у хмарних середовищах є важливим аспектом інформаційної безпеки, що регулюється низкою нормативно-правових актів. Правове регулювання спрямоване на визначення основних вимог до зберігання, обробки та передачі даних, а також на забезпечення їхньої конфіденційності, цілісності та доступності. У цьому розділі розглянуто основні законодавчі та нормативні положення, що регламентують захист даних у хмарних технологіях, а також їхню відповідність сучасним викликам у сфері кібербезпеки.

2.1.1 Закон України «Про захист персональних даних» 2297-VI від 01.06.2010 [10]

Закон України «Про захист персональних даних» 2297-VI встановлює правові засади обробки та захисту персональних даних, що є особливо актуальним у контексті використання хмарних технологій. Закон України "Про захист персональних даних" встановлює чіткі вимоги та обов'язки для організацій, що обробляють персональні дані, включаючи ті, що використовують хмарні технології. Дотримання цих положень забезпечує збереження прав і свобод суб'єктів персональних даних та мінімізує ризики, пов'язані з обробкою інформації у хмарних середовищах.

Основною статтею в даному випадку можна виділити Статтю 24, що зобов'язує володільців та розпорядників персональних даних забезпечити захист цих даних від випадкової втрати, знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних. У контексті хмарних середовищ це вимагає впровадження належних технічних та організаційних заходів безпеки для запобігання несанкціонованому доступу або обробці даних.

2.1.2 Закон України «Про хмарні послуги» 2075-IX від 17.02.2022

Закон України «Про хмарні послуги» №2075-IX від 17 лютого 2022 року [11] встановлює правові засади надання та використання хмарних послуг, а також визначає вимоги до захисту даних у хмарних середовищах. Цей закон є ключовим нормативно-правовим актом, що регулює відносини між постачальниками та споживачами хмарних послуг в Україні.

Стаття 3 класифікує хмарні послуги на кілька категорій, серед яких:

– інфраструктура як послуга (*IaaS*): надання обчислювальних ресурсів, ресурсів зберігання або систем електронних комунікацій;

– платформа як послуга (*PaaS*): доступ до інфраструктури та наборів комп’ютерних програм;

– програмне забезпечення як послуга (*SaaS*): доступ до прикладних комп’ютерних програм через онлайн-сервіс або комп’ютерні програми-агенти.

Хмарні сховища, які використовуються в даній роботі можна віднести до категорії *SaaS*, оскільки вони забезпечують доступ до прикладних програм для зберігання та обміну файлами через інтернет.

Стаття 8 встановлює вимоги до надавачів хмарних послуг та/або послуг центру обробки даних. Зокрема, надавачі зобов'язані не використовувати для надання хмарних послуг технічні засоби, розміщені на територіях, де органи державної влади України тимчасово не здійснюють свої повноваження, або на територіях держав, визнаних Верховною Радою України державами-агресорами чи окупантами, а також не використовувати технічні засоби, що належать суб'єктам, до яких застосовано санкції відповідно до Закону України «Про санкції». Надавачі повинні вживати пропорційних технічних та організаційних заходів для управління ризиками, що виникають для безпеки електронних комунікаційних мереж та інформаційних систем, які використовуються для надання хмарних послуг.

Стаття 11 визначає особливості використання хмарних послуг публічними користувачами, зокрема органами державної влади. Надання хмарних послуг таким користувачам повинно здійснюватися з дотриманням вимог законодавства

про захист персональних даних, захист інформації та кібербезпеку. Забороняється обробка інформації, що становить державну таємницю, за допомогою хмарних ресурсів, розміщених за кордоном або на тимчасово окупованих територіях України, а також тих, що належать державам-агресорам чи суб'єктам, до яких застосовано санкції. І хоча навчальні заклади не завжди підпадають під визначення публічних користувачів, дотримання вимог цієї статті може бути корисним для забезпечення належного рівня безпеки та відповідності законодавству при використанні хмарних сховищ у навчальному процесі.

У контексті використання хмарних сховищ, таких як *Google Drive, OneDrive, Dropbox* та *Mega* для надання студентам доступу до бази знань, важливо враховувати положення статті 13 Закону, яка регулює обробку персональних даних при наданні хмарних послуг. Зокрема, обробка персональних даних у хмарних середовищах повинна здійснюватися відповідно до вимог раніше згаданого Закону України «Про захист персональних даних». Це означає, що при використанні зазначених сервісів необхідно забезпечити конфіденційність, цілісність та доступність персональних даних студентів, а також отримати їх згоду на обробку таких даних.

Крім того, стаття 14 Закону акцентує увагу на захисті інформації при наданні хмарних послуг. Постачальники хмарних послуг зобов'язані впроваджувати належні технічні та організаційні заходи для забезпечення безпеки інформації, включаючи захист від несанкціонованого доступу, випадкової втрати або знищення даних. Це особливо актуально при використанні хмарних сховищ для зберігання та обміну навчальними матеріалами, оскільки гарантує збереження інтелектуальної власності та персональних даних користувачів.

Таким чином, Закон України «Про хмарні послуги» встановлює чіткі вимоги щодо надання та використання хмарних сервісів, спрямовані на забезпечення безпеки та законності обробки даних. При впровадженні хмарних

сховищ у навчальний процес необхідно дотримуватися цих положень, забезпечуючи належний рівень захисту інформації та прав користувачів.

2.1.3 ДСТУ *ISO/IEC* 27001:2023

ДСТУ *ISO/IEC* 27001:2023 є національним стандартом України, що відповідає міжнародному стандарту *ISO/IEC* 27001:2022[12]. Даний стандарт встановлює вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ) в організаціях. Основна мета – забезпечити конфіденційність, цілісність та доступність інформації шляхом систематичного управління ризиками інформаційної безпеки.

У контексті використання хмарних сховищ для надання студентам доступу до бази знань, впровадження СУІБ відповідно до ДСТУ *ISO/IEC* 27001:2023 є критично важливим. Це забезпечує захист чутливої інформації від несанкціонованого доступу, втрати або пошкодження.

Стандарт визначає процеси управління ризиками, які включають ідентифікацію, оцінку та обробку ризиків, пов’язаних з інформаційною безпекою. Це дозволяє організаціям виявляти потенційні загрози та вразливості, розробляти відповідні заходи контролю та впроваджувати їх для мінімізації ризиків.

Важливо зазначити, що ДСТУ *ISO/IEC* 27001:2023 містить оновлені вимоги та рекомендації щодо управління інформаційною безпекою, враховуючи сучасні виклики та технологічні зміни. Зокрема, стандарт узгоджений з оновленою структурою управлінських систем та містить актуалізований перелік заходів безпеки, що відповідають сучасним загрозам.

Додаток А містить перелік контрольних заходів інформаційної безпеки, які організація може застосовувати відповідно до результатів оцінки ризиків. Ці заходи охоплюють аспекти, пов’язані з політиками безпеки, організацією інформаційної безпеки, управлінням активами, контролем доступу, криптографією, фізичною та екологічною безпекою, безпекою персоналу,

безпекою комунікацій та операцій, управлінням інцидентами інформаційної безпеки, аспектами безперервності бізнесу та відповідністю вимогам.

Таким чином, для забезпечення належного рівня захисту інформації при використанні хмарних сховищ у навчальному процесі, навчальним закладам рекомендовано впроваджувати та підтримувати СУІБ відповідно до вимог ДСТУ *ISO/IEC* 27001:2023. Це сприятиме підвищенню довіри студентів та інших зацікавлених сторін до безпеки обробки та зберігання інформації.

2.1.4 НД ТЗІ 2.5-004-99 та НД ТЗІ 1.1-002-99

Нормативні документи НД ТЗІ 2.5-004-99 та НД ТЗІ 1.1-002-99 є [13, 14] важливими для забезпечення захисту інформації в комп'ютерних системах, зокрема при використанні хмарних сховищ, таких як *Google Drive, OneDrive, Dropbox, Mega*, для надання студентам доступу до бази знань.

НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу» визначає методологічні основи захисту інформації в комп’ютерних системах. Документ підкреслює важливість створення комплексної системи захисту інформації (КСЗІ), яка поєднує технічні та організаційні заходи для запобігання несанкціонованому доступу та зниження потенційних ризиків. У контексті хмарних сховищ це означає, що навчальні заклади повинні впроваджувати як технічні засоби захисту (наприклад, шифрування даних, автентифікація користувачів), так і організаційні заходи (розробка політик безпеки, навчання персоналу) для забезпечення безпеки інформації студентів.

Основні аспекти документа:

– постановка проблеми захисту інформації: визначає необхідність створення системи заходів для запобігання реалізації загроз інформації, що обробляється в комп’ютерних системах (КС);

– концепція забезпечення захисту інформації: включає визначення основних загроз, політики безпеки, моделі порушника та комплексів засобів захисту;

– основні принципи забезпечення захисту інформації: охоплюють планування захисту, керування доступом, надання послуг безпеки та гарантій;

– принципи реалізації програмно-технічних засобів: описують функції та механізми захисту, реалізацію комплексу засобів захисту та концепцію диспетчера доступу.

Даний документ наголошує на важливості комплексного підходу до захисту інформації, поєднуючи технічні та організаційні заходи.

НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» надає методологічну базу для визначення вимог до захисту інформації та оцінки захищеності комп'ютерних систем. Документ становлює критерії для оцінки рівня захищеності інформації, що обробляється в КС, від несанкціонованого доступу (НСД). Ключовими положеннями документа є:

– функціональні критерії захищеності: визначають набір послуг безпеки, які повинні бути реалізовані в КС для забезпечення захисту від НСД;

– рівні гарантій безпеки: визначають ступінь впевненості в тому, що реалізовані функції захисту відповідають встановленим вимогам. Рівні гарантій варіюються від Г1 до Г7, де кожен наступний рівень передбачає більш жорсткі вимоги до процесів розробки, впровадження та експлуатації засобів захисту.

Документ також містить рекомендації щодо оцінки відповідності КС встановленим критеріям захищеності та надає основу для сертифікації систем на відповідність вимогам захисту інформації.

Отже хмарні сховища повинні забезпечувати наступні умови:

– конфіденційність: захист даних від несанкціонованого доступу, що може бути досягнуто через шифрування та контроль доступу;

– цілісність: забезпечення точності та повноти даних, наприклад, через механізми контролю версій та перевірки цілісності файлів;

– доступність: гарантія того, що авторизовані користувачі мають доступ до необхідних даних у будь-який час, що вимагає надійної інфраструктури та планів відновлення після збоїв;

– спостережуваність: можливість відстеження дій користувачів та адміністраторів, що дозволяє виявляти та реагувати на потенційні загрози.

НД ТЗІ 2.5-004-99 та НД ТЗІ 1.1-002-99 є фундаментальними для побудови ефективних систем захисту інформації в Україні, забезпечуючи методологічну та нормативну базу для розробки, впровадження та оцінки комплексних систем захисту інформації в комп'ютерних системах. Тож використання даних нормативних документів допоможе розробити та впровадити ефективні заходи захисту інформації при використанні хмарних сховищ для надання студентам доступу до бази знань.

2.1.6 Закон України «Про захист інформації в інформаційно-комунікаційних системах» № 80/94-ВР від 05.07.1994

Закон України «Про захист інформації в інформаційно-комунікаційних системах» №80/94-ВР від 5 липня 1994 року [15] є ключовим нормативно-правовим актом, що регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Його положення мають безпосереднє відношення до захисту даних у хмарних середовищах, оскільки такі середовища є різновидом інформаційно-комунікаційних систем.

Цей закон встановлює правові відносини між володільцями інформації, власниками систем, користувачами та іншими суб'єктами, які беруть участь у процесі зберігання, передачі та обробки інформації. Відповідно до закону, об'єктами захисту в інформаційно-комунікаційних системах є:

– інформація з обмеженим доступом;

– конфіденційна інформація;

– інформація, вимога щодо захисту якої встановлена законом.

У контексті освітнього процесу під ці категорії можуть підпадати навчальні матеріали, персональні дані студентів та викладачів, результати академічних досліджень тощо. Це означає, що при використанні хмарних сервісів для надання доступу студентам до навчальних матеріалів необхідно

забезпечити належний рівень захисту даних, особливо якщо вони містять персональну або іншу конфіденційну інформацію.

Стаття 2 визначає об'єкти захисту в системі, до яких відносяться «інформація, що обробляється в системі», «програмні та технічні засоби» та «засоби захисту інформації». У хмарних середовищах ці об’єкти включають дані користувачів, програмне забезпечення для обробки та зберігання цих даних, а також механізми та протоколи безпеки, що забезпечують їх захист.

Стаття 4 регулює доступ до інформації в системі, встановлюючи, що «доступ до інформації в системі визначається володільцем інформації або уповноваженою ним особою відповідно до закону». Це означає, що в хмарних середовищах користувачі мають право визначати, хто і на яких умовах може отримувати доступ до їхніх даних, що підкреслює важливість налаштування прав доступу та контролю за ними.

Стаття 5 закону визначає, що суб'єктами відносин у сфері захисту інформації є:

– володільці інформації;

– власники систем;

– користувачі та інші особи, які забезпечують захист інформації.

Якщо застосувати цю норму до використання хмарних сховищ у навчальних цілях, то володільцем інформації буде адміністратор (власник інформації), власником системи – провайдер хмарного сервісу (наприклад, *Google* для *Google Drive* або *Microsoft* для *OneDrive*), а користувачами – студенти.

Відповідно до закону, володілець інформації має право визначати порядок доступу до неї та зобов’язаний вживати заходів для її захисту. В контексті хмарних технологій це означає необхідність встановлення правил розмежування прав доступу до файлів, шифрування даних та використання багатофакторної аутентифікації. Наприклад, у разі використання *Google Drive* для зберігання навчальних матеріалів необхідно чітко встановити, хто може переглядати, редагувати чи завантажувати файли.

Закон також накладає зобов’язання на власників інформаційно-комунікаційних систем щодо забезпечення захисту інформації від кіберзагроз, втрати або пошкодження. Це безпосередньо стосується провайдерів хмарних сервісів, які повинні гарантувати збереження інформації, а також можливість її відновлення у випадку втрати. Тому адміністратор, котрий використовує такі сервіси, повинен перевіряти рівень безпеки, що надається обраним хмарним сховищем.

Крім того Закон передбачає, що користувачі інформаційної системи зобов’язані дотримуватися встановлених правил доступу та не допускати дій, що можуть призвести до порушення безпеки інформації. Це означає, що студенти, які отримують доступ до навчальних матеріалів у хмарних сховищах, повинні використовувати надійні паролі, уникати поширення конфіденційної інформації стороннім особам і дотримуватися правил безпеки встановлених адміністратором.

Таким чином, положення Закону України «Про захист інформації в інформаційно-комунікаційних системах» створюють правову основу для захисту даних у хмарних середовищах, визначаючи обов’язки як користувачів, так і провайдерів послуг щодо забезпечення конфіденційності, цілісності та доступності інформації. Це передбачає встановлення чітких правил доступу до навчальних матеріалів, забезпечення шифрування даних, використання багатофакторної аутентифікації та укладання угод із провайдерами хмарних послуг. Відповідальність за безпеку даних розподіляється між адміністратором, провайдерами послуг та користувачами, що вимагає комплексного підходу до організації захисту інформації.

2.2 Постановка задач захисту

Предметом дослідження виступає база знань *Obsidian*, оскільки функціонал, який надає безкоштовна версія є достатнім для проведення

необхідних перевірок. Крім того, обрана база знань є достатньо популярною серед студентів і достатньо простою у використанні.

Obsidian – це персональна база знань і програма для створення нотаток, яка працює з файлами *Markdown*. Дозволяє користувачам створювати внутрішні посилання між нотатками, а потім візуалізувати зв'язки у вигляді графа. Особливістю багатокористувацької роботи з *Obsidian*, без використання корпоративної версії, є те що зміни в файлах в момент введення нових значень, що забезпечує синхронізацію даних у всіх користувачів.

Так як програму буде використовувати багато користувачів важливо забезпечити баланс між зручністю використання та рівнем захисту даних у обраному хмарному середовищі. Дана роботи з інформацією повинна задовольняти наступні вимоги:

– легка доступність до матеріалів;

– розділення прав доступу до матеріалів (читання, редагування);

– багатофакторна аутентифікація;

– зберігання та передавання інформації в зашифрованому вигляді .

Доступ до інформації буде мати значна кількість користувачів, що робить її досить вразливою до стороннього втручання та відкриває доступ до певних каналів витоку інформації. Причини витоку інформації:

– зламання електронної пошти;

– перехоплення передачі даних;

– доступ до комп’ютера зі встановленим клієнтом хмарним сховищем.

При роботі з хмарними сховищами, які використовуються для зберігання та обміну базою знань, необхідно враховувати ряд загроз, які можуть призвести до витоку даних або компрометації інформації. Захист бази знань *Obsidian* при її використанні у хмарному сховищі потребує комплексного підходу, що включає аналіз загроз, визначення ризиків та розробку заходів безпеки. Тож виникає потреба в визначенні основних задач захисту, необхідних для гарантування конфіденційності, цілісності та доступності інформації.

Основними загрозами для безпеки даних у хмарному середовищі при використанні *Obsidian* є:

– злом облікових засобів (злом пошти): доступ до бази знань здійснюється через електронну пошту, що робить її вразливою до атак методом перебору паролів, фішингових атак тощо;

– перехоплення передачі даних: у разі використання незахищених з'єднань зловмисники можуть отримати несанкціонований доступ до переданої інформації;

– несанкціонований доступ до комп’ютера: якщо зловмисник отримує доступ до пристрою користувача, він може отримати контроль над клієнтом хмарного сховища.

– витік даних через неправильне налаштування доступу: відсутність належного розмежування прав користувачів може призвести до несанкціонованого поширення інформації.

– шкідливе програмне забезпечення: віруси, кейлогери та інші загрози можуть спричинити втрату чи компрометацію даних.

Для забезпечення безпеки бази знань *Obsidian* у вибраному хмарному середовищі необхідно вирішити наступні завдання захисту[16].

1) Забезпечення контролю доступу. Одним з основних завдань захисту є обмеження прав доступу до інформації лише для авторизованих користувачів. Це включає:

– використання політики мінімальних привілеїв (розмежування прав доступу): впровадження ролей користувачів (власник, редактор, коментатор, читач) для контролю редагування та перегляду файлів;

– впровадження БФА: застосування додаткового рівня захисту для входу в акаунт користувачів;

– аудит облікових записів та доступу до даних: ведення журналів доступу та змін для виявлення підозрілих дій.

2) Захист даних під час зберігання та передачі. Аби запобігти несанкціонованому доступу до файлів у разі злому хмарного сховища або перехоплення трафіку необхідно реалізувати наступні заходи:

– шифрування під час передачі даних: використання протоколів *TLS/SSL* для захисту трафіку між клієнтом і сервером (забезпечується хмарним сховищем);

– шифрування файлів на сервері: перевірка алгоритмів шифрування (*AES*-256, *AES*-128) які використовує обране хмарне сховище;

– застосування програми *Cryptomator*: забезпечення наскрізного шифрування файлів перед їхнім завантаженням у хмарне середовище, що дозволяє уникнути доступу сторонніх осіб, включаючи самих постачальників хмарних послуг, навіть у разі компрометації хмарного сховища;

– використання *VPN* або захищених мереж: уникнення відкритих *Wi-Fi* без додаткового захисту при підключенні до хмарного сховища;

– захист від атак типу «людина посередині» (*MITM*): забезпечення перевірки сертифікатів *SSL/TLS* (забезпечується обраних хмарним середовищем).

3) Захист облікових записів користувачів. Так як доступ до хмарного сховища здійснюється через облікові записи користувачів, важливо запобігти їх компрометації:

– посилена політика паролів: вимога до використання складних паролів, періодичне їх оновлення;

– двофакторна аутентифікація: вимога обов’язкового застосування додаткового захисту акаунта, задля забезпечення захисту від викрадення паролів;

– виявлення та запобігання фішинговим атакам: проведення додаткових лекцій для навчання користувачів та перевірка джерел електронної пошти.

4) Захист від несанкціонованого фізичного доступу. Доступ до хмарного сховища може бути скомпрометовано у разі злому пристрою користувача. Для цього необхідно:

– захист локального пристрою: використання антивірусного ПЗ, контроль встановлених програм;

– блокування пристрою: встановлення складних паролів для входу в систему та використання біометричних методів автентифікації (за можливості), використання автоматичного блокування пристрою після переходу в режим бездіяльності;

– віддалене блокування пристрою: налаштування можливості видалення даних у разі втрати або крадіжки пристрою (за можливості).

5) Виявлення та реагування на інциденти. Крім зовнішніх атак, необхідно враховувати ризики, пов’язані з діями користувачів:

– моніторинг активності користувачів: впровадження моніторингу активності та виявлення аномальних змін у файлах;

– контроль доступу до чутливих даних: встановлення обмежень для редагування або копіювання користувачами інформації;

– резервне копіювання даних: регулярне створення резервних копій для відновлення у разі компрометації або випадкового видалення;

– регулярний аудит безпеки: перевірка налаштувань хмарного сховища.

Висновок по розділу

Реалізація зазначених заходів дозволить мінімізувати ризики несанкціонованого доступу, втрати або компрометації даних у хмарному сховищі. Комплексний підхід до безпеки включає технічні та організаційні заходи, спрямовані на захист бази знань та забезпечення її безпечного використання в багатокористувацькому середовищі.

3 РОЗРОБКА СИСТЕМИ ЗАХИСТУ

3.1 Аналіз вразливостей захисту хмарного середовища *Google Drive*

Хмарні сервіси зберігання даних, зокрема *Google Drive*, значно підвищують ефективність роботи з інформацією, особливо в освітньому, дослідницькому та корпоративному середовищах.

Широке використання хмарних сервісів зберігання даних, зокрема *Google Drive*, супроводжується зростанням загроз інформаційній безпеці. Тож питання захисту даних, що зберігаються в хмарі, є вкрай актуальним. На основі аналізу рекомендацій *Google, Cloud Security Alliance, OWASP* та звітів провідних компаній з кібербезпеки (зокрема, *Varonis, TrendMicro, Sophos*), можна виокремити низку сучасних підходів, спрямованих на підвищення рівня безпеки даних, що зберігаються в *Google Drive* [17,18].

Однією з ключових рекомендацій є впровадження багатофакторної автентифікації [19]. Це дозволяє захистити обліковий запис навіть у разі компрометації основного пароля. Найефективнішими рішеннями для облікових записів, що мають доступ до конфіденційних даних, є обов’язкове застосування БФА. У межах *Google Workspace* підтримується як автентифікація за допомогою одноразових кодів, так і апаратні ключі (*FIDO2*-сумісні), що дозволяють ефективно протидіяти фішинговим атакам. Адміністративна консоль *Google* дозволяє централізовано контролювати стан БФА у всій організації, що є критично важливим у навчальних та освітніх структурах із великою кількістю користувачів.

Іншим не менш важливим напрямом є керування доступом до даних. Практика впровадження принципу найменших привілеїв (*PoLP*) передбачає, що кожен користувач отримує лише ті права, які необхідні для виконання його завдань. Це дозволяє уникнути як навмисного, так і випадкового втручання у важливі документи. *Google Drive* дозволяє налаштовувати гнучкі рівні доступу, від повного редагування до перегляду без коментарів. Особливу увагу слід

приділяти вимкненню можливості доступу за загальнодоступним посиланням («*Anyone with the link*»), що є одним із найпоширеніших векторів витоку інформації.

Особливої уваги заслуговує концепція клієнтського шифрування (*Client-Side Encryption* (*CSE*)). На відміну від серверного шифрування, яке виконується вже після завантаження файлів на сервер *Google* (з використанням *TLS* при передачі та *AES*-256 при зберіганні), клієнтське шифрування передбачає захист даних ще до їх передачі у хмару. У такому випадку шифрування й дешифрування здійснюються виключно на стороні клієнта, а ключі залишаються недоступними навіть для провайдера. Це гарантує максимальний рівень конфіденційності. Серед рішень, що дозволяють реалізувати клієнтське шифрування для *Google Drive*, було обрано *Cryptomator* – безкоштовний програмний інструмент з відкритим кодом, який створює віртуальний зашифрований диск. Усі файли, що додаються до нього, автоматично шифруються, а контейнер можна синхронізувати із *Google Drive* без втрати захисту. Для корпоративних користувачів *Google* також пропонує *Google Workspace Client-Side Encryption* (*CSE*) – рішення, що дозволяє зберігати ключі в незалежній інфраструктурі: власному сервері або через партнера (наприклад, *Thales* чи *FlowCrypt*). Таким чином, навіть якщо хмарний акаунт буде скомпрометовано, зловмисник не зможе отримати доступ до шифрованого вмісту без клієнтського ключа.

Крім технічних заходів, таких як автентифікація та шифрування, велике значення має постійний моніторинг активності. Завдяки журналам подій (*Audit Logs*), що підтримуються *Google Workspace*, адміністратори можуть отримувати повну інформацію про зміни в документах, надання доступів, підозрілу активність тощо. Це дозволяє вчасно виявляти аномалії у роботі користувачів або зловмисні дії. При інтеграції з зовнішніми системами моніторингу (наприклад, *SIEM*-рішеннями) забезпечується автоматизоване виявлення інцидентів.

Наступним елементом побудови безпечного хмарного середовища є контроль над кінцевими пристроями. Інструменти *Endpoint Management*

дозволяють обмежити доступ лише до авторизованих пристроїв, встановити політики шифрування локального сховища (наприклад, через *BitLocker* або *FileVault*), а також забезпечити можливість віддаленого очищення даних у разі втрати пристрою. Це особливо важливо в умовах використання персональних комп'ютерів або мобільних телефонів у навчальному процесі.

Окреме місце у сучасному підході до безпеки займає стратегія резервного копіювання. Сервіси *Google* забезпечують певний рівень збереження даних, проте не захищають від випадкового видалення або навмисного пошкодження з боку користувача. Тому критично важливим є створення регулярних офлайн копій ключових файлів. Додатково в корпоративних середовищах рекомендується впроваджувати політики класифікації даних із подальшим застосуванням інструментів *Data Loss Prevention* (*DLP*), які автоматично виявляють конфіденційну інформацію та не дозволяють її несанкціонований експорт або пересилання.

Останнім, але не менш важливим, є фактор користувача. Людські помилки, нехтування правилами безпеки, використання простих паролів або натискання на фішингові посилання – усе це значно підвищує ризик витоку інформації. Тому систематичне навчання користувачів – обов'язкова частина комплексного захисту хмарного середовища. Доцільним є проведення інструктажів, створення навчальних матеріалів, запуск внутрішніх кампаній із підвищення цифрової грамотності та залучення користувачів до створення безпечного інформаційного простору.

Таким чином, комплексний підхід до безпеки *Google Drive* охоплює технічні, адміністративні та освітні заходи. Він передбачає не лише налаштування стандартних механізмів захисту, але й використання сторонніх інструментів, таких як *Cryptomator*, для підвищення рівня конфіденційності, а також впровадження політик управління ризиками й навчання кінцевих користувачів.

3.2 Налаштування хмарного середовища

На основі викладених рекомендацій і сучасних практик в подальшому буде реалізовано практичну частину захисту даних у хмарному середовищі *Google Drive* [20] – шляхом налаштування доступу до бази знань та впровадження клієнтського шифрування за допомогою *Cryptomator*. Це дозволяє автоматично оновлювати локальні копії файлів та синхронізувати зміни з хмарною версією бази знань. Такий підхід дає змогу працювати з файлами будь-якого формату (а не лише з документами, що підтримуються компанією *Google*) із практично миттєвою синхронізацією.

Оскільки доступ до бази знань *Obsidian* здійснюється безпосередньо через хмарне сховище *Google Drive*, необхідно налаштувати доступ до нього на кожному пристрої. Для цього спочатку завантажуємо клієнт *Google Drive* з офіційного сайту *Google* (рис. 3.1).

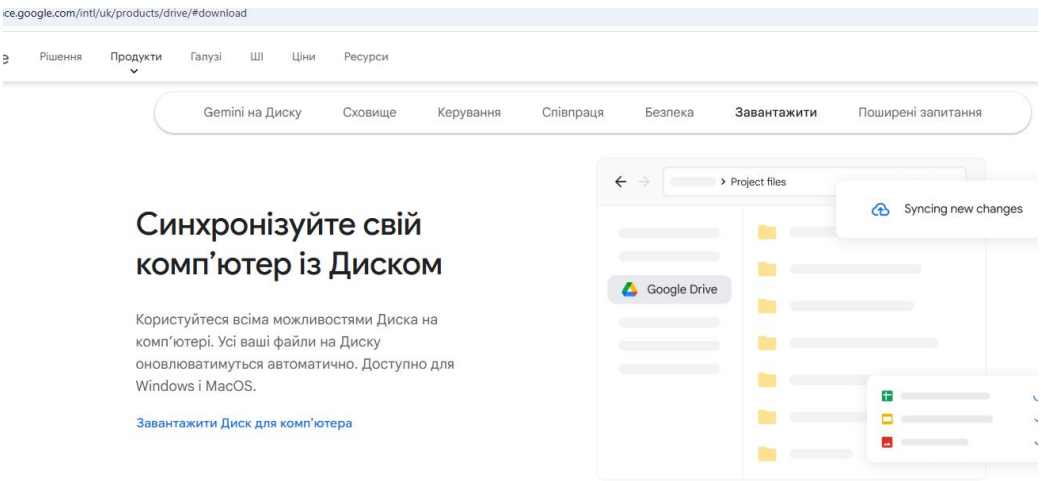

Рисунок 3.1 – Завантаження *Google Drive* з офіційного сайту

Після встановлення та підключення акаунту адміністратора, виконується завантаження бази знань, яка містить файли підготовки до ЄДКІ (рис. 3.2).

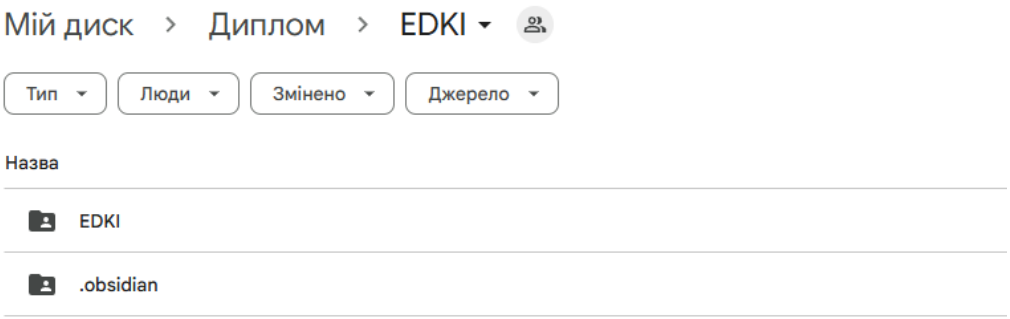

Рисунок 3.2 – Завантаження бази знань на *Google Drive*

Далі аби забезпечити доступність інформації та не порушити її цілісність встановлюємо «обмежений доступ» до папки, де зберігається база знань (рис. 3.3). За допомогою системи керування доступом поштові акаунти довірених користувачів отримують відповідні права (рис. 3.4):

– студенти, які активно беруть участь у навчальному процесі, отримують право редагування;

– студенти, що нерегулярно відвідують заняття, мають можливість коментування для внесення пропозицій та уточнень, які будуть розглядатися редакторами;

– користувачі з мінімальною активністю отримують лише права перегляду, що запобігає випадковому видаленню або внесенню некоректної інформації.

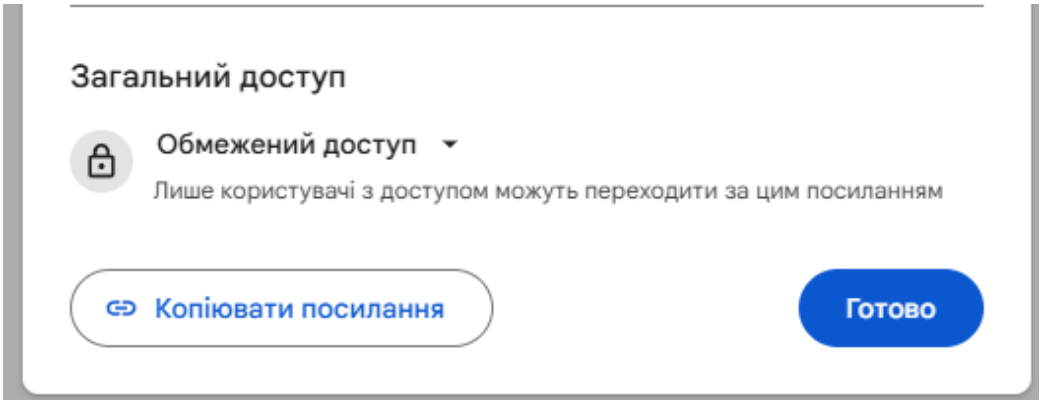

Рисунок 3.3 – Налаштування обмеженого доступу

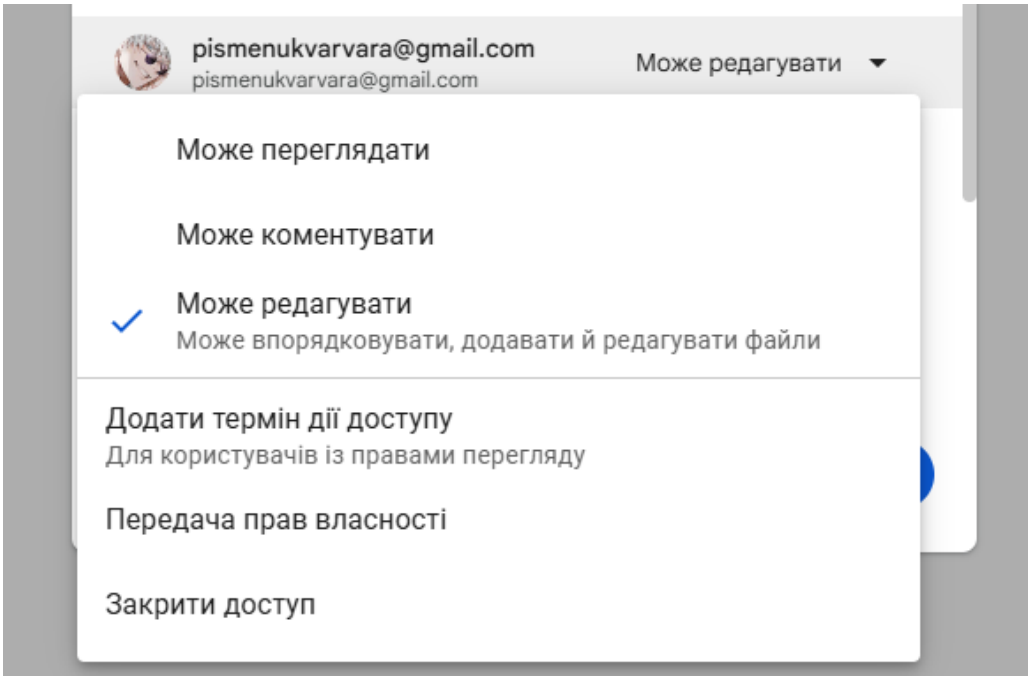

Рисунок 3.4 – Надання доступу довіреним користувачам

Окрім цього, адміністратор створює у себе окрему папку з резервною копією бази знань, яку періодично оновлює. Це дозволяє відновити дані у разі непередбачуваних ситуацій, таких як випадкове видалення файлів або несанкціоновані зміни.

3.3 Налаштування персонального комп’ютера для роботи з хмарним середовищем

Для запобігання витоку даних та порушення їхньої цілісності, які можуть виникнути внаслідок злому акаунту користувача або отримання зловмисником доступу до пристрою, на якому встановлено клієнт *Google Drive* із доступом до бази знань, було впроваджено додатковий рівень захисту. А саме використано програму *Cryptomator*, яка забезпечує локальне шифрування файлів перед їхнім завантаженням у хмарне сховище. Це дозволяє зробити дані недоступними для сторонніх осіб навіть у разі несанкціонованого доступу до облікового запису або пристрою користувача.

Спочатку необхідно завантажити *Cryptomator* із офіційного сайту розробників та встановити програму на пристрій (рис. 3.5, 3.6).

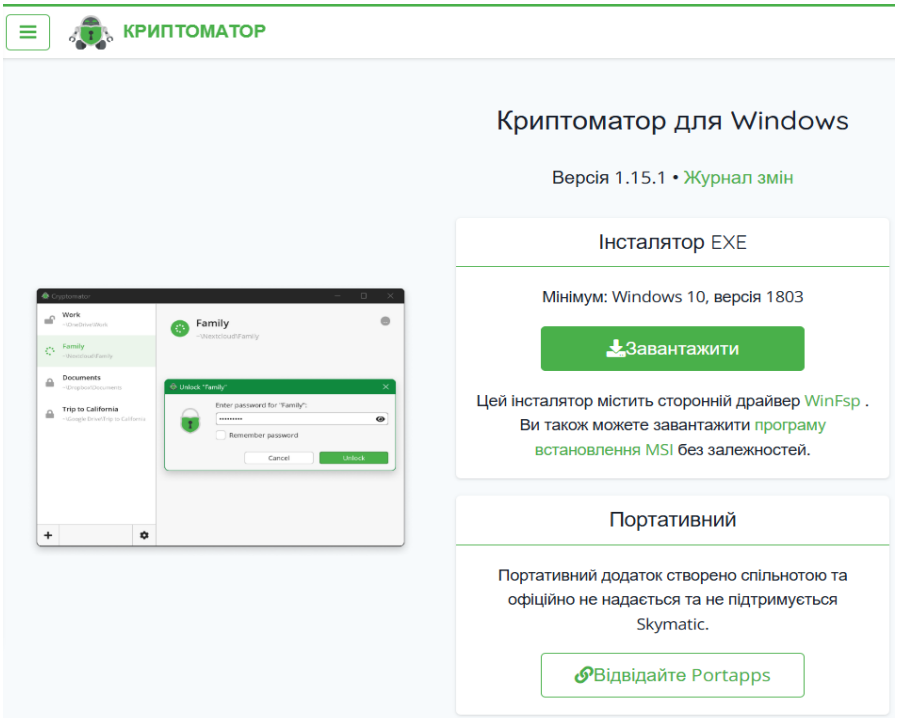

Рисунок 3.5 – Завантаження *Cryptomator*

Рисунок 3.6 – Встановлення програми

Після успішного встановлення необхідно створити контейнер (віртуальний диск), у якому буде зберігатися база знань. Для цього відкриваємо програму *Cryptomator*, натискаємо «Додати» та вводимо назву для контейнеру, котрий буде створено безпосередньо у хмарному сховищі (рис. 3.7).

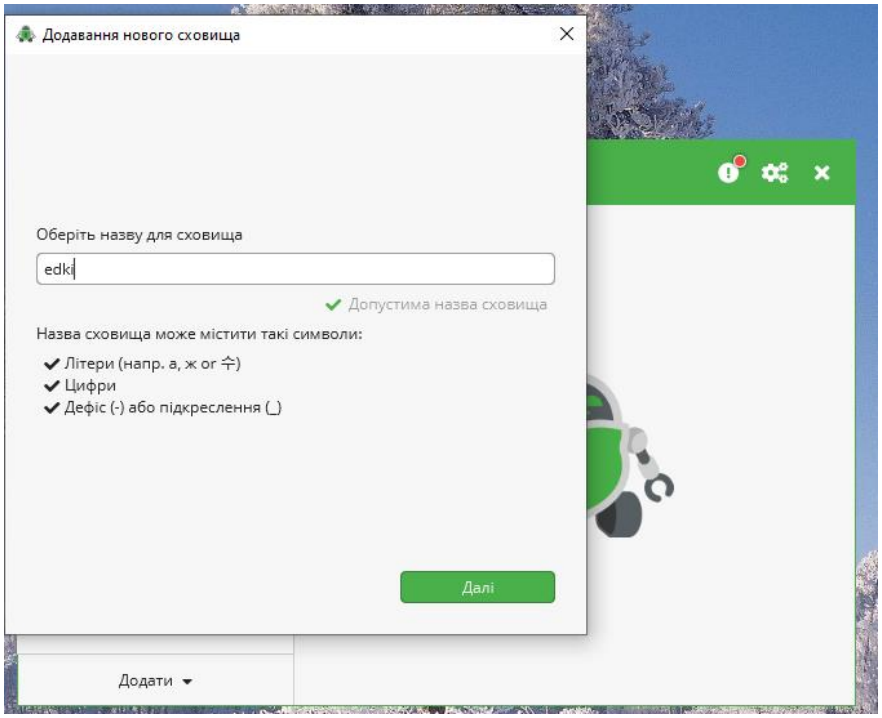

Рисунок 3.7 – Створення захищеного контейнера

Для створеного контейнеру встановлюється складний пароль, який повинен містити спеціальні символи, цифри та літери латинського алфавіту. Це значно ускладнює можливість злому пароля шляхом підбору або використання інформації про користувача (рис. 3.8).

Оскільки існує ризик втрати або забуття пароля, рекомендовано створити ключ відновлення, який дозволить розблокувати контейнер у разі його втрати. Для забезпечення безпеки ключ відновлення має зберігатися окремо, наприклад, на флеш-накопичувачі, доступ до якого має лише адміністратор.

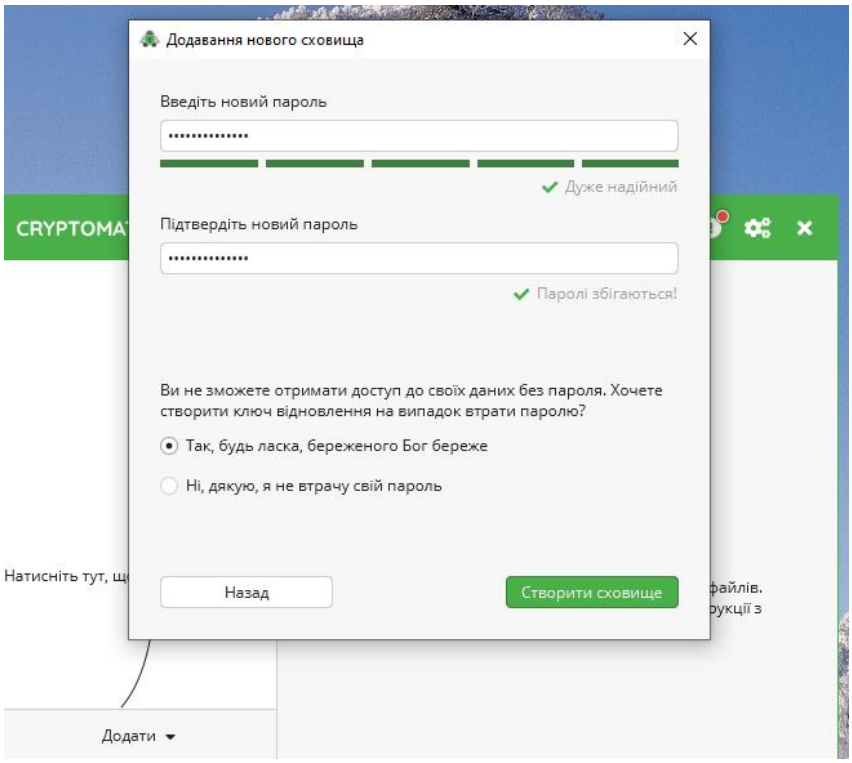

Рисунок 3.8 – Встановлення надійного паролю для контейнера

Після створення контейнера програма автоматично генерує зашифровану директорію, доступ до якої можливий лише після введення правильного пароля (рис. 3.9). Користувачі, які мають відповідні права, можуть працювати з файлами у захищеному середовищі, не ризикуючи їхнім несанкціонованим розголошенням.

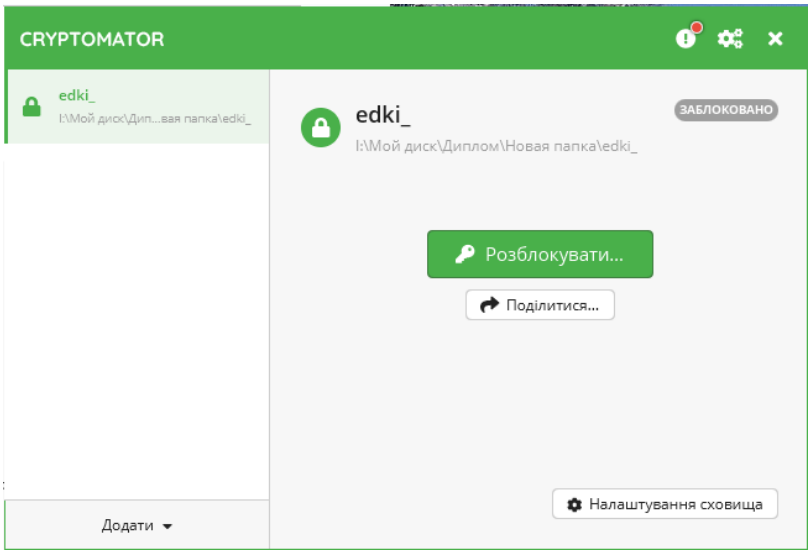

Рисунок 3.9 – Зашифровану директорію успішно створено

Після виконання всіх вищезазначених дій процес налаштування ПК для безпечної роботи з хмарним середовищем можна вважати завершеним. Даний підхід дозволяє не тільки працювати з базою знань у хмарному сховищі, але й забезпечує високий рівень конфіденційності та захисту даних.

Висновок по розділу

Аналіз вразливостей *Google Drive* є відсутність наскрізного шифрування, що може створювати певні ризики для збереження конфіденційних даних. Для усунення цього недоліку було запропоновано використання *Cryptomator* – програми для локального шифрування файлів перед їх завантаженням у хмарне сховище. Це забезпечує додатковий рівень захисту та гарантує, що навіть у разі витоку даних вони залишатимуться недоступними для сторонніх осіб.

Таким чином, запропоноване рішення поєднує в собі зручність і функціональність *Google Drive* із додатковим захистом через шифрування *Cryptomator*, що значно підвищує рівень безпеки збережених даних.

4 ТЕСТУВАННЯ СИСТЕМИ

4.1 Тестування системи для користувача з максимальним рівнем доступу

Після успішного налаштування хмарного середовища та впровадження засобів захисту необхідно перевірити ефективність реалізованих механізмів безпеки та коректність роботи системи.

На першому етапі тестування перевіряється функціональність системи у випадку, коли всі операції виконує користувач із максимальними правами доступу. Це може бути адміністратор або користувач із правами редактора, який має можливість розблоковувати зашифровані дані та редагувати файли в базі знань.

Для початку користувач відкриває папку на локальному диску, у якій зберігається зашифрований контейнер із базою знань. У цій папці знаходиться файл контейнера «*Vault*», який необхідно запустити за допомогою програми *Cryptomator*. Після запуску програма ідентифікує зашифроване сховище та запитує пароль для його розблокування (рис. 4.1 – 4.3).

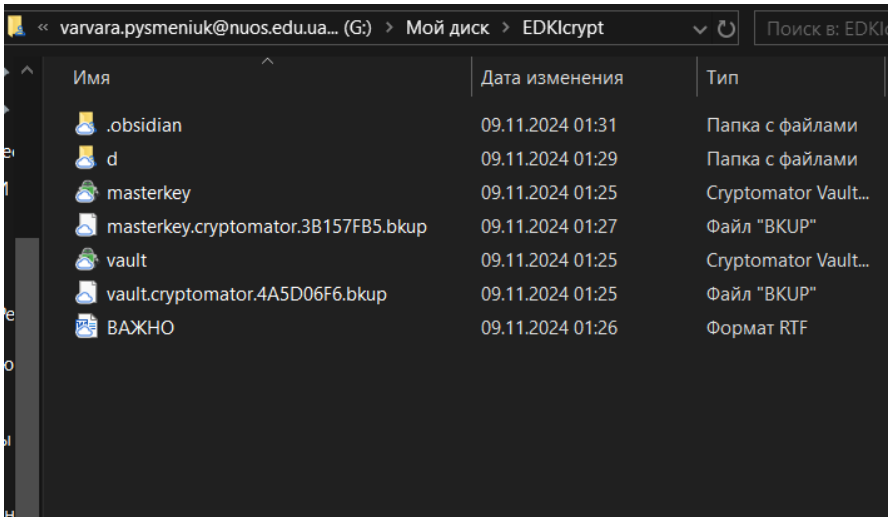

Рисунок 4.1 – Зашифрована папка з базою знань

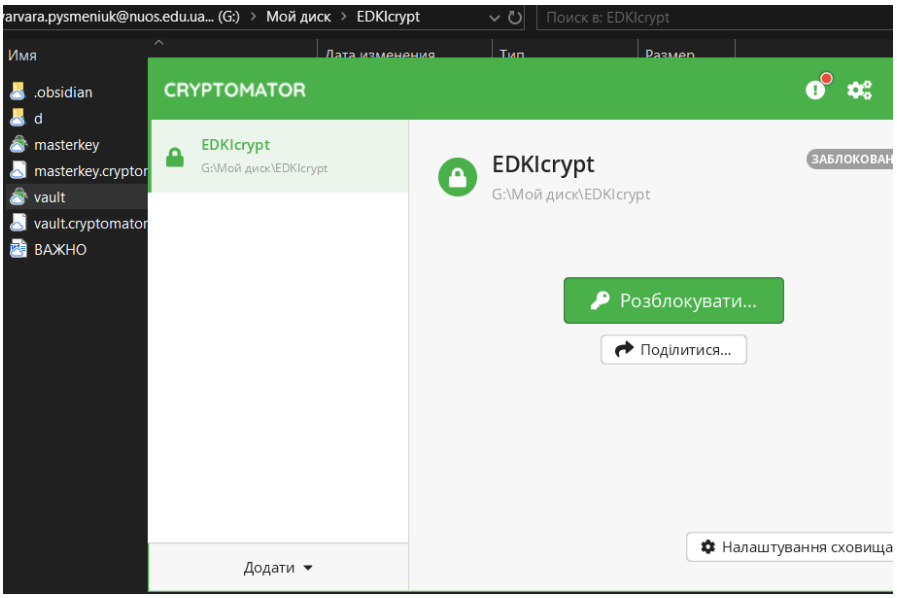

Рисунок 4.2 – Ідентифікація зашифрованого сховища

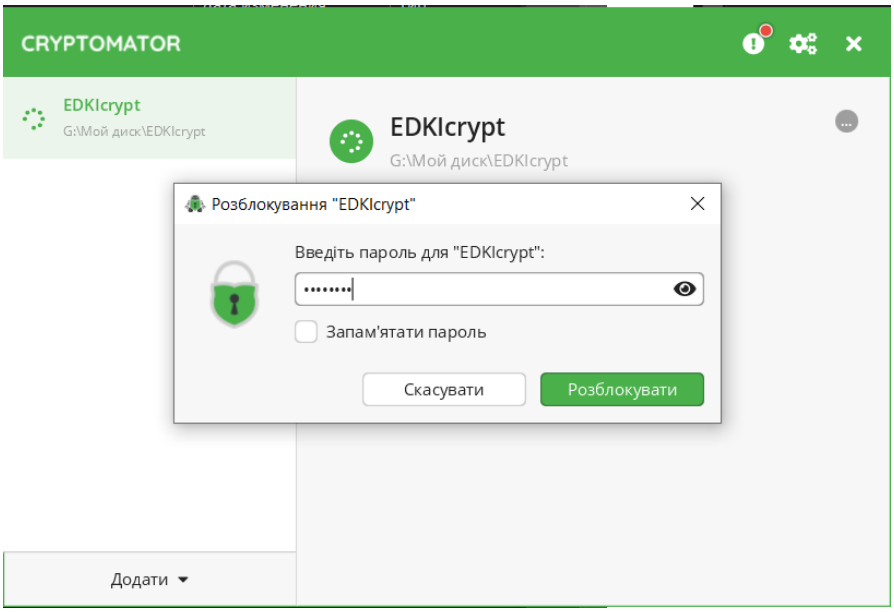

Рисунок 4.3 – Введення паролю для розблокування сховища

Після успішного введення пароля *Cryptomator* пропонує змонтувати розблокований контейнер як окремий віртуальний диск. Для цього необхідно натиснути кнопку «Розгорнути диск», після чого користувач отримує повний доступ до файлів бази знань (рис. 4.4).

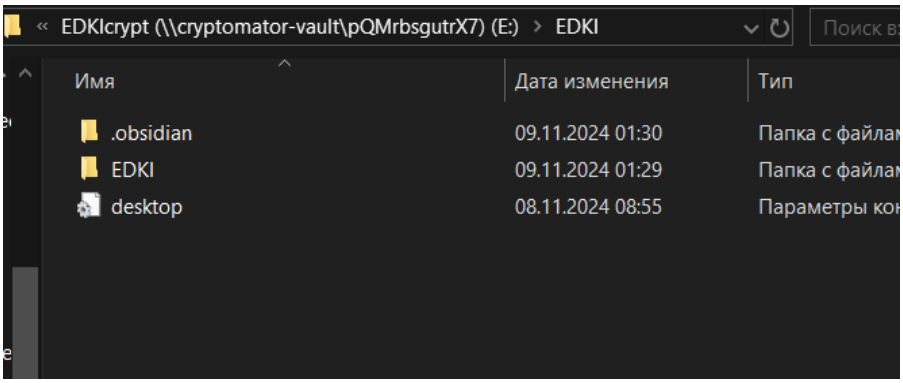

Рисунок 4.5 – Доступ до файлів успішно отримано

Далі запускається програма *Obsidian*, яка використовується для роботи з базою знань. У налаштуваннях програми користувач обирає шлях до змонтованого контейнера (рис. 4.6). Після цього всі файли стають доступними для перегляду, редагування та синхронізації.

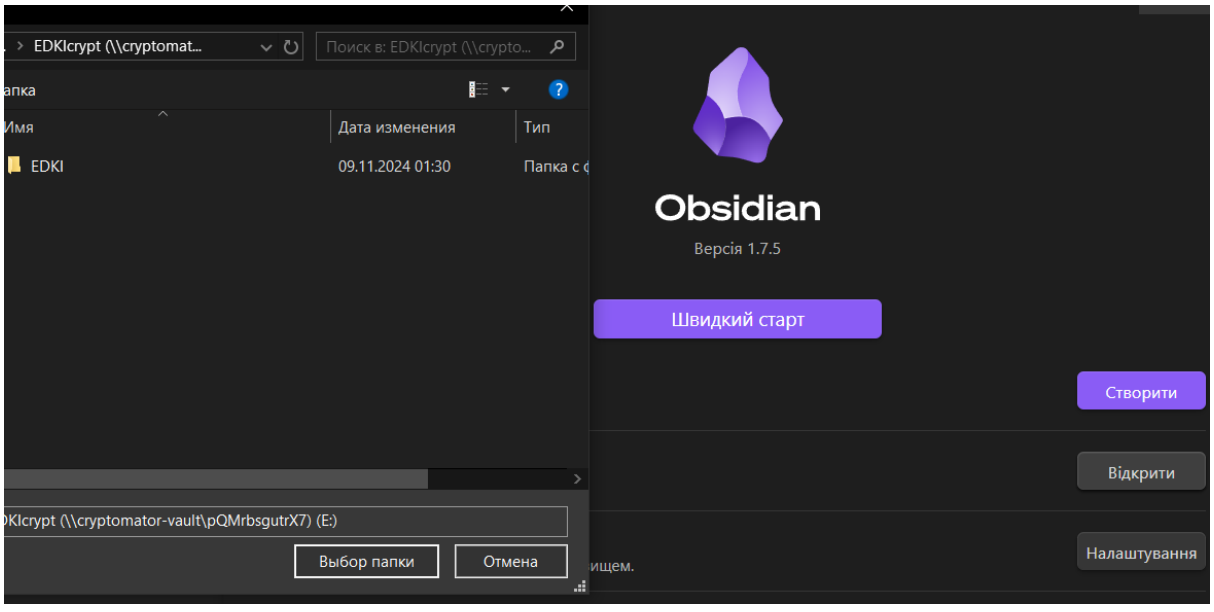

Рисунок 4.6 – Запуск бази знань в програмі *Obsidian*

Як показано на рис. 4.7, система успішно працює, а користувач із відповідними правами отримує доступ до інформації без обмежень.

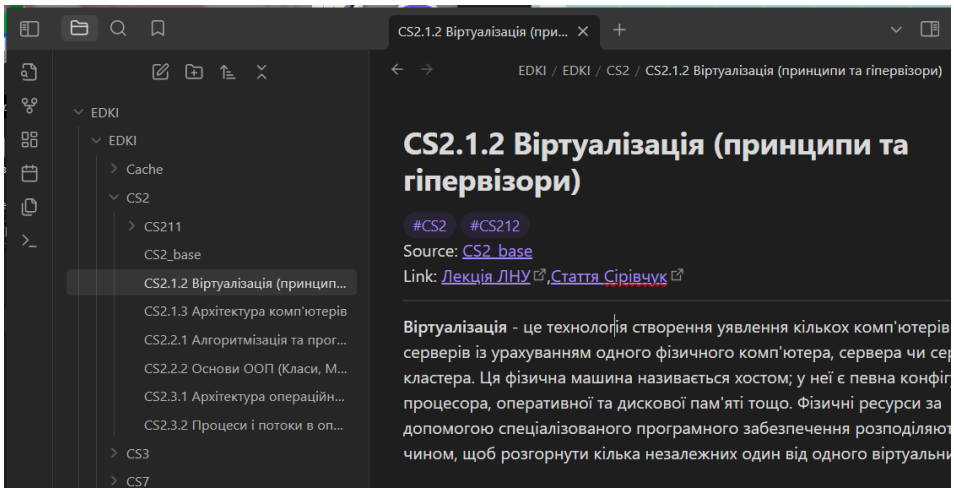

Рисунок 4.7 – База знань успішно відкрита

4.2 Одночасна робота кількох користувачів

Наступний етап тестування спрямований на перевірку коректності роботи системи в умовах одночасного використання бази знань кількома користувачами. Це дозволить оцінити, як синхронізуються зміни між користувачами та чи виникають можливі конфлікти під час редагування даних.

Для початку користувач із правами редактора або адміністратор вносить зміни до бази знань. Зокрема, створюється нова тека під назвою «Перевірка» та додається новий нотаток «Тестування роботи системи» (рис. 4.8).

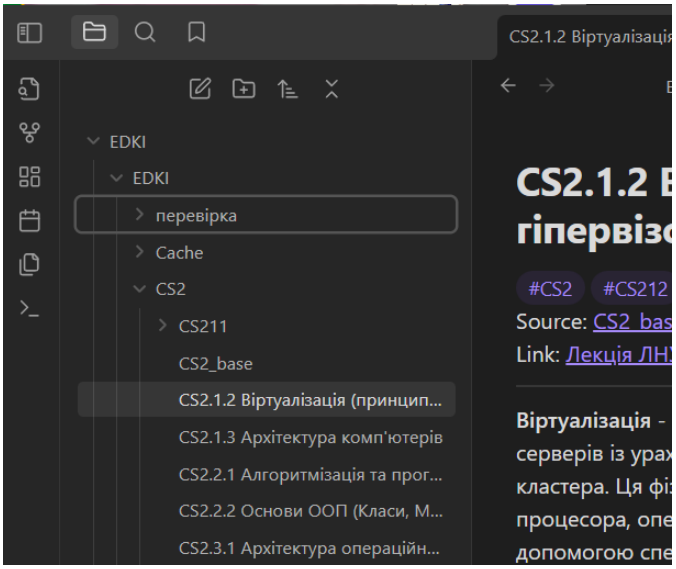

Рисунок 4.8 – Перевірка роботи системи

Як показано на рис. 4.9, нова тека успішно створена та відображається у структурі папок.

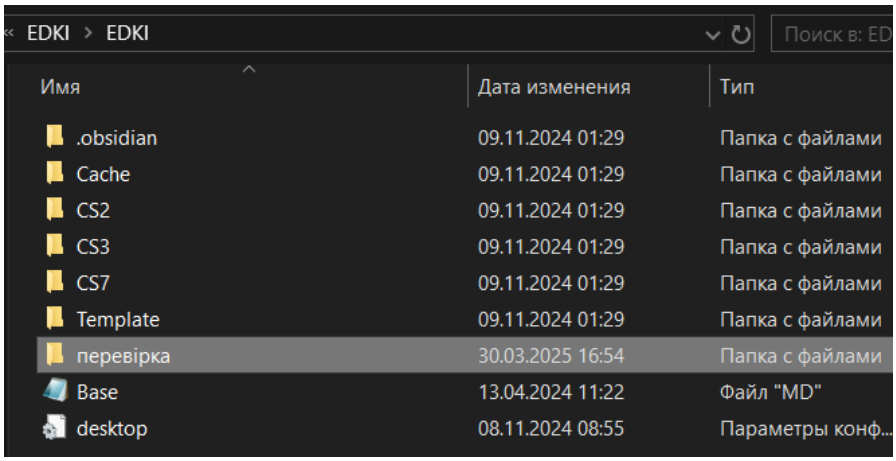

Рисунок 4.9 – Нова тека успішно створена

Далі база знань відкривається з акаунту іншого користувача, який має доступ до папки. У нього також коректно відображаються всі внесені зміни: нова тека та нотаток «Тестування роботи системи» (рис. 4.10).

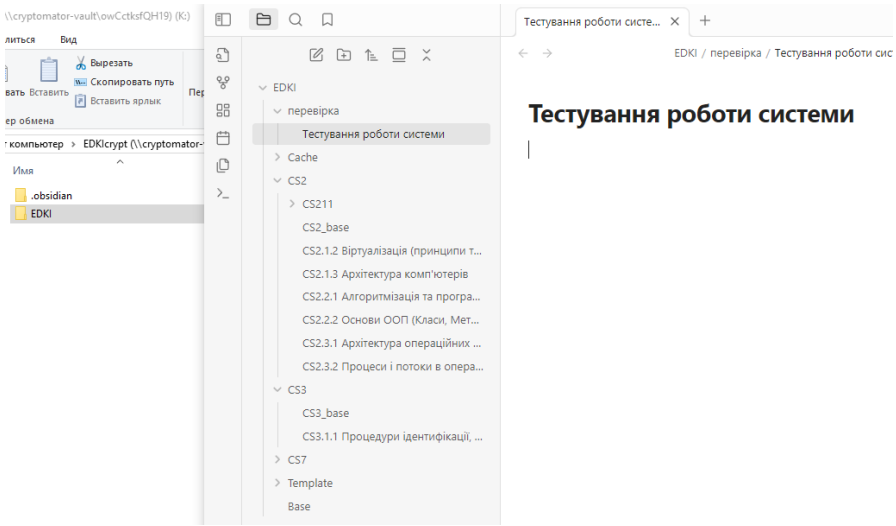

Рисунок 4.10 – Запуск бази знань з іншого акаунта

Варто зазначити, що процес синхронізації файлів між користувачами відбувається практично миттєво, однак для повного оновлення структури бази знань у програмі *Obsidian* іншим користувачам може знадобитися

перезавантаження застосунку або примусове оновлення вмісту сховища. Це дозволяє уникнути потенційних розбіжностей у відображенні даних та забезпечує коректну спільну роботу з інформацією.

4.3 Користувачі з рівнем доступу читача та коментатора

На цьому етапі тестування перевіряється функціональність системи для користувачів, які мають обмежені права доступу – читача або коментатора. Це дозволяє оцінити, наскільки ефективно реалізовано захист від несанкціонованих змін та забезпечено збереження цілісності бази знань.

При спробі розблокувати захищене сховище користувачем із правами читача або коментатора виникає помилка (рис. 4.11). Це пояснюється тим, що такі користувачі не мають прав для редагування контейнера, а доступ до його вмісту можливий лише у режимі перегляду.

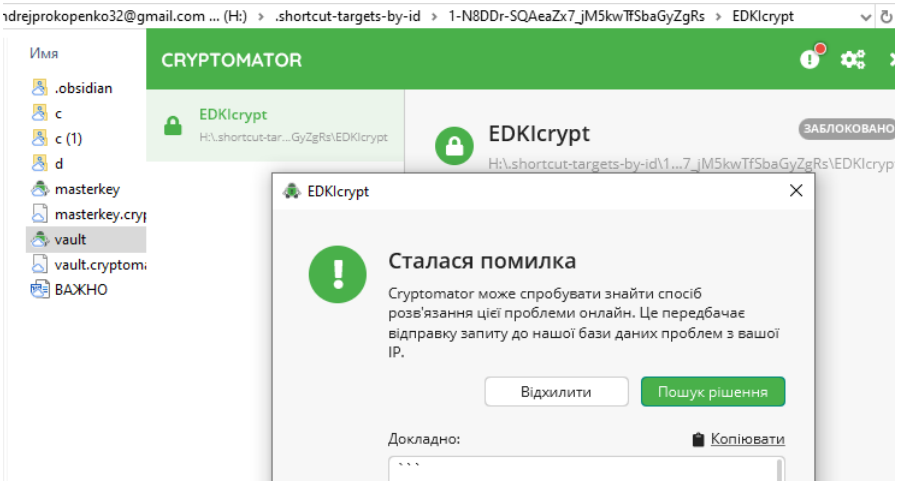

Рисунок 4.11 – Помилка при спробі розблокувати сховище

Для того щоб переглядати файли в захищеному сховищі, користувачам із відповідними правами необхідно в налаштуваннях *Cryptomator* вказати параметр «Тільки для перегляду» (рис. 4.12). Цей параметр накладає додаткові обмеження, що унеможливлюють будь-які зміни у файлах, навіть випадкові. Таким чином, захист реалізовано на двох рівнях: хмарне сховище *Google Drive*, яке розмежовує

права доступу та не дозволяє користувачам з обмеженими правами вносити зміни; програма *Cryptomator*, яка забезпечує додаткове шифрування файлів, не даючи змоги несанкціоновано їх модифікувати.

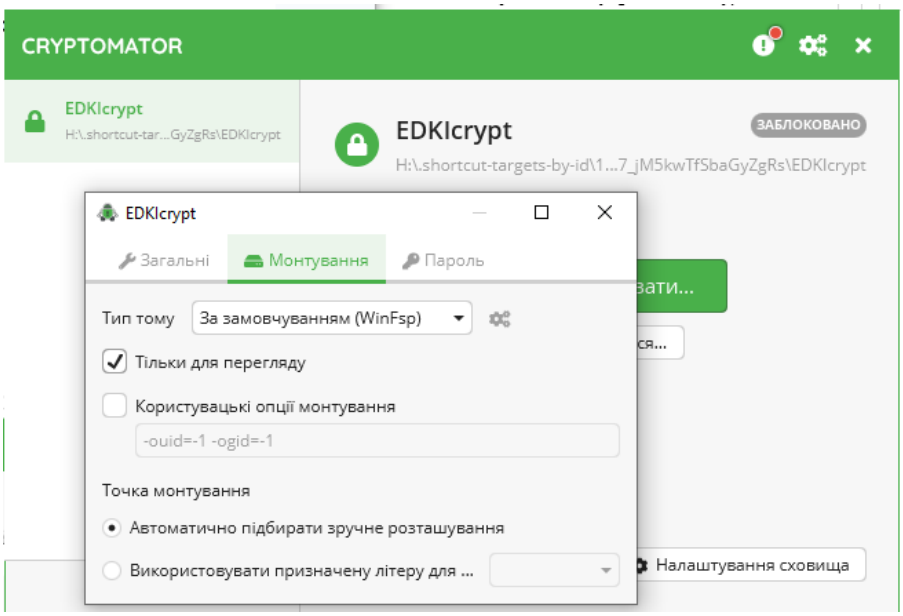

Рисунок 4.12 – Налаштування параметрів сховища

При спробі користувача з рівнем доступу читача скопіювати файли бази знань у інше місце або завантажити власні файли до контейнера виникає помилка (рис. 4.13). Це гарантує збереження оригінальної структури даних та запобігає їх випадковому видаленню або підміні.

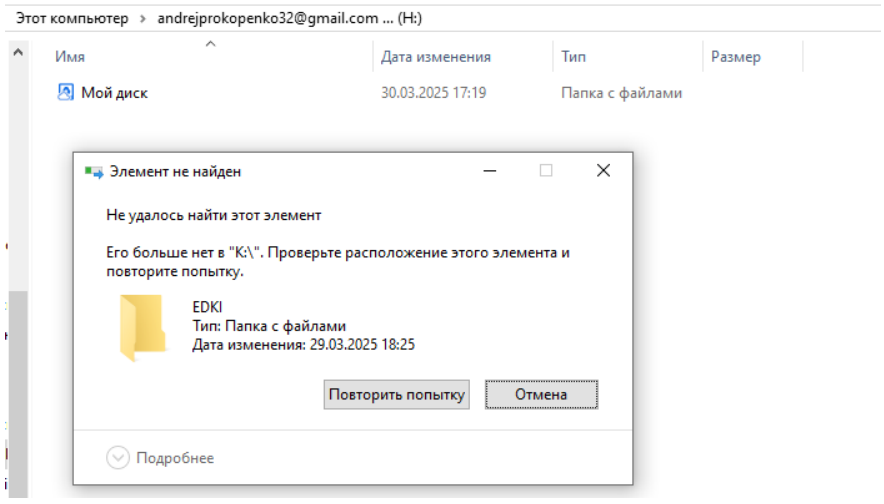

Рисунок 4.13 – Спроба скопіювати файл без відповідних прав доступу

Крім того, як показано на рис. 4.14, користувачі без прав редактора не можуть редагувати файли безпосередньо в базі знань. При спробі внесення змін та їх збереження система видає відповідне повідомлення про помилку. Це підтверджує, що обмеження доступу налаштовані коректно та ефективно виконують свою функцію.

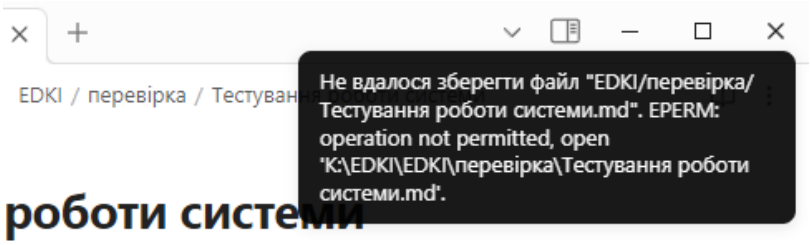

Рисунок 4.14 – Спроба зробити зміни до змісту без відповідних прав доступу

4.4 Невідомий ключ розшифрування контейнера

У цьому тестуванні перевіряється безпека системи у випадку, якщо зловмисник отримає доступ до акаунту студента та, відповідно, до папки з базою знань у хмарному сховищі.

Як показано на рис. 4.15, 4.16 без знання пароля для розблокування контейнера, вміст папки виглядає як набір зашифрованих файлів, що не мають зрозумілого змісту. Усі файли у сховищі перетворюються на невпізнавані, їхні назви змінені, а самі дані представлені у закодованому вигляді.

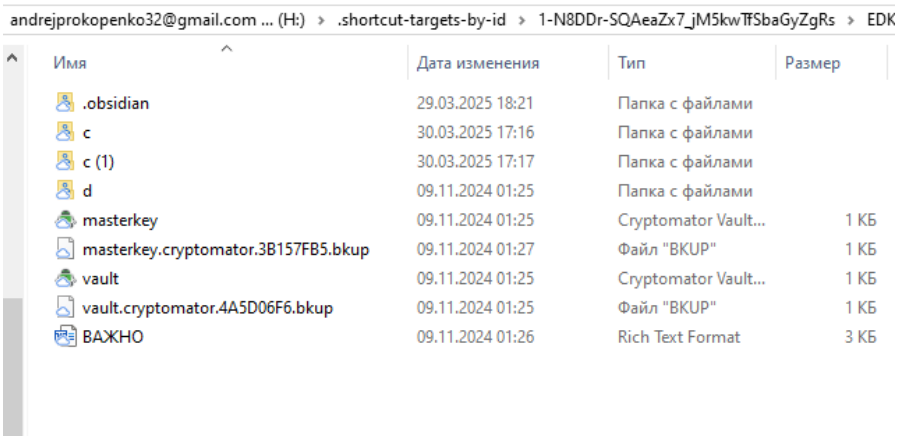

Рисунок 4.15 – Вигляд вмісту папки без розблокування

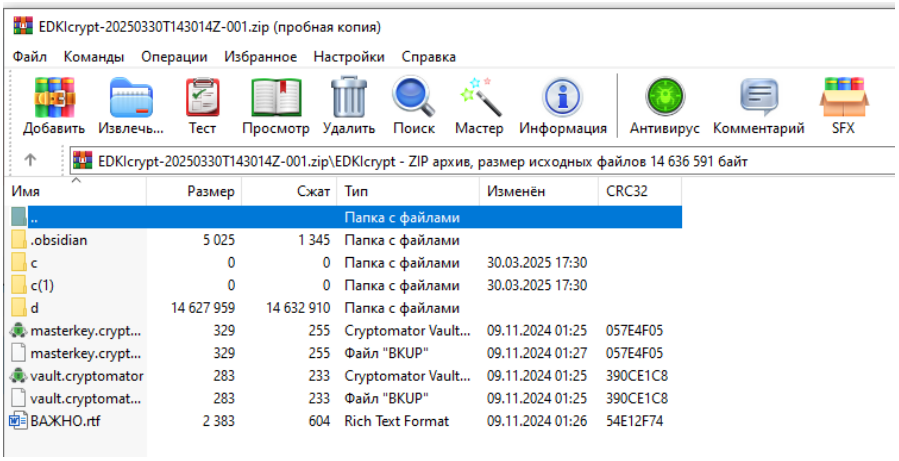

Рисунок 4.16 – Вміст папки при завантаженні на ПК без введення паролю для розблокування

Навіть якщо зловмисник спробує відкрити файли бази знань за допомогою програми *Obsidian*, він не отримає доступу до корисної інформації. Замість структурованих текстів і нотаток, у програмі відобразяться лише беззмістовні символи (рис. 4.17).

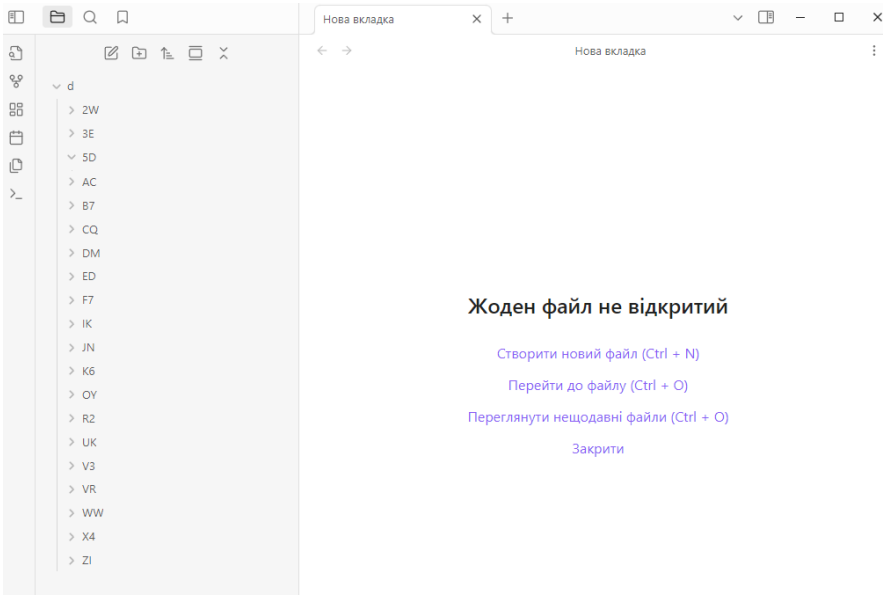

Рисунок 4.17 – Вміст бази знань без розблокування

Проведене тестування підтвердило ефективність реалізованих механізмів захисту бази знань, а також коректність роботи системи в різних сценаріях використання.

Висновок до розділу

Було встановлено, що користувачі з максимальними правами доступу (адміністратори та редактори) можуть безперешкодно працювати з базою знань: розблоковувати зашифроване сховище, редагувати файли та синхронізувати зміни між пристроями. Одночасна робота кількох користувачів проходить коректно, хоча для оновлення змін у програмі *Obsidian* може знадобитися перезавантаження або примусове оновлення сховища.

Система також забезпечує надійний захист даних від користувачів із обмеженим рівнем доступу (читачів та коментаторів). Вони можуть лише переглядати інформацію, але не мають можливості змінювати, копіювати чи видаляти файли, що гарантує збереження цілісності бази знань.

Окрему увагу було приділено питанню безпеки у разі компрометації облікового запису студента. Навіть якщо зловмисник отримає доступ до

хмарного сховища, без відповідного ключа шифрування він не зможе розшифрувати файли, оскільки весь вміст контейнера залишається у зашифрованому вигляді.

Таким чином, використання *Cryptomator* у поєднанні з хмарним сховищем забезпечує високий рівень безпеки даних, запобігає несанкціонованому доступу та дозволяє ефективно організувати спільну роботу над базою знань.

ВИСНОВКИ

В даній дипломній роботі було проведено дослідження захисту даних у хмарних середовищах. Було проаналізовано існуючі загрози витоку інформації, розглянуто методи шифрування та засоби безпеки для захисту користувацьких даних у хмарних сервісах.

Під час дослідження встановлено, що одним із ключових факторів забезпечення безпеки даних є наскрізне шифрування, яке гарантує, що навіть постачальник хмарного сховища не матиме доступу до інформації користувача. Було визначено, що такі сервіси, як *Google Drive*, *Dropbox* і *OneDrive*, не забезпечують повного наскрізного шифрування, що може призвести до потенційних загроз. Натомість *MEGA* пропонує наскрізне шифрування, однак має обмеження щодо функціональності спільного доступу.

У процесі роботи розглянуто програмне рішення *Cryptomator*, яке дозволяє локальне шифрування файлів перед їх передачею в хмарне сховище. Це рішення забезпечує додатковий рівень захисту та підвищує конфіденційність користувацьких даних. Впровадження *Cryptomator* у робочий процес дозволяє використовувати популярні хмарні сервіси без ризику компрометації інформації.

Окрім цього, було проведено тестування системи захисту даних, яке підтвердило ефективність застосованих методів безпеки. Аналіз отриманих результатів засвідчив, що поєднання зручності використання хмарних сервісів із додатковим шифруванням забезпечує оптимальний баланс між функціональністю та конфіденційністю даних.

Таким чином, у дипломній роботі було сформовано рекомендації щодо вибору хмарних сховищ та засобів шифрування залежно від потреб користувачів. Отримані результати можуть бути використані для підвищення рівня безпеки даних при роботі з хмарними сервісами як в особистих, так і корпоративних цілях.

ПЕРЕЛІК ПОСИЛАНЬ

1. *17 Security Risks of Cloud Computing in 2025 URL: https://www.sentinelone.com/cybersecurity-101/cloud-security/security-risks-of-cloud-computing/*

2. *Cyberattacks and Security of Cloud Computing: A Complete Guideline URL: https://www.mdpi.com/2073-8994/15/11/1981*

3. *Network communications interception URL: https://licelus.com/resources/guide-to-mobile-application-protection/threats/network-communications-interception*

4. *What is Google Drive? URL: https://www.techtarget.com/searchmobilecomputing/definition/Google-Drive*

5. *What is Dropbox? URL: https://www.dropbox.com/en_GB/features*

6. *Overview of OneDrive in Microsoft 365 URL: https://learn.microsoft.com/en-us/sharepoint/onedrive-overview*

7. *MEGA URL: https://mega.io/storage*

8. *Dropbox vs Google Drive vs OneDrive: Comparing the Big Three in 2025 URL: https://www.cloudwards.net/dropbox-vs-google-drive-vs-onedrive/*

9. *Cryptomator Documentation URL: https://docs.cryptomator.org/*

10. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI *URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text*

11. Про хмарні послуги: Закон України від 17.02.2022 № 2075-IX *URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text*

12. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги. *URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_iec_27001_2023.pdf*

13. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. *URL: https://tzi.com.ua/downloads/2.5-004-99.pdf*

14. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого *URL: https://tzi.com.ua/downloads/1.1-002-99.pdf*

15. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР *URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text*

16 Щерба М.О. Дослідження методів забезпечення інформаційної безпеки у хмарному середовищі // Міжнародна науково-технічна конференція «Інформаційно-комунікаційні технології та кібербезпека (ІКТК-2023)). - 2023. – С. 206-207. *URL: https://openarchive.nure.ua/server/api/core/bitstreams/5a8a2078-9d6f-48c8-ac2f-74daf4156bec/content?utm_source=chatgpt.com*

17. *Cloud Security Alliance (CSA) – Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 URL: https://anskaffelser.no/sites/default/files/csa_security_guidance_v4.0.pdf?utm_source=chatgpt.com*

18. *Data Protection Guide: How To Secure Google Drive for Your Business URL: https://www.varonis.com/blog/how-to-secure-google-drive*

19. *Enhance Google Drive Security: 7 Best Practices To Follow URL: https://www.zluri.com/blog/google-drive-security-best-practices#:~:text=Although%20Google%20encrypts%20the%20data,such%20as%20Boxcryptor%20or%20Cryptomator.*

20. *Google Workspace Admin Help URL: https://support.google.com/a*