Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Драгана Тараса Сергійовича

на здобуття ступеня вищої освіти Бакалавра

Система безпечного зберігання конфіденційної інформації на зовнішніх пристроях

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

КРБКБ.2102145.21.02.24 ПЗ

Виконав студент 4 курсу, група КБ-21-2 01.06.25 Тарас ДРАГАН
Підпис, дата Ініціали, прізвище

Керівник канд. тех. наук, доцент 01.06. Володимир ДЖУЛІЙ
Науковий ступінь, вчене звання Підпис, дата Ініціали, прізвище

Нормоконтролер старший викладач 11.06.25р. Сергій МОСТОВИЙ
Науковий ступінь, вчене звання Підпис, дата Ініціали, прізвище

До захисту допускаю:

Зав. кафедри кібербезпеки _____ Юрій КЛЬОЦ
Підпис, дата Ініціали, прізвище

11 06 2025р.

Хмельницький, 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2025 р.

З А В Д А Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Драган Тарас Сергійович

1 Тема роботи Система безпечного зберігання конфіденційної інформації на зовнішніх пристроях

Керівник роботи канд. тех. наук, доц. Володимир Миколайович Джулій

Затверджено наказом ректора університету від 7 лютого 2025 № 23

2 Строк подання студентом кваліфікаційної роботи на кафедру 06.06.2025

3 Вихідні дані до роботи Розробити ефективну систему безпечного зберігання конфіденційної інформації на зовнішніх пристроях. Дослідити сучасні загрози несанкціонованого доступу, методи захисту даних, проаналізувати наявні програмно-апаратні засоби.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Проаналізувати види зовнішніх носіїв інформації та їх вразливості. Дослідити загрози конфіденційній інформації на зовнішніх пристроях і методи її захисту. Проаналізувати існуючі програмно-апаратні засоби безпеки. Розробити структуру системи захисту та обґрунтувати вибір технологій. Навести етапи впровадження системи та оцінити її ефективність.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) «Структурна схема системи захисту інформації», «Алгоритм шифрування та доступу до даних», «Схема захисту даних на зовнішньому накопичувачі».

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Лютий	
Аналіз загроз та вразливостей конфіденційних даних на зовнішніх пристроях	Лютий	
Дослідження методів захисту інформації від шкідливого програмного забезпечення	Лютий	
Постановка задачі та визначення вимог до системи захисту зовнішніх носіїв	Березень	
Формування загальних принципів побудови системи захисту	Березень	
Розробка архітектури системи захисту	Квітень	
Реалізація механізмів захисту на основі вибраного інструменту	Квітень	
Розгортання системи захисту зовнішніх носіїв інформації	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Червень	
Захист КР	Червень	

Студент Тарас ДРАГАН

Керівник кваліфікаційної роботи Володимир ДЖУЛІЙ

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система безпечного зберігання конфіденційної інформації на зовнішніх пристроях».

Автор роботи: студент групи КБ-21-2 Драган Тарас Сергійович.

Керівник роботи: канд. тех. наук, доцент кафедри кібербезпеки Джулій Володимир Миколайович.

Пояснювальна записка: 77 с., 30 рис., 67 джерел, 2 додатки.

Графічна частина: 4 плакати.

Конфіденційна інформація, зовнішні пристрої, безпека інформації, шифрування, аутентифікація, антивірусний захист, захист даних.

Кваліфікаційна робота бакалавра присвячена розробці системи безпечного зберігання конфіденційної інформації на зовнішніх пристроях, таких як флеш-накопичувачі, зовнішні жорсткі диски та інші портативні засоби зберігання.

У роботі детально розглянуті основні загрози та вразливості, пов'язані з використанням зовнішніх пристроїв для зберігання даних, а також методи та засоби їх захисту. Зокрема, розглянуто використання шифрування даних, аутентифікацію користувачів, антивірусний захист, а також апаратні засоби захисту для забезпечення безпеки інформації. Окремо оцінено ефективність сучасних програмних рішень. У результаті дослідження надано аналіз існуючих рішень, що дозволяють знизити ризики несанкціонованого доступу до конфіденційної інформації.

01.06.2025 _____

ABSTRACT

Topic of qualification work: «A system for securely storing confidential information on external devices».

Author of the work: student of the group CS-21-2 Drahan Taras Serhiyovich.

Head of work: Ph.D. tech. Sciences, Associate Professor of the Department of Cybersecurity Jhuliy Volodymyr Mykolayovych.

Explanatory note: 77 p., 30 Fig., 67 sources, 2 appendices.

Graphic part: 4 posters.

CONFIDENTIAL INFORMATION, EXTERNAL DEVICES, INFORMATION SECURITY, ENCRYPTION, AUTHENTICATION, ANTIVIRUS PROTECTION, DATA PROTECTION.

The bachelor's thesis is dedicated to the development of a secure storage system for confidential information on external devices, such as flash drives, external hard drives, and other portable storage media.

The work thoroughly examines the main threats and vulnerabilities associated with using external devices for data storage, as well as methods and means of protection. Specifically, it covers data encryption, user authentication, antivirus protection, and hardware-based protection mechanisms to ensure information security. The thesis also evaluates the effectiveness of modern software solutions and offers recommendations for improving security systems for storing data on external devices. As a result of the research, an analysis and comparison of existing solutions are provided, aimed at reducing the risks of unauthorized access to confidential information.

01.06.2025 _____

ЗМІСТ

СПИСОК СКОРОЧЕНЬ

AES – Advanced Encryption Standard

CASB – Cloud Access Security Broker

CBC – Cipher Block Chaining

DLP – Data Loss/Leak Prevention

ECM – Enterprise Content Management

GDPR – General Data Protection Regulation

HIPAA – Health Insurance Portability and Accountability Act

IDS/IPS – Intrusion Detection and Prevention System

IIS – Internet Information Services

MITM – Man in the Middle

PCI – Payment Card Industry

SEG – Secure Email Gateway

SQL – Structured Query Language

SWG – Secure Web Gateway

XSS – Cross Site Scripting

НСД – Несанкціонований доступ

ПЗ – Програмне забезпечення

ПК – Портативний комп'ютер

СЗІ – Система захисту інформації

ЗП – Зовнішні пристрої

ВСТУП

В умовах стрімкого розвитку інформаційних технологій питання захисту конфіденційної інформації постає як одне з найактуальніших. Зовнішні носії інформації, зокрема флеш-накопичувачі, зовнішні жорсткі диски, SSD-диски та інші пристрої, що використовуються для зберігання та передачі даних, активно застосовуються як у побуті, так і в професійній діяльності. Їх зручність, мобільність, компактність і висока ємність роблять їх незамінним інструментом сучасної цифрової інфраструктури. Водночас саме ці переваги створюють серйозні загрози у сфері інформаційної безпеки.

Несанкціонований доступ, втрата або крадіжка пристрою, наявність шкідливого програмного забезпечення, а також відсутність належного контролю над процесом зберігання чи передавання інформації — усе це підвищує ризик витоку або модифікації конфіденційних даних. Зовнішні пристрої часто залишаються поза межами централізованих систем захисту, що значно ускладнює забезпечення цілісності та конфіденційності збережених на них даних. У зв’язку з цим зростає потреба в ефективних програмно-апаратних рішеннях, які здатні захистити інформацію на таких пристроях навіть у разі фізичної втрати або потрапляння в чужі руки.

У сучасних реаліях традиційні методи захисту, які базуються виключно на антивірусному захисті або файлових паролях, вже не є достатніми. Надійний захист конфіденційної інформації має ґрунтуватися на комплексному підході, який включає криптографічні алгоритми шифрування та дешифрування, багаторівневу автентифікацію, контроль доступу, ідентифікацію пристроїв та аудит дій користувачів. Такі системи повинні бути простими у використанні, але достатньо надійними для забезпечення захисту навіть у разі серйозних кіберзагроз.

Актуальність даного дослідження також визначається зростанням вимог до захисту персональних і конфіденційних даних у законодавчому полі. Зокрема, в Україні це Закони «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», а також рекомендації ДСТУ щодо інформаційної

безпеки. На міжнародному рівні вагоме значення мають положення Загального регламенту ЄС із захисту даних GDPR, що передбачає жорсткі вимоги до зберігання та обробки персональної інформації. Виконання цих норм вимагає наявності ефективних технічних та організаційних заходів захисту, серед яких ключову роль відіграє використання криптографічних технологій на рівні пристроїв зберігання.

Метою цієї кваліфікаційної роботи є аналіз сучасних загроз для конфіденційної інформації на зовнішніх пристроях та розробка системи її безпечного зберігання, що дозволяє мінімізувати ризики витоку, спотворення або знищення даних. У межах роботи проведено дослідження типів зовнішніх носіїв, методів їх ідентифікації, сучасних векторів атак, а також вивчено можливості застосування криптографічних алгоритмів для захисту даних. Особливу увагу приділено практичному проєктуванню програмно-апаратної системи, яка реалізує безпечне шифрування даних на зовнішньому пристрої з подальшим тестуванням її ефективності.

Результатом дослідження стало створення структурно-функціональної моделі системи безпечного зберігання інформації та її реалізація з використанням сучасних засобів програмного забезпечення. Запропонована система дозволяє суттєво підвищити рівень захищеності конфіденційної інформації на зовнішніх носіях, а також забезпечити відповідність сучасним вимогам інформаційної безпеки.

1 АНАЛІЗ ЗАГРОЗ БЕЗПЕЧНОГО ЗБЕРІГАННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ НА ЗОВНІШНІХ ПРИСТРОЯХ

1.1 Цифрові носії інформації. Ознаки ідентифікації

У 1995 році американський студент університету загубив у бібліотеці дискету, на якій зберігав дипломну роботу. Через тиждень дискета була знайдена, однак файл виявився зіпсованим — пристрій був пошкоджений через вплив магнітного поля з охоронної системи. Цей випадок змусив молодого дослідника задуматися над надійністю та вразливістю цифрових носіїв. Відтоді технології зберігання інформації пройшли довгий шлях: від вразливих магнітних дисків до надшвидких твердотільних накопичувачів з апаратним шифруванням і навіть хмарних сервісів, захищених багатоетапною автентифікацією. Але разом з розвитком з’являлися і нові загрози, що вимагали нових підходів до класифікації, ідентифікації та захисту інформації.

Цей випадок наочно демонструє, наскільки важливим є питання ідентифікації та захисту цифрових носіїв інформації. У сучасному світі, де щодня передаються, зберігаються й обробляються гігабайти конфіденційних даних, розуміння типів носіїв, їхніх характеристик і вразливостей є критично важливим для забезпечення інформаційної безпеки. Тому далі розглянемо, що саме являють собою цифрові носії інформації, які їх основні класифікації та ознаки ідентифікації.

Цифрові носії інформації – це фізичні або логічні пристрої, призначені для зберігання, передачі та обробки цифрових (тобто представлених у вигляді двійкового коду) даних. До таких носіїв належать жорсткі диски (HDD, SSD), флеш-накопичувачі, карти пам’яті, оптичні диски (CD/DVD), а також зовнішні мережеві сховища (NAS) і хмарні сервіси.[1]

Кожен цифровий носій має унікальні ознаки ідентифікації, що дають змогу відрізнити один пристрій від іншого. Основними ознаками ідентифікації цифрових носіїв є:

1. Серійний номер – унікальний ідентифікатор, який присвоюється виробником пристрою та зберігається у прошивці або апаратному контролері.

2. Модель та виробник пристрою – інформація про тип, серію й бренд носія.

3. Фізичні характеристики – об’єм пам’яті, тип інтерфейсу (USB, SATA, NVMe тощо), швидкість читання/запису.

4. MAC– адреса (для мережевих пристроїв зберігання) – унікальний ідентифікатор мережевого інтерфейсу.

5. Інформація з файлової системи – метадані, що містять дату створення, останнього доступу, форматування тощо.

6. Ідентифікаційні сліди в ОС – залишки використання носія в реєстрі або журналах системи (наприклад, у Windows – у розділі реєстру USBSTOR).[2]

Цифрові носії інформації (рис.1.1) є ключовими елементами сучасних інформаційних систем, забезпечуючи зберігання, передачу та обробку даних. Їх класифікація базується на технологічних принципах, конструктивних особливостях та функціональних можливостях, що визначають їх застосування та рівень безпеки збереження інформації.

Рисунок 1.1– Види зовнішніх цифрових носіїв інформації [1]

Основним критерієм класифікації є тип носія, що використовується для зберігання даних. До таких носіїв належать електронно-оптичні, магнітні та

твердотільні пристрої. Електронно-оптичні носії, зокрема CD, DVD та Blu-ray диски, характеризуються здатністю зберігати великі обсяги інформації при відносно низькій вартості, але мають обмежену швидкість читання і запису, а також чутливість до оптичних і температурних впливів, що може впливати на довгострокову збереженість даних [3].

Магнітні носії, такі як зовнішні жорсткі диски HDD, використовують магнітне зчитування і запис інформації, що забезпечує високі обсяги збереження при прийнятних швидкостях доступу, проте вони можуть бути вразливими до механічних пошкоджень і електромагнітних впливів [4].

Твердотільні накопичувачі (SSD) набувають все більшої популярності завдяки своїм високим швидкостям читання та запису, а також більшій стійкості до механічних впливів порівняно з магнітними дисками. Проте вартість таких пристроїв залишається вищою, що обмежує їх широке застосування в деяких сегментах ринку [5].

Іншим важливим аспектом класифікації цифрових носіїв є спосіб підключення до комп'ютерних систем. Сучасні технології забезпечують можливість підключення через інтерфейси USB, Thunderbolt, eSATA, а також бездротові технології, що дозволяють здійснювати передачу даних на високих швидкостях і забезпечують зручність використання.[6]

Зокрема, найбільш поширеним є інтерфейс USB, який підтримує різні версії від USB 2.0 до USB 4.0, кожна з яких відрізняється швидкістю передачі даних, енергоспоживанням та сумісністю. Thunderbolt, у свою чергу, пропонує ще вищу пропускну здатність і широко застосовується у професійному середовищі для роботи з великими обсягами даних, наприклад, у відеомонтажі. eSATA використовується переважно для підключення зовнішніх жорстких дисків, забезпечуючи високу швидкість передачі, порівнянну з внутрішніми інтерфейсами. Бездротові способи, як-от Wi-Fi Direct або Bluetooth, хоч і мають нижчу швидкість, забезпечують гнучкість та мобільність, що особливо важливо для користувачів мобільних пристроїв.

Крім того, класифікація може здійснюватися за принципом портативності: існують мобільні зовнішні носії, які легко транспортувати і використовувати в

різних умовах, а також стаціонарні пристрої, що забезпечують більш високий рівень збереження даних завдяки можливості організації більш складних систем охолодження та захисту від фізичних впливів.[7]

До портативних носіїв відносяться флеш-накопичувачі, зовнішні SSD-диски, SD-карти та інші компактні пристрої, які користувач може носити із собою. Їх перевагою є легкість, невеликий розмір та зручність підключення. Стаціонарні ж носії, як правило, представлені зовнішніми RAID-масивами, NAS-серверами або великими зовнішніми HDD, які підключаються до робочої станції або мережі й мають більшу ємність зберігання.

Не менш важливим критерієм класифікації є рівень захисту інформації, який забезпечує кожен тип пристрою. Сучасні зовнішні пристрої можуть бути обладнані апаратними засобами шифрування, що дозволяють забезпечити високий рівень конфіденційності збережених даних, навіть у випадку втрати або викрадення пристрою. Такі пристрої зазвичай мають вбудовані криптографічні модулі, що відповідають міжнародним стандартам безпеки, наприклад, FIPS 140-2 або ISO/IEC 27001.

Апаратне повне шифрування диску (рис.1.2) — це метод шифрування диска цілком, в якому шифрування відбувається за допомогою спеціалізованих обчислювальних пристроїв. Схема дії апаратного шифрування показано на фото:

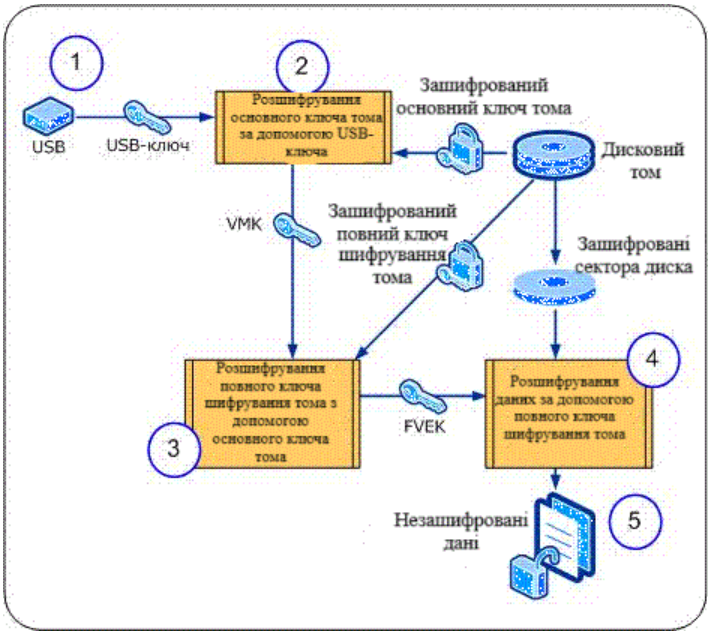


Рисунок 1.2 – Схема апаратного повного шифрування диску [2]

Апаратне повне шифрування реалізується безпосередньо на рівні накопичувача за допомогою вбудованого контролера, який виконує шифрування та дешифрування даних у реальному часі з використанням криптографічного алгоритму AES. Такий підхід забезпечує високий рівень безпеки інформації без помітного впливу на продуктивність системи, а також мінімізує ризики витоку даних при фізичній втраті носія.

Апаратне шифрування дозволяє захищати дані без суттєвого зниження продуктивності пристрою, оскільки криптографічні операції виконуються спеціалізованим процесором або чіпом, окремим від основної системи. Це знижує ризик компрометації через уразливості операційної системи або програмного забезпечення. Багато таких пристроїв мають додаткові функції, як-от автентифікація за допомогою PIN-коду, біометричної перевірки або навіть самознищення даних у разі несанкціонованих спроб доступу.

Крім апаратних рішень, на зовнішніх носіях можуть застосовуватися також програмні засоби захисту, які включають багаторівневу аутентифікацію, контроль доступу та системи моніторингу, що дозволяють в режимі реального часу відслідковувати всі спроби доступу до даних.[8]

Такі програмні рішення як BitLocker, VeraCrypt або AxCrypt, забезпечують ефективне шифрування, часто із використанням алгоритмів AES з довжиною ключа 256 біт. Програмне забезпечення може включати можливість створення віртуальних зашифрованих дисків, журналювання подій, автоматичне блокування при бездіяльності, інтеграцію з Active Directory тощо. Деякі сучасні рішення також підтримують хмарну синхронізацію із шифруванням на стороні клієнта, що дозволяє захищати інформацію навіть у випадку зламу хмарного сервісу.

Наукові дослідження в галузі інформаційної безпеки підкреслюють, що правильна класифікація зовнішніх пристроїв є базою для розробки ефективних систем захисту, оскільки вона дозволяє систематизувати загрози, оцінити рівень ризиків і визначити оптимальні методи забезпечення безпеки для кожного типу носія.

Наприклад, для портативних пристроїв головною загрозою є фізична втрата або крадіжка, тоді як для стаціонарних — підвищені ризики кібератак через

постійне мережеве з’єднання. Визначення типових векторів атак для кожної категорії носіїв дозволяє застосовувати цілеспрямовані засоби захисту — як технічні, так і організаційні, включаючи політики безпечного використання, обмеження доступу, резервне копіювання та аудит безпеки.

Таким чином, розуміння характеристик різних типів зовнішніх пристроїв і їх класифікація є фундаментальними для розробки комплексних заходів, спрямованих на забезпечення безпеки конфіденційної інформації в умовах сучасного цифрового середовища.

Тільки з урахуванням усіх технічних, функціональних і безпекових особливостей зовнішніх носіїв можна створити стійку інфраструктуру захисту даних, що відповідатиме вимогам сучасного бізнесу, державного управління або наукових досліджень. Врахування класифікаційних ознак дозволяє адаптувати засоби захисту до специфіки середовища, де використовується носій, підвищуючи ефективність як профілактичних, так і реактивних заходів протидії загрозам.

1.2 Загрози безпечного зберігання конфіденційної інформації на флеш-накопичувачі

Із початку 2000-х років, коли на ринку з’явилися перші комерційно доступні USB-флеш-накопичувачі, відбулося справжнє переосмислення підходів до зберігання й перенесення цифрових даних. Замість громіздких дискет і компакт-дисків користувачі отримали компактний, надійний і зручний спосіб зберігати гігабайти інформації в кишені. Вже до 2010-х років USB-накопичувачі стали стандартом у повсякденній роботі — як у побутовому, так і в корпоративному середовищі. Їх почали використовувати у навчальних закладах, органах державної влади, медичних установах та військових структурах. Це забезпечило їм надзвичайну популярність, але одночасно й привернуло увагу зловмисників.

Еволюція флеш-накопичувачів супроводжувалася й еволюцією загроз, пов’язаних з їхнім використанням. Ще у 2008 році світ побачив одну з перших масштабних кібератак через USB-пристрої — інцидент з розповсюдженням вірусу

Agent.btz у військових мережах США. Цей випадок став каталізатором глобального перегляду політик безпеки щодо використання зовнішніх носіїв у державних і комерційних структурах. [9]

Сучасні флеш-накопичувачі – це не лише носії інформації, а потенційні канали витоку даних, поширення шкідливого ПЗ або втручання у функціонування інформаційних систем. Їхні малі габарити, універсальність і простота використання водночас створюють серйозні виклики для забезпечення інформаційної безпеки. Достатньо одного забутого або загубленого пристрою – і критично важлива інформація може потрапити до рук третіх осіб. Атаки типу “drop attack”, коли заражені флешки навмисне залишають у громадських місцях, досі залишаються актуальними інструментами соціальної інженерії. [10]

Загрози, пов’язані з використанням USB-накопичувачів, охоплюють як фізичні аспекти- втрата, крадіжка, ушкодження, так і кіберзагрози несанкціонований доступ, шкідливе ПЗ, порушення політик безпеки. У результаті, USB-пристрої сьогодні вважаються одним із найуразливіших елементів в інформаційній інфраструктурі, особливо коли мова йде про зберігання конфіденційної інформації. [11]

У цьому підрозділі розглянуто основні загрози, які виникають при використанні флеш-накопичувачів для зберігання або перенесення конфіденційних даних, а також окреслено потенційні сценарії атак та їхні наслідки для безпеки персональних і корпоративних інформаційних систем.

Флеш-накопичувачі (USB-накопичувачі) залишаються одними з найпопулярніших засобів зберігання й перенесення цифрових даних. Їх популярність зумовлена мобільністю, універсальністю, легкістю використання та відносною дешевизною. Проте, окрім своїх переваг, флеш-накопичувачі мають і суттєві недоліки з точки зору інформаційної безпеки. Вони часто стають джерелом витоків даних, поширення шкідливого програмного забезпечення або вектором кібератак. У цьому підрозділі розглянуто основні загрози, пов’язані з використанням флеш-накопичувачів для зберігання конфіденційної інформації.

Втрата або крадіжка пристрою. Однією з найпоширеніших загроз є втрата або крадіжка пристрою. Через малі габарити та портативність USB-накопичувачів

їх легко загубити або залишити без нагляду. Якщо пристрій не захищено паролем або шифруванням, доступ до інформації на ньому може отримати будь-хто. У випадках, коли на флеш-накопичувачі зберігається конфіденційна інформація, наслідки можуть бути критичними для безпеки організації чи окремої особи. [12]

Поширення шкідливого ПЗ. USB-накопичувачі часто використовуються як вектори поширення шкідливого програмного забезпечення. Кіберзлочинці можуть навмисно залишити заражені флешки у громадських місцях, розраховуючи на те, що хтось їх підключить до свого комп'ютера. Відомі атаки, як-от Stuxnet, продемонстрували ефективність такого підходу. Навіть коротке підключення зараженого USB-накопичувача може призвести до інфікування системи вірусами, руткітами або троянами. [13]

Несанкціонований доступ до даних. Пристрої без належного контролю доступу є вразливими до копіювання, зміни або знищення даних. Якщо USB-порт не заблокований або не контрольований, зловмисник може легко підключити власний накопичувач і викрасти важливу інформацію. Цей тип загроз особливо актуальний у корпоративному середовищі, де працівники можуть мати доступ до конфіденційних даних. [14]

Обхід політик інформаційної безпеки. У деяких організаціях співробітники можуть використовувати особисті флеш-накопичувачі для перенесення робочих файлів. Це створює серйозний ризик, адже пристрої можуть бути зараженими або не відповідати політикам безпеки підприємства. Крім того, інформація, перенесена за межі захищеного середовища, може потрапити в руки сторонніх осіб. [15]

Відсутність шифрування даних. Багато користувачів зберігають важливу інформацію на флешках у відкритому вигляді, без жодного шифрування або захисту паролем. Це робить дані доступними у разі втрати або крадіжки пристрою. Застосування шифрування допомагає суттєво знизити ймовірність витоку, навіть якщо пристрій потрапить до рук третіх осіб. [16]

Фізичне пошкодження пристрою. Попри свою простоту, флеш-накопичувачі не захищені від фізичних ушкоджень. Їх можна легко зламати, пошкодити водою, температурою чи механічним впливом. У разі пошкодження можуть бути

втрачені всі збережені дані, що є критичним для конфіденційної інформації без резервного копіювання. [17]

Використання флеш-накопичувачів у кібератаках. Флеш-накопичувачі можуть бути використані як засіб для збирання даних або інфільтрації захищених мереж. Наприклад, спеціальні "USB Rubber Ducky" пристрої можуть імітувати клавіатуру та автоматично вводити зловмисні команди в систему жертви. Ці типи атак є дуже важко виявити звичайними засобами захисту.[18]

Таким чином, флеш-накопичувачі, незважаючи на свою зручність, становлять серйозну загрозу для інформаційної безпеки, особливо в корпоративному середовищі. Застосування комплексного підходу до захисту, що включає шифрування, контроль доступу, політики безпечного використання та технічний моніторинг, є необхідним кроком до збереження конфіденційної інформації.

1.3 Дослідження загроз конфіденційної інформації на ЗП

Актуальні статистичні дані підтверджують, що зовнішні пристрої залишаються одним із ключових векторів атак у сфері кібербезпеки. Згідно зі звітом компанії Honeywell за 2024 рік, 51% усіх шкідливих програм було спеціально розроблено для USB-пристроїв, що є шестикратним зростанням у порівнянні з 9% у 2019 році. Крім того, 82% з цих загроз здатні викликати критичні порушення в роботі промислових систем, включаючи втрату контролю над обладнанням. [19]

У першій половині 2023 року було зафіксовано триразове зростання атак з використанням заражених USB-накопичувачів. Зокрема, кампанії SOGU та SNOWYDRIVE активно використовували USB-пристрої для інфільтрації корпоративних та державних мереж. [20]

Окрему небезпеку становить нехтування базовими заходами захисту. Так, за даними аналітичного порталу Verdict, 55% британських компаній не

використовують шифрування для захисту знімних носіїв, що створює високий ризик витоку даних у разі їх втрати або крадіжки. [21]

Компанія Kaspersky повідомляє, що впродовж 2024 року виявлялося в середньому 467 тисяч шкідливих файлів щодня, що на 14% більше, ніж у попередньому році. Особливо стрімке зростання спостерігалося у категорії троянських програм – на 33% у порівнянні з 2023 роком. [22]

Ці цифри свідчать про актуальність і серйозність загроз, пов'язаних із зовнішніми носіями інформації, та підтверджують необхідність комплексного підходу до їхнього захисту на всіх рівнях.

У сучасну епоху цифрових технологій зовнішні пристрої зберігання даних, такі як USB-флеш-накопичувачі, зовнішні жорсткі диски HDD, твердотільні накопичувачі SSD, SD-карти, а також портативні пристрої з інтерфейсами бездротового з'єднання – є невіддільною частиною повсякденного використання як у побуті, так і в професійній діяльності. Ці носії стали стандартними інструментами для зберігання, резервного копіювання та перенесення цифрової інформації між пристроями.

Історія використання зовнішніх носіїв сягає ще 1960-х років, коли з'явилися перші магнітні стрічки й диски для комп'ютерів мейнфрейм-класу. Пізніше, у 1980-х роках, популярності набули дискети, які хоч і мали обмежену ємність (1,44 МБ), але на той час були революційним кроком у мобільному зберіганні даних. У 1990-х роках на зміну їм прийшли компакт-диски CD та DVD, а на початку 2000-х USB-флешки. Ці еволюційні зміни супроводжувалися стрімким зростанням обсягів даних і потребою в зручному способі їхньої мобільності.

Проте зі зростанням кількості мобільних пристроїв зберігання зростали й інциденти витоку конфіденційної інформації. Один із найгучніших випадків стався у Великій Британії у 2008 році, коли втрачений USB-накопичувач з даними понад 12 млн громадян, включаючи адреси, дати народження та банківські рахунки, спричинив скандал на національному рівні та призвів до серйозної перевірки систем державного захисту даних. [23]

Особливу загрозу зовнішні носії становлять через свою портативність, що робить їх легкими для викрадення, загублення або несанкціонованого

підключення до систем без відповідного контролю. Більше того, такі пристрої можуть бути використані як інструмент активної атаки. Наприклад, спеціальні пристрої типу USB Rubber Ducky виглядають як звичайні флешки, але всередині мають мікроконтролери, які імітують клавіатуру і автоматично вводять шкідливі команди при підключенні. [24]. Такі методи стали частиною арсеналу соціальної інженерії.

Ще однією проблемою є відсутність у багатьох пристроях шифрування за замовчуванням або недостатньо ефективна його реалізація. Якщо дані зберігаються у відкритому вигляді, будь-хто, хто отримає доступ до пристрою, може легко прочитати або скопіювати їх. Це особливо критично для конфіденційної інформації, що стосується персональних даних, комерційної таємниці, медичних записів або державної документації.

Актуальність дослідження загроз, пов’язаних із зовнішніми пристроями зростає також у зв’язку з переходом до гібридних і дистанційних форматів роботи. Користувачі дедалі частіше використовують особисті пристрої для роботи з робочими файлами, що створює серйозні виклики для контролю інформаційної безпеки на рівні підприємств та організацій.

Крім того, сучасні пристрої можуть мати приховані функції як модулі бездротового зв’язку Wi-Fi або Bluetooth, які дозволяють передавати інформацію навіть без прямого підключення до комп’ютера. Такі технології сильно ускладнюють виявлення та блокування витоку даних стандартними засобами безпеки конфіденційної інформації.

З огляду на вищезазначене, особливої уваги заслуговує проблема відсутності ефективної політики контролю доступу до портів USB у більшості організацій. За результатами дослідження Ponemon Institute, понад 70% компаній не мають чітко визначених процедур щодо виявлення та блокування несанкціонованого підключення зовнішніх пристроїв, що створює критичну вразливість у корпоративній інфраструктурі.

Створено таблицю (1.1) про загрози конфіденційної інформації на зовнішніх пристроях, про опис та можливі заходи захисту інформації:

Таблиця 1.1– Загрози конфіденційної інформації на зовнішніх пристроях

№	Загроза	Опис загрози	Можливі заходи захисту
1	Несанкціонований доступ до пристрою	Використання фізичного доступу до зовнішнього пристрою для крадіжки або зміни даних.	Використання апаратного шифрування, двофакторної аутентифікації, паролів.
2	Втрата пристрою	Фізична втрата або крадіжка зовнішнього пристрою з конфіденційною інформацією.	Використання функцій віддаленого блокування або знищення даних.
3	Віруси та шкідливе програмне забезпечення	Потрапляння шкідливого програмного забезпечення, яке може викрасти або знищити дані.	Використання антивірусного програмного забезпечення, регулярні оновлення.
4	Неавторизоване копіювання інформації	Незаконне копіювання або передача конфіденційної інформації з пристрою сторонніми особами.	Шифрування даних, контроль доступу, аудит дій користувачів.
5	Атаки через порти та інтерфейси	Вразливість через незахищені порти або інтерфейси для підключення до зовнішнього пристрою.	Використання VPN, налаштування брандмауерів, обмеження доступу до портів.
6	Невірне зберігання даних	Зберігання конфіденційної інформації в незахищеному вигляді на зовнішньому пристрої (без шифрування).	Шифрування даних, використання паролів, встановлення обмежень доступу.
7	Атаки через вразлвості програмного забезпечення	Використання вразливостей у програмному забезпеченні для отримання доступу до даних.	Оновлення програмного забезпечення, використання патчів безпеки.
8	Витік інформації через мережу	Викрадення данних серех мережеві зєднання	Використання шифрування даних під час передачі, обмеження доступу до мережі
9	Невірне використання пристрою	Використання зовнішнього пристрою без належних засобів безпеки	Навчання користувачів, застосування політик безпеки, контроль доступу
10	Атаки через скомпрометовані пристрої	Використання заражених пристроїв для інфікування інших пристроїв	Перевірка пристроїв перед використанням, контроль за пристроями з підозрілою історією

Таким чином, дослідження загроз, пов’язаних із зовнішніми носіями інформації, є важливою складовою у сфері інформаційної безпеки. Воно дозволяє сформувати ефективну політику захисту, включаючи організаційні, технічні та програмні заходи, спрямовані на запобігання витоку або втрати критично важливої інформації.

Зовнішні пристрої для зберігання даних, такі як флеш-накопичувачі, зовнішні жорсткі диски, твердотільні накопичувачі та інші подібні пристрої, широко застосовуються для збереження, перенесення та обміну конфіденційною інформацією між пристроями та користувачами. Їх компактність, висока швидкість передачі даних та зручність у використанні зробили їх надзвичайно популярними як у побутовому, так і в корпоративному середовищі. Однак, незважаючи на їх очевидні переваги, ці пристрої становлять серйозні загрози для інформаційної безпеки, оскільки можуть бути джерелом витоку, втрати або компрометації даних. Цей підрозділ присвячено детальному аналізу основних загроз, що виникають у процесі використання зовнішніх пристроїв для зберігання інформації.

Втрата або крадіжка пристрою є однією з найбільш поширених і небезпечних загроз для конфіденційної інформації є втрата або крадіжка зовнішніх пристроїв. Через свої невеликі розміри флеш-накопичувачі, карти пам’яті та інші портативні носії даних легко можуть бути загублені або вкрадені. У разі відсутності відповідного захисту, зокрема шифрування даних або встановлення пароля, сторонні особи можуть отримати прямий доступ до чутливої інформації. Це створює високий ризик витоку персональних, фінансових, службових або державних даних. Особливо це критично в умовах використання зовнішніх накопичувачів у сфері охорони здоров’я, банківської справи чи державного управління, де обробляється велика кількість конфіденційної інформації. За даними Cybersecurity & Infrastructure Security Agency, втрата флеш-накопичувача може призвести до серйозних наслідків, якщо дані на ньому не зашифровані або не захищені паролем [25]. У багатьох випадках такі інциденти призводять до репутаційних втрат, судових позовів або штрафів з боку регуляторних органів.

Поширення шкідливого програмного забезпечення. Зовнішні пристрої, зокрема USB-флешки, дуже часто використовуються зловмисниками для розповсюдження шкідливого програмного забезпечення. Носії можуть бути заражені вірусами, троянами, шпигунськими або рекламними програмами, які автоматично активуються при підключенні до комп'ютера. Такий механізм зараження дозволяє зловмиснику отримати доступ до системних файлів, внести несанкціоновані зміни до ОС, перехоплювати введення з клавіатури або передавати вкрадені дані на віддалені сервери. Відомим прикладом є атака на ядерні об'єкти Ірану за допомогою вірусу Stuxnet, який поширювався саме через USB-накопичувачі [26]. У корпоративному середовищі використання заражених пристроїв може спричинити повне знищення локальної мережі, втрату резервних копій або компрометацію критично важливої інформації. Більше того, деякі типи шкідливого ПЗ здатні самостійно розмножуватися, що ускладнює процес ліквідації загрози.

Несанкціонований доступ до даних є ще однією серйозною загрозою, пов'язаною з використанням зовнішніх накопичувачів. У багатьох організаціях не впроваджено належних технічних і адміністративних заходів безпеки для обмеження доступу до USB-портів. Якщо зловмисник отримує фізичний доступ до комп'ютера, він може просто підключити свій пристрій та скопіювати конфіденційні файли, інсталювати шпигунське ПЗ або змінити параметри системи. Це стосується не тільки зовнішніх загроз, а й внутрішніх — працівників компанії, які мають доступ до важливої інформації. У зв'язку з цим, контроль використання зовнішніх пристроїв, ведення журналів доступу та запровадження політики "білого списку USB-пристроїв" є важливими елементами інформаційної безпеки в будь-якій установі [27].

Використання флеш-накопичувачів для обходу політик безпеки. Навіть за наявності розроблених внутрішніх політик безпеки, співробітники іноді навмисно або через незнання використовують особисті пристрої, щоб обійти встановлені обмеження. Вони можуть копіювати службові файли на особисті флеш-накопичувачі з метою подальшої роботи вдома або передачі інформації третім особам. У результаті, навіть при дотриманні всіх формальних заходів безпеки в

межах корпоративної мережі, виникає загроза витоку конфіденційної інформації за її межами. Також, несанкціоновані флешки, які використовуються без перевірки антивірусним ПЗ, можуть стати джерелом зараження внутрішньої ІТ-інфраструктури. Впровадження політик контролю знімних носіїв, програмного блокування USB-портів та навчання персоналу щодо загроз, пов’язаних із використанням таких пристроїв, допомагає ефективно зменшити ризики [28].

Не менш важливою загрозою є фізичне пошкодження зовнішніх накопичувачів. Такі пристрої, хоч і призначені для мобільного використання, залишаються досить вразливими до впливу зовнішніх факторів. Флеш-накопичувачі можуть легко пошкодитись при падінні, дії вологи, екстремальних температур, електростатичних розрядів або неправильної експлуатації. У результаті пристрій може стати непридатним для використання, а збережені на ньому дані — безповоротно втраченими. Особливо критичним це є у випадках, коли дані не були попередньо скопійовані або зашифровані, а сам пристрій є єдиним місцем їх зберігання. Для мінімізації таких ризиків доцільно використовувати надійні чохли, вологозахищені моделі, а також дотримуватися правил зберігання й транспортування пристроїв [29].

Використання флеш-накопичувачів для кібератак. Зовнішні накопичувачі можуть бути використані як активний інструмент для здійснення цілеспрямованих кібератак. Спеціальні пристрої типу USB Rubber Ducky або "BadUSB" здатні імітувати дії клавіатури, виконуючи автоматичний набір шкідливих команд одразу після підключення до комп’ютера. Це дозволяє обійти традиційні методи захисту, зокрема антивіруси, фаєрволи або системи контролю доступу. Атаки з використанням таких пристроїв можуть бути практично непомітними для користувача та ІТ-відділу, що ускладнює їх виявлення та своєчасне реагування. Внаслідок цього зловмисники можуть викрадати дані, змінювати системні конфігурації або завантажувати нове ПЗ без згоди адміністратора системи. З метою захисту рекомендується обмежити доступ до USB-портів, використовувати антивірусні рішення для моніторингу активності зовнішніх пристроїв і проводити навчання персоналу з кібергігієни [30].

1.4 Постановка задачі

У першому розділі було здійснено комплексний аналіз цифрових носіїв інформації, їх класифікації, ознак ідентифікації, а також основних загроз, що виникають при зберіганні конфіденційної інформації на зовнішніх пристроях. Розглянуто сучасні методи та засоби захисту, як програмні, так і апаратні. У результаті цього аналізу було виявлено, що незважаючи на широкий спектр існуючих рішень, значна частина користувачів все ще піддається ризику втрати конфіденційних даних через недостатній рівень захисту або через недосконаліть існуючих технологій.

Однією з ключових проблем є те, що багато зовнішніх носіїв, особливо з недорогого сегменту (USB-накопичувачі, карти пам’яті), не мають вбудованих механізмів апаратного шифрування чи аутентифікації користувача. У поєднанні з їх компактністю та широкою поширеністю це робить їх привабливими об'єктами для зловмисників. Навіть при використанні програмного шифрування дані можуть бути вразливими при фізичному доступі до пристрою, некоректному зберіганні ключів чи соціальній інженерії. Також окрему загрозу становлять шкідливі програми, здатні автоматично копіювати вміст зовнішнього носія або модифікувати дані без відома користувача.

Враховуючи наведене, виникає необхідність у розробці ефективного, адаптивного та зручного механізму захисту конфіденційної інформації на зовнішніх пристроях. Такий механізм має поєднувати криптографічні методи, багатофакторну автентифікацію, а також враховувати технічні обмеження різних типів носіїв. Крім того, варто приділити увагу сумісності запропонованого рішення з поширеними операційними системами та сценаріями використання, як у персональному, так і корпоративному середовищі.

Метою цієї бакалаврської роботи є дослідження, проєктування та обґрунтування підходу до захисту конфіденційної інформації на зовнішніх пристроях від несанкціонованого доступу, з урахуванням реальних загроз та актуального рівня технологічного розвитку.

Для досягнення поставленої мети необхідно виконати такі дії:

1. Провести аналіз загроз безпечного зберігання конфіденційної інформації на зовнішніх пристроях.

2. Дослідити алгоритми шифрування/дешифрування конфіденційної інформації на зовнішніх пристроях від несанкціонованого доступу.

3. Оцінити рівень ефективності й доцільності використання таких рішень для різних категорій зовнішніх носіїв USB, HDD, SSD, карти пам’яті.

4. Розробити систему безпечного зберігання конфіденційної інформації на зовнішніх пристроях.

5. Провести тестування та аналіз програмного забезпечення шифрування конфіденційної інформації службою захисту.

Таким чином, постановка задачі охоплює всі ключові аспекти проблеми – від аналізу середовища й ризиків до розробки та перевірки реального інструменту захисту. Це забезпечує комплексний підхід до проблеми безпечного використання зовнішніх пристроїв для зберігання конфіденційної інформації.

2 ПРОЄКТУВАННЯ СИСТЕМИ БЕЗПЕЧНОГО ЗБЕРІГАННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ НА ЗОВНІШНІХ ПРИСТРОЯХ

2.1. Алгоритми шифрування/дешифрування конфіденційної інформації

У сучасному цифровому середовищі, де обсяг конфіденційної інформації постійно зростає, забезпечення її захисту на зовнішніх пристроях, таких як USB-накопичувачі, зовнішні жорсткі диски та інші портативні носії, є критично важливим. Основним методом забезпечення конфіденційності даних є їх шифрування, яке перетворює відкриту інформацію у форму, недоступну для розуміння без відповідного ключа.

Однією з основних переваг апаратних засобів захисту інформації на зовнішніх пристроях є їхня здатність виконувати криптографічні операції незалежно від операційної системи, на якій вони працюють. Це дозволяє мінімізувати ризики, пов’язані з уразливістю програмного забезпечення, та забезпечує додатковий рівень ізоляції даних. Наприклад, використання спеціалізованих мікроконтролерів, що реалізують алгоритми шифрування на фізичному рівні, дозволяє знизити ризик несанкціонованого доступу, навіть у разі компрометації операційної системи користувача. Таке апаратне шифрування часто реалізується на основі алгоритмів AES з довжиною ключа 256 біт, що на сьогодні вважається еталоном стійкості до атак перебором [31].

Симетричні алгоритми шифрування. Це шифрування використовує один і той самий ключ як для шифрування, так і для дешифрування даних конфіденційної інформації. Одним із найпоширеніших симетричних алгоритмів є Advanced Encryption Standard. AES є блочним шифром, який працює з блоками даних розміром 128 біт і підтримує ключі довжиною 128, 192 або 256 біт. Цей алгоритм був затверджений Національним інститутом стандартів і технологій США NIST у 2001 році як заміна застарілого DES і з того часу став стандартом для захисту конфіденційної інформації в багатьох сферах, включаючи урядові та комерційні застосування [32].

На рисунку представлено принцип роботи симетричного блочного шифрування, зокрема схему перетворення відкритих даних у зашифрований вигляд та навпаки, за допомогою одного спільного ключа (рис.2.1) :

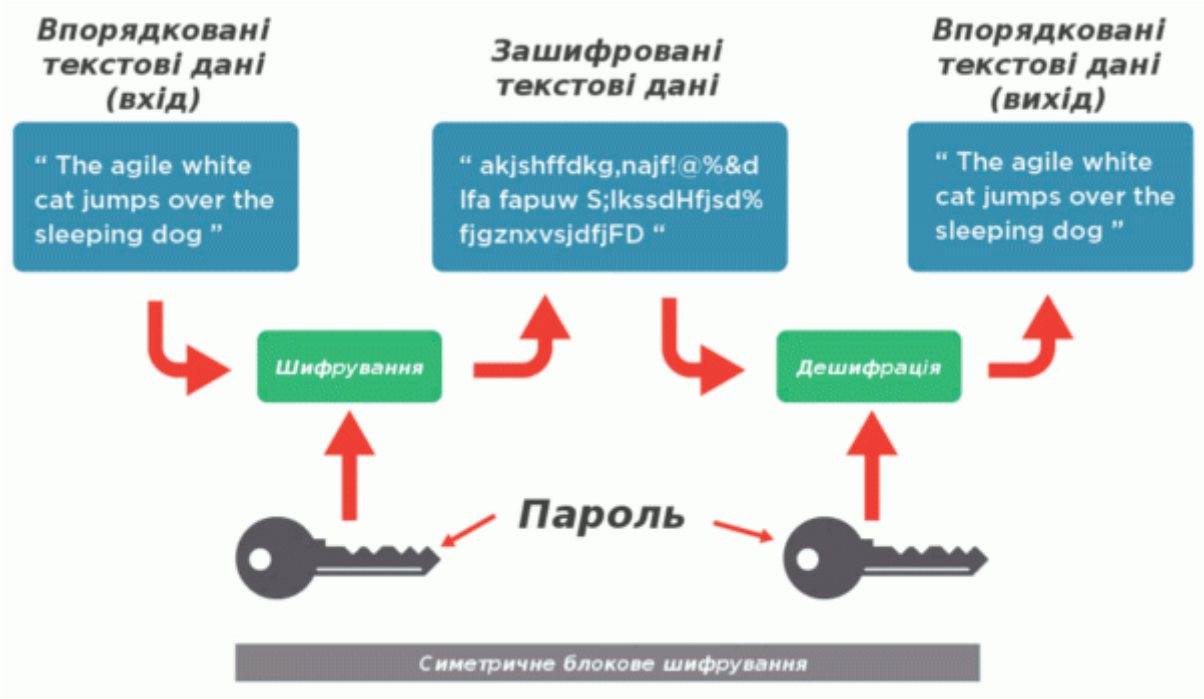


Рисунок 2.1– Алгоритм шифрування/дешифрування

Як показано на схемі, симетричне шифрування передбачає використання одного і того ж ключа як для шифрування, так і для дешифрування. Це забезпечує високу швидкодію та ефективність, проте вимагає безпечного зберігання та передачі самого ключа, адже компрометація пароля автоматично відкриває доступ до всіх захищених даних. З цієї причини симетричні алгоритми часто поєднують із асиметричними у гібридних криптографічних системах.

Переваги AES включають високу швидкість обробки, ефективність у програмному та апаратному забезпеченні, а також стійкість до відомих криптографічних атак. Його надійність підтверджена численними дослідженнями та практичним використанням у всьому світі [33].

Асиметричні алгоритми шифрування. Асиметричне шифрування використовує пару ключів: відкритий ключ для шифрування та закритий ключ для дешифрування. Найвідомішим асиметричним алгоритмом є RSA, який базується

на складності факторизації великих простих чисел. RSA широко використовується для захисту даних при передачі через незахищені канали зв'язку, а також для цифрового підпису та автентифікації [34].

Однак через високу обчислювальну складність RSA не є ефективним для шифрування великих обсягів даних. Тому на практиці часто застосовуються гібридні схеми шифрування, які поєднують переваги симетричних та асиметричних методів.

Гібридні схеми шифрування. Гібридні схеми шифрування поєднують симетричне та асиметричне шифрування для досягнення високої швидкості та безпеки. У таких схемах симетричний алгоритм, наприклад AES, використовується для шифрування основного вмісту даних, тоді як асиметричний алгоритм, такий як RSA, застосовується для шифрування симетричного ключа. Це дозволяє ефективно захищати великі обсяги даних, забезпечуючи при цьому безпечну передачу ключів [35].

Гібридні схеми широко використовуються в різних протоколах безпеки, таких як SSL/TLS, і є стандартом для захисту даних у хмарних сервісах та інших сучасних технологіях [36].

Режими роботи блочних шифрів. Режими роботи визначають, як блочний шифр, такий як AES, обробляє дані, що перевищують розмір одного блоку. Основні режими включають:

1. Electronic Codebook: кожен блок шифрується незалежно. Недоліком є те, що однакові блоки відкритого тексту шифруються в однакові блоки шифротексту, що може призвести до витоку інформації.

2. Cipher Block Chaining: кожен блок відкритого тексту перед шифруванням поєднується з попереднім блоком шифротексту, що забезпечує кращу безпеку, але ускладнює паралельну обробку.

3. Cipher Feedback та Output Feedback: перетворюють блочний шифр у потоковий, що дозволяє обробляти дані по байтах або бітам.

4. Counter: використовує лічильник для генерації потоку ключів, що дозволяє ефективну паралельну обробку та є стійким до деяких типів атак [37].

Вибір режиму залежить від конкретних вимог до безпеки та продуктивності системи.

У виборі алгоритмів шифрування потрібно відзначити важливість балансування між швидкодією та стійкістю. Наприклад, шифрування великих обсягів інформації на зовнішньому накопичувачі може суттєво знижувати продуктивність системи, особливо при використанні слабших обчислювальних потужностей. Тому при впровадженні необхідно здійснювати попереднє тестування продуктивності обраного рішення, враховуючи характер та обсяг оброблюваних даних.

Для забезпечення надійного захисту конфіденційної інформації на зовнішніх пристроях доцільно використовувати гібридні схеми шифрування, які поєднують швидкість симетричних алгоритмів, таких як AES, з безпекою асиметричних алгоритмів, таких як RSA. Правильний вибір режиму роботи блочного шифру також є критичним для забезпечення цілісності та конфіденційності даних.

2.2. Архітектура та компоненти DLP-системи для використання в системах безпечного зберігання конфіденційної інформації

Сучасні DLP-рішення поєднують класичні засоби захисту брандмауери, антивірусне ПЗ, засоби моніторингу мережі, контролі доступу до пристроїв) із передовими підходами, що базуються на штучному інтелекті, машинному навчанні та автоматизації процесів. Це дає змогу своєчасно виявляти, запобігати й аналізувати інциденти, пов’язані з витоком критично важливої інформації.

Існує п’ять ключових типів запобігання витоку даних DLP, кожен із яких охоплює окремі етапи роботи з інформацією:

1. Ідентифікація конфіденційних даних — це процес виявлення важливої інформації у цифровому середовищі організації, незалежно від її розташування: у корпоративній електронній пошті, хмарних сховищах, системах для спільної роботи чи інших програмних інструментах.

2. Виявлення витоку даних — автоматизована процедура фіксації спроб несанкціонованого привласнення, переміщення або поширення конфіденційної інформації, навіть якщо дані були викрадені або неправильно розміщені в інфраструктурі організації.

3. Data-in-Motion DLP — контроль за даними під час їхньої передачі мережею. Цей тип захисту забезпечує, щоб інформація досягала кінцевого пункту призначення цілісною та без втручання третіх осіб.

4. Data-at-Rest DLP — охоплює дані, що не переміщуються і зберігаються на дисках, у базах даних або файлових сховищах. Для їх захисту застосовуються різні методи — від шифрування до обмеження доступу на рівні кінцевих пристроїв або хмари.

5. Data-in-Use DLP — захист інформації, з якою наразі працюють користувачі. Система блокує або фіксує підозрілу активність, таку як копіювання, вставлення, друк, запис екрана або несанкціоноване переміщення файлів, запобігаючи можливому витоку або зловживанню. [38]

Системи запобігання витоку інформації поділяються також на три основні категорії за способом реалізації рішення:

1. Мережевий DLP. Цей тип системи контролює трафік у корпоративній мережі та в хмарних середовищах. DLP відстежує пересилання файлів, електронні листи, повідомлення, фіксує спроби порушення політик безпеки та веде журнал дій користувачів. Зокрема, створюється база даних, що фіксує факти доступу до чутливої інформації: хто, коли та куди здійснював передавання даних. Це дозволяє забезпечити повну прозорість переміщення критичних даних мережею компанії.

2. DLP на рівні кінцевих точок контролює пристрої, на яких зберігаються або використовуються дані: сервери, комп’ютери, ноутбуки, смартфони, зовнішні носії тощо. Endpoint DLP дозволяє запобігати втраті або несанкціонованому переміщенню інформації навіть за межами корпоративної мережі.

Також ця система допомагає класифікувати дані за рівнем критичності (конфіденційні, персональні, регламентовані законом тощо), що спрощує аудит та дотримання нормативних вимог.

3. Хмарний DLP є підмножиною мережевого DLP і зосереджений на захисті даних у хмарних сервісах. Cloud DLP автоматично виявляє та шифрує конфіденційну інформацію перед її завантаженням у хмару, зберігає перелік авторизованих сервісів і користувачів, а також веде облік доступу до даних. У разі порушення правил або підозрілої активності система повідомляє відповідальних осіб про інцидент. Такий підхід забезпечує наскрізну видимість усіх операцій із даними в хмарній інфраструктурі. [39]

В умовах зростання кількості кібератак, фішингових кампаній, інсайдерських загроз та витоків даних, організації дедалі частіше стикаються з необхідністю забезпечення надійного зберігання та контролю доступу до зовнішніх носіїв. До зовнішніх пристроїв, що використовуються для зберігання даних, належать USB-флеш-накопичувачі, зовнішні жорсткі диски HDD, твердотільні накопичувачі SSD, а також спеціалізовані захищені пристрої типу HSM і USB-ключі з апаратним шифруванням. Кожен із цих типів пристроїв має свої переваги й призначений для конкретних сценаріїв використання — від особистого застосування до забезпечення корпоративної політики безпеки.

Захищені зовнішні носії інформації вирізняються тим, що мають вбудовані механізми захисту, які можуть включати апаратне шифрування, біометричну автентифікацію, PIN-коди, засоби самознищення при спробах злому тощо [40]. Наприклад, деякі пристрої автоматично знищують ключі шифрування після кількох невдалих спроб входу, що унеможливлює розшифрування навіть за фізичного доступу до пристрою. Інші рішення передбачають авторизацію лише за наявності фізичного дотика до сенсора або з використанням одноразового коду, надісланого на зареєстрований пристрій.

USB-накопичувачі з апаратним шифруванням використовують мікросхему, яка автоматично шифрує дані при записі й дешифрує при зчитуванні. Найчастіше застосовуються алгоритми AES-256, що забезпечують високий рівень криптографічного захисту. Такі пристрої мають додаткові механізми захисту: вбудовані PIN-клавіатури, біометричні сенсори, автознищення вмісту після певної кількості невдалих спроб доступу [41]. Крім того, деякі моделі підтримують функції автозаблокування при неактивності або під час підключення до

неавторизованих пристроїв. Це суттєво знижує ризик несанкціонованого доступу у разі втрати або крадіжки накопичувача.

Компанії, що виробляють подібні пристрої, зокрема Kingston лінійка IronKey, Apricorn серія Aegis, Corsair, SanDisk і інші, орієнтовані на корпоративний сегмент, де вимоги до збереження конфіденційності особливо високі [42]. Ці виробники також забезпечують сертифікацію своїх продуктів відповідно до міжнародних стандартів, таких як FIPS 140-2, що гарантує відповідність певним рівням криптографічної безпеки. Для підприємств така відповідність є критично важливою при проходженні аудитів і впровадженні внутрішніх політик інформаційної безпеки.

Зовнішні жорсткі диски з вбудованим шифруванням — це пристрої, які здебільшого мають більший обсяг пам’яті та підходять для резервного копіювання великих обсягів даних. Деякі моделі підтримують автоматичне шифрування диска Full Disk Encryption на основі апаратних засобів. Прикладом є зовнішні диски від WD серії My Passport з апаратним шифруванням AES та програмним керуванням через фірмові утиліти [43]. Також такі пристрої часто підтримують додаткові функції, зокрема захист паролем, керування правами доступу на рівні користувача, а також автоматичне резервне копіювання даних із внутрішніх систем.

Твердотільні накопичувачі (SSD) з інтерфейсом USB або Thunderbolt також можуть оснащуватись засобами захисту інформації. Їхньою перевагою є висока швидкість обміну даними, що робить їх зручними для обробки великих масивів конфіденційної інформації. Окремі моделі мають вбудовані контролери з апаратною підтримкою шифрування та додатковим програмним забезпеченням для автентифікації [44]. Крім цього, SSD-накопичувачі стійкіші до фізичних пошкоджень, порівняно з HDD, що є додатковою перевагою в умовах мобільного або польового використання.

Смарт-карти та токени є частиною двофакторної автентифікації та служать як фізичні ключі для доступу до зашифрованої інформації. Вони можуть містити криптографічні ключі, сертифікати або навіть цілі шифрувальні модулі. USB-токени широко застосовуються в державних установах, банках, а також в

корпоративному IT-секторі [45]. Завдяки використанню апаратного захисту, такі пристрої забезпечують високий рівень безпеки при виконанні електронного цифрового підпису, автентифікації в системах електронного документообігу, або під час доступу до зашифрованих сховищ.

Крім того, актуальним є питання розмежування прав доступу до інформації, що зберігається на зовнішніх пристроях. У багатьох випадках реалізуються механізми автентифікації за допомогою смарт-карт, біометричних даних або одноразових паролів. Це дозволяє чітко контролювати, хто саме має доступ до захищених даних і в якій формі — лише для перегляду, редагування або повного копіювання. У результаті створюється багаторівнева модель захисту, що включає як ідентифікацію користувача, так і безпосередній контроль над шифруванням та дешифруванням даних [46]. Такі моделі також можуть інтегруватися з централізованими системами управління політиками доступу (наприклад, Active Directory або LDAP), що забезпечує масштабованість та ефективність безпеки в великих організаціях.

Апаратні HSM – це високозахищені пристрої, що використовуються для створення, збереження та управління криптографічними ключами. Вони мають вбудовану операційну систему та сертифіковані за стандартами безпеки(наприклад, FIPS 140-2 Level 3 або 4. HSM використовуються там, де необхідна максимальна безпека — в центрах обробки даних, банківських системах, сертифікаційних центрах [47]. Сучасні HSM також підтримують апаратне прискорення криптографічних операцій, що дозволяє значно зменшити затримки під час обробки транзакцій, шифрування/дешифрування повідомлень і генерування ключів.

У процесі розробки систем безпечного зберігання конфіденційної інформації особливу увагу також приділяють питанню надійного зберігання ключів шифрування. Відомо, що безпека будь-якої криптографічної системи напряму залежить від збереження та секретності криптографічних ключів. У зв’язку з цим все частіше використовуються апаратні модулі безпеки, які здатні генерувати, зберігати і управляти ключами у захищеному середовищі. Завдяки апаратним характеристикам такі модулі мають підвищену стійкість до фізичних

атак, зокрема до атак сторонніми каналами, наприклад аналізу електромагнітного випромінювання або споживання електроенергії [48]. Додатково вони можуть використовувати модулі виявлення вторгнень, системи журналювання подій безпеки та засоби дистанційного керування, що забезпечують високий рівень інтеграції в загальну систему інформаційної безпеки підприємства.

Safetica ONE є універсальним інструментом для захисту інформації, який ефективно протидіє витокам даних і внутрішнім загрозам. Система дозволяє своєчасно виявляти потенційні загрози безпеці, контролювати переміщення даних в інформаційному середовищі організації та забезпечувати надійний захист конфіденційної інформації. Однією з ключових переваг Safetica ONE є її здатність допомагати організаціям дотримуватися вимог чинного законодавства та нормативних документів у сфері захисту даних.

Крім того, програмне забезпечення надає можливість оперативного реагування на інциденти інформаційної безпеки завдяки функціям миттєвого сповіщення та створення детальних звітів. Рішення відзначається простотою у впровадженні та масштабованістю, що робить його придатним для підприємств будь-якого розміру. [49]

Як комплексне корпоративне рішення, Safetica ONE охоплює всі аспекти захисту від внутрішніх ризиків, пов'язаних з витоком або ненавмисним розголошенням цінної інформації. Програмне забезпечення мінімізує вплив людського фактору та зловмисних дій за рахунок превентивного виявлення загроз і активного запобігання витоку даних. Це сприяє запобіганню небажаній поведінці всередині організації та оптимізує витрати на забезпечення інформаційної безпеки.

На рисунку представлено типову архітектуру DLP-системи в корпоративному середовищі (рис.2.2).

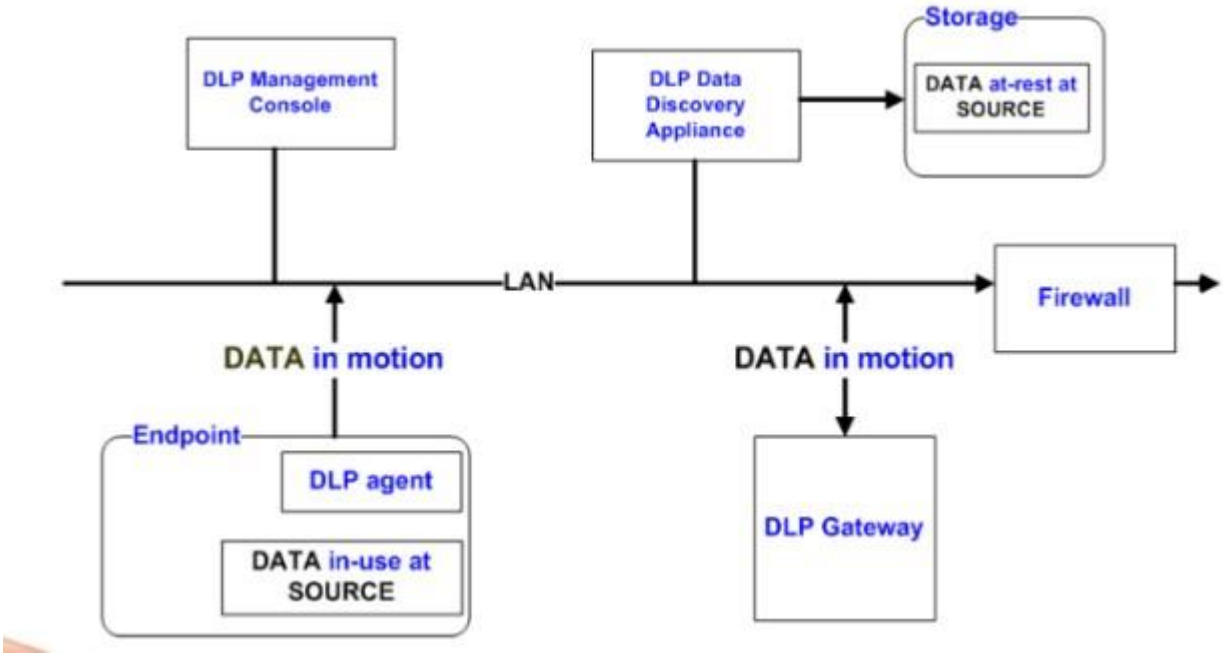


Рисунок 2.2– Типова архітектура DLP системи

Safetica ONE являє собою універсальне програмне рішення, призначене для запобігання витокам даних і нейтралізації інсайдерських загроз. Воно забезпечує ефективне виявлення потенційних ризиків інформаційної безпеки, дозволяє здійснювати контроль над передачею даних та гарантує захист конфіденційної інформації. Окрім цього, Safetica ONE сприяє дотриманню вимог законодавчих та регуляторних актів у сфері захисту даних, забезпечуючи відповідність корпоративної політики безпеки актуальним стандартам.

Користувачам надається можливість оперативного реагування на загрози завдяки функції миттєвих сповіщень про інциденти, а також через доступ до розширених аналітичних звітів. Важливо зазначити, що система відзначається простотою встановлення та налаштування, а також масштабованістю, що робить її придатною для організацій будь-якого розміру. [50]

Як рішення корпоративного рівня, Safetica ONE охоплює всі ключові аспекти внутрішніх загроз, пов’язаних із ненавмисним або навмисним витоком важливої інформації. Система ефективно захищає дані від помилок працівників і навмисних дій зловмисників, запобігаючи витоку ще до того, як інцидент набуде критичного характеру. Застосування функцій контролю використання програмного забезпечення та веб-ресурсів дозволяє сформувати захищене

інформаційне середовище та зменшити периметр потенційних ризиків. Такий підхід сприяє запобіганню небажаній активності в межах компанії та оптимізації витрат на забезпечення кібербезпеки.

З метою порівняння ефективності та рівня безпеки різних типів зовнішніх пристроїв, у таблиці 2.1 наведено основні характеристики та їх застосування в системі захисту конфіденційної інформації за допомогою Safetica ONE.

Таблиця 2.1– характеристики в системі захисту конфіденційної інформації

Тип пристрою/ середовища	Рівень захисту	Механізми захисту	Швидкість доступу	Додаткові засоби безпеки	Сфера застосування
USB-флешка	Високий	Контроль копіювання, моніторинг файлів, блокування незахищених USB	Висока	Виявлення конфіденційних даних, звітність про дії, офлайн-контроль	Персональне та корпоративне використання
Зовнішній жорсткий диск (HDD/SDD)	Середній –високий	Класифікація даних, контроль передачі, політики доступу	Висока	Автоматичне шифрування, повідомлення про інциденти, контроль поза мережею	Резервне копіювання, передача даних, робота з віддаленими пристроями
Хмарне середовище (OneDrive, Google Drive)	Високий	Cloud DLP, політики контролю хмарних сервісів	Висока	Контроль доступу, блокування/реагування на аномалії, журналювання	Спільна робота з файлами, віддалена робота, хмарні офіси
Електронна пошта та месенджери	Високий	Network DLP, контроль Data-in-Motion	Залежить від каналу	Аналіз вкладень, ключових слів, блокування чи шифрування перед відправленням	Обмін діловими файлами, внутрішня та зовнішня комунікація

Як видно з таблиці 2.1, аналіз функціональних можливостей Safetica ONE засвідчує її високу ефективність як рішення класу DLP для захисту конфіденційної інформації на рівні підприємства. Програма забезпечує всебічний контроль за обробкою даних, запобігає витокам інформації через зовнішні пристрої, хмарні сервіси або мережеві канали, а також надає інструменти для аналітики та відповідності вимогам безпеки. Зручний інтерфейс, гнучкі налаштування політик доступу та інтеграція з іншими IT-системами роблять Safetica ONE доцільним вибором для організацій, які прагнуть впровадити комплексну систему захисту від несанкціонованого доступу та втрати конфіденційних даних.

Усі перевірені інциденти та журнали можна автоматично надсилати до рішень SIEM, наприклад Splunk, IBM QRadar, LogRhythm або ArcSight, для подальшого дослідження. REST API надає зібрані дані таким інструментам, як Power BI або Tableau, для розширеного аналізу (рис.2.3).

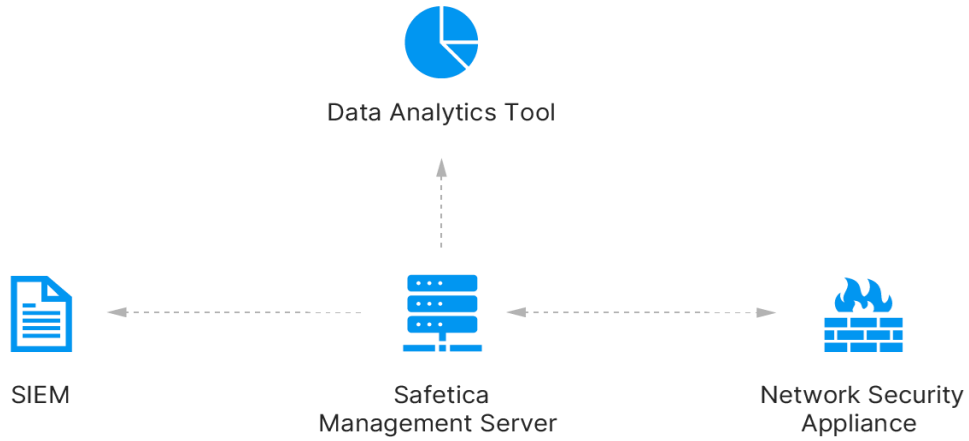


Рисунок 2.3– Схема надсилання звітів Safetica

Safetica забезпечує всебічний захист конфіденційної інформації незалежно від місця її зберігання чи формату. До категорій даних, які підлягають захисту, належать:

– персональні відомості;

– стратегічні документи компанії;

– клієнтські бази даних;

– платіжна інформація, зокрема номери банківських карток;

– об’єкти інтелектуальної власності;

– промислові зразки, комерційні таємниці, ноу-хау;

– контракти та інші критично важливі документи.

Рішення Safetica відповідає вимогам основних міжнародних стандартів і регуляцій у сфері захисту даних, зокрема: GDPR, HIPAA, SOX, PCI-DSS, GLBA, ISO/IEC 27001, CCPA. Це дозволяє організаціям дотримуватися чинного законодавства та галузевих норм без необхідності суттєвих змін у внутрішніх процесах. Крім того, Safetica сприяє підвищенню рівня обізнаності персоналу, навчаючи правилам роботи з конфіденційною інформацією у звичному робочому середовищі.

Програмне забезпечення спроектоване для швидкого впровадження без залучення висококваліфікованих спеціалістів або додаткових ресурсів. Уже протягом кількох годин після початкового налаштування можна забезпечити захист важливої інформації шляхом визначення безпечних каналів передачі даних і встановлення базових політик безпеки.

Система також здатна розпізнавати потенційно небезпечні дії або ризикові ситуації. Залежно від режиму роботи, Safetica може автоматично блокувати підозрілу активність, повідомляти адміністратора або ненав’язливо нагадувати працівникам про встановлені правила інформаційної безпеки.

Окремим функціональним компонентом є Safetica Discovery, який виконує роль інструмента аудиту та моніторингу. Він дає змогу виявляти способи використання корпоративних даних незалежно від їхнього розташування чи шляху переміщення. Аналіз логів та історії дій користувачів дозволяє вчасно виявляти потенційні витоки інформації, а також формувати цілісне уявлення про внутрішні процеси компанії. Завдяки цьому організації отримують змогу глибше розуміти приховані загрози та оптимізувати систему захисту.

Safetica Protection забезпечує створення безпечного інформаційного середовища в межах організації, сприяє підвищенню обізнаності працівників щодо інформаційної безпеки, виявляє потенційні ризики та захищає корпоративні

дані від несанкціонованого доступу. Система дозволяє гнучко налаштовувати політики безпеки для всіх каналів передавання інформації, що забезпечує адаптацію до специфіки бізнес-процесів.

Залежно від потреб компанії, можна обрати відповідну реакцію на інциденти: від простого аудиту або сповіщення до автоматичного блокування дій, що суперечать політиці безпеки. У процесі взаємодії з конфіденційною інформацією користувач отримує сповіщення про потенційне порушення встановлених правил, що підвищує рівень обережності та впевненості персоналу при роботі з критичними даними.

Система дозволяє реалізовувати точні сценарії обробки цінної інформації відповідно до внутрішніх політик компанії. Захист функціонує не лише в онлайн-режимі, але й при відсутності з'єднання з мережею. Усі дії, здійснені в офлайн-режимі, синхронізуються з сервером одразу після відновлення доступу до мережі, зберігаючи цілісність системи контролю.

Safetica Protection також контролює всі підключені до системи пристрої, запобігаючи використанню незареєстрованих або неавторизованих носіїв. Система обмежує доступ до портативних пристроїв, забезпечує моніторинг корпоративних мобільних рішень і дозволяє відстежувати переміщення даних із хмарного середовища, зокрема сервісів на зразок Microsoft Office 365 (рис. 2.4).

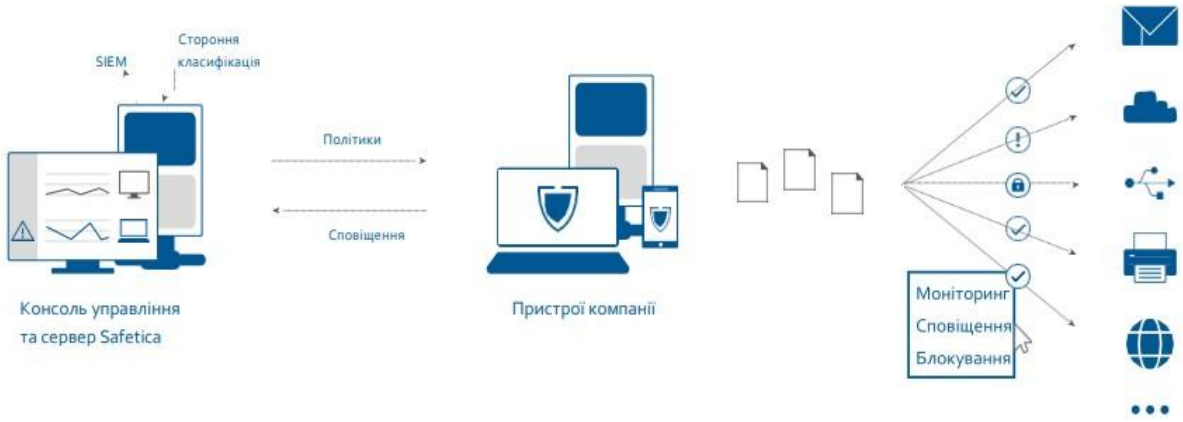


Рисунок 2.4– Схема роботи Safetica

2.3. Проєктування структурної та функціональної схеми системи

Проєктування системи безпечного зберігання конфіденційної інформації на зовнішніх пристроях є критичним етапом у забезпеченні її захисту від несанкціонованого доступу, витоку або модифікації. Така система має забезпечувати не лише конфіденційність, а й цілісність, доступність та контрольованість даних протягом усього циклу їхнього зберігання та обробки. Ці принципи відомі як тріада CIA і є основою інформаційної безпеки.

У контексті зовнішніх носіїв, таких як USB-накопичувачі та портативні SSD, забезпечення конфіденційності означає, що лише авторизовані користувачі можуть отримати доступ до даних. Цілісність гарантує, що дані не були змінені або пошкоджені без дозволу, а доступність забезпечує, що авторизовані користувачі можуть отримати доступ до даних, коли це необхідно [51].

Для досягнення цих цілей, системи безпечного зберігання повинні бути спроєктовані з урахуванням принципів "безпеки за дизайном" Secure by Design, що передбачає інтеграцію заходів безпеки на всіх етапах розробки та експлуатації системи. Це включає використання шифрування, автентифікації, контролю доступу та моніторингу для виявлення та запобігання потенційним загрозам.

Згідно з підручником «Захист інформації в комп'ютерних системах», ефективне проєктування таких систем передбачає врахування сучасних загроз, таких як несанкціонований доступ, витік даних та їх модифікація. Система повинна гарантувати конфіденційність, цілісність, доступність та контрольованість інформації на всіх етапах її життєвого циклу [52].

Важливо враховувати нормативно-правові вимоги, такі як відповідність стандартам ISO/IEC 27001, NIST SP 800-53, GDPR (якщо система працює з персональними даними), що дозволяє забезпечити не лише технічну, а й юридичну захищеність даних.

Крім того, важливо враховувати фізичні аспекти безпеки зовнішніх пристроїв, такі як захист від механічних пошкоджень, впливу температури та вологи, особливо якщо пристрої використовуються в польових умовах або в середовищах з підвищеним рівнем ризику. Використання промислових флеш-

накопичувачів зі спеціальним захистом від впливу зовнішнього середовища може значно підвищити загальний рівень безпеки системи.

Функціональна схема, у свою чергу, визначає послідовність операцій, які забезпечують захист інформації. Вона починається з етапу автентифікації користувача через введення PIN-коду, паролю або за допомогою біометричних даних. У разі успішної ідентифікації активується модуль дешифрування даних або надається доступ до віртуального зашифрованого контейнера. При цьому зчитування й запис інформації відбуваються лише через внутрішній криптографічний процесор пристрою [53].

Структурна схема системи включає основні компоненти: зовнішній носій інформації з вбудованими засобами шифрування, програмне забезпечення для управління доступом, інтерфейси підключення до комп'ютерної системи, систему автентифікації користувача та централізовану службу адміністрування. У разі корпоративного використання до структури може також входити сервер управління ключами Key Management Server, який відповідає за розподіл, зберігання та ротацію криптографічних ключів [54].

Система автентифікації може підтримувати кілька факторів, включаючи введення пароля, біометричну перевірку та апаратні токени. Централізована служба адміністрування дозволяє IT-відділу віддалено моніторити стан пристроїв, оновлювати політики безпеки та блокувати доступ у разі втрати або крадіжки носія.

Важливою функцією є реалізація політик автоматичного блокування доступу до накопичувача після закінчення сесії, тривалого простою або при спробі фізичного втручання у пристрій. Крім того, передбачено засоби ведення журналу дій користувача, що дає змогу виявляти підозрілу активність та запобігати витоку даних.

Для наочного уявлення про складові елементи системи безпечного зберігання конфіденційної інформації на зовнішніх пристроях нижче подано структурну схему, яка демонструє основні компоненти системи та їх взаємозв'язок (рис. 2.5).

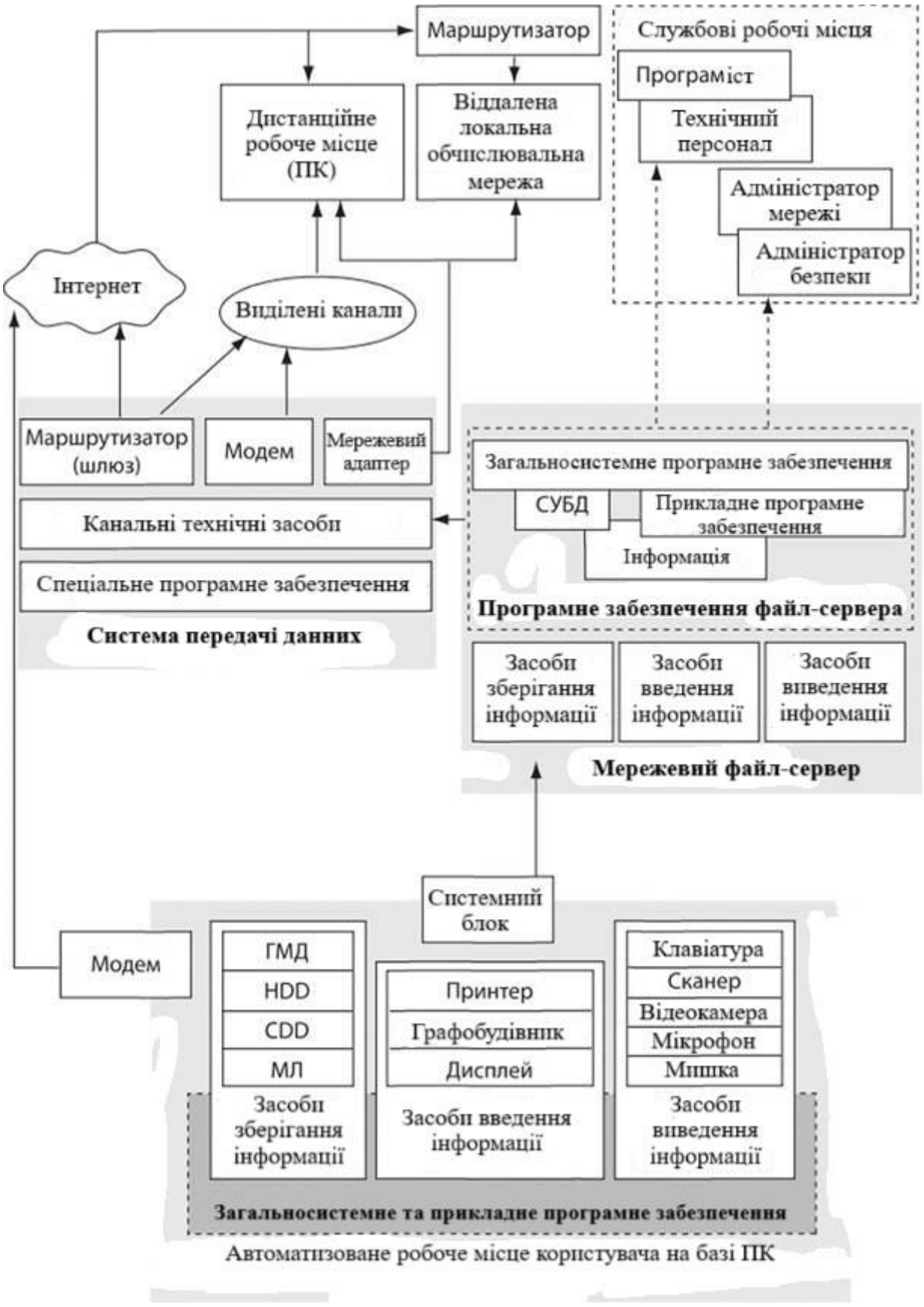


Рисунок 2.5– Структурна схема захисту даних на зовнішньому накопичувачі [3]

Як видно зі схеми, система побудована таким чином, щоб забезпечити багаторівневий захист даних за допомогою апаратних і програмних засобів.

Кожен компонент виконує визначену функцію, спрямовану на підтримання конфіденційності, цілісності та доступності інформації.

Важливою функцією є реалізація політик автоматичного блокування доступу до накопичувача після закінчення сесії, тривалого простою або при спробі фізичного втручання у пристрій. Крім того, передбачено засоби ведення журналу дій користувача, що дає змогу виявляти підозрілу активність та запобігати витоку даних.

Функціональна схема відображає стадії забезпечення безпеки у виробничому процесі. Для забезпечення даного процесу, задіяні позаштатні адміністратори служби захисту інформації. Кожен етап захисту інформаційної безпеки установи/організації, супроводжується організаційнорозпорядчою документацією, яка регламентує діяльність СЗІ і персоналу щодо конкретного захисного процесу.

Результатом такого підходу має бути безпечне та компетентне діловодство установи [55].

Для підвищення стійкості системи до зовнішніх атак важливо передбачити підтримку апаратного шифрування за алгоритмами AES, а також використання надійного протоколу з’єднання (наприклад, USB-C з апаратним захистом або Thunderbolt з підтримкою шифрування каналу). Пристрій також повинен мати захист від brute-force атак – наприклад, шляхом автоматичного знищення ключа шифрування після кількох невдалих спроб автентифікації [56].

Не менш важливою є і стійкість зовнішніх пристроїв до механічних впливів, перепадів температури, вологи тощо, адже в багатьох випадках вони використовуються в польових умовах або в середовищах з підвищеним рівнем ризику. У таких випадках застосовуються промислові флеш-накопичувачі зі спеціальним захистом від впливу зовнішнього середовища. Зазвичай вони мають металеві або герметизовані корпуси, стійкі до пилу та води, а також використовують алгоритми самодіагностики для виявлення можливих збоїв [57].

Централізоване адміністрування системи передбачає можливість дистанційного керування доступом до накопичувача, зміну паролів, блокування або знищення вмісту в разі втрати пристрою. Це забезпечується або за допомогою

спеціалізованого ПЗ виробника пристрою, або за допомогою вбудованих сервісів у корпоративному середовищі, наприклад, через Active Directory або системи управління політиками безпеки GPO.

Візуалізація структурної та функціональної схеми дозволяє наочно продемонструвати взаємозв'язки між компонентами системи, а також розподіл ролей між апаратними та програмними елементами. Зокрема, система може бути реалізована за моделлю «endpoint device – user – security gateway – central server», де кожен з компонентів виконує чітко визначену функцію захисту [58].

Проєктування такої системи має базуватись на принципах гнучкості, масштабованості та сумісності з сучасними стандартами безпеки. Це дозволяє адаптувати систему до змін у законодавстві, зростаючих обсягів інформації, а також нових загроз кібербезпеки.

У результаті, грамотно спроєктована система безпечного зберігання конфіденційної інформації на зовнішніх пристроях є основою побудови надійної цифрової інфраструктури як для особистого використання, так і для потреб підприємств та організацій, що оперують чутливою інформацією [59].

Окрім базової архітектури, при проєктуванні структурної схеми доцільно також враховувати логічну взаємодію між компонентами системи безпеки. Це включає як внутрішні модулі пристрою (шифрувальний чип, контролер доступу, пам'ять), так і зовнішні сервіси (сервер аутентифікації, системи моніторингу, резервне копіювання). Наприклад, у сучасних системах можливе впровадження TPM або Secure Enclave – апаратних рішень для зберігання ключів та забезпечення апаратного кореня довіри [60].

У функціональному аспекті ефективна система має передбачати декілька рівнів захисту: базову автентифікацію, шифрування, контроль доступу на основі політик RBAC а також аудит подій. Це дозволяє реалізувати концепцію Zero Trust Architecture — коли кожен запит до системи перевіряється незалежно від його джерела. Такий підхід значно знижує ймовірність компрометації навіть при проникненні у внутрішнє середовище мережі.

Сучасні архітектури систем безпечного зберігання конфіденційної інформації на зовнішніх пристроях також активно інтегрують принципи нульової

довіри ZTA. Це означає, що жодному компоненту системи не надається довіра за замовчуванням. Будь-який доступ до ресурсів повинен бути перевірений і дозволений лише після відповідної автентифікації, авторизації та оцінки контексту звернення. Таким чином, навіть у разі успішного проникнення зловмисника в одну частину системи, він не зможе автоматично отримати доступ до всіх даних [61].

Крім цього, доцільно враховувати можливість створення віртуальних сегментів на пристрої для ізоляції інформації різного ступеня конфіденційності. Такий підхід широко застосовується у корпоративних системах з багаторівневим доступом, зокрема у фінансових структурах або державних установах.

Одним із важливих компонентів функціональної схеми є механізм відновлення доступу у разі втрати пароля або ключа. Це може бути реалізовано через резервні ключі, збережені у захищених сховищах, або з використанням многофакторної автентифікації (наприклад, одноразовий код, резервна адреса електронної пошти, біометричні дані). У таких системах важливо дотримуватись балансу між зручністю користування та рівнем безпеки.

Також необхідно впровадити алгоритми виявлення аномальної активності. Це дозволяє виявити підозрілі спроби доступу або передачі даних — наприклад, спробу підключення пристрою до неавторизованого комп’ютера чи зчитування великого обсягу інформації за короткий час. У таких випадках система має автоматично запускати процедури блокування або повідомлення адміністратора.

Візуалізація структури та функціоналу може бути представлена у вигляді діаграми типу DFD, або у вигляді схемного подання з поясненням потоків даних, точок контролю доступу, вузлів шифрування/дешифрування, а також логіки реагування на загрози [62].

Ще одним цікавим напрямом, що активно досліджується та впроваджується, є поєднання технологій блокчейн із системами захисту інформації на зовнішніх пристроях. У цьому контексті блокчейн може виступати як механізм ведення незмінного журналу доступу до даних, що дозволяє точно встановити, хто, коли і з якою метою звертався до тих чи інших записів.

Загалом, структура системи безпечного зберігання даних на зовнішніх пристроях повинна охоплювати такі основні компоненти:

1. Зовнішній накопичувач із вбудованим криптомодулем;
2. Засоби аутентифікації користувача;
3. Інтерфейс управління;
4. Програмні засоби шифрування/дешифрування;
5. Лог-файли подій;
6. Система захисту від фізичних і логічних атак;
7. Механізми резервного копіювання та відновлення.

Окремої уваги заслуговує сертифікація безпеки апаратного та програмного забезпечення. На міжнародному рівні найбільш визнаними є сертифікати FIPS 140-2/3 (США) та Common Criteria (Європа), які підтверджують відповідність пристроїв вимогам захисту інформації.

Крім технологічного аспекту, не менш важливою є організаційна складова забезпечення захисту даних. Зокрема, йдеться про створення та впровадження політик інформаційної безпеки, що регламентують порядок використання зовнішніх пристроїв, вимоги до резервного копіювання, ведення логів та регулярного оновлення програмного забезпечення. Часто проблема несанкціонованого доступу виникає не через недосконаліть технічних засобів, а через людський фактор — необережність або недотримання внутрішніх інструкцій.

Також необхідно розглянути аспект фізичної безпеки зовнішніх носіїв. Наприклад, пристрій із зашифрованою інформацією може бути вкрадений або загублений. У таких випадках важливо, щоб реалізована система захисту могла гарантувати, що дані не будуть розшифровані сторонніми особами навіть у разі повного фізичного доступу до носія. Це досягається шляхом впровадження функцій самознищення ключа, блокування при багаторазовому введенні неправильного пароля або навіть автоматичного стирання інформації за певних умов [63].

2.4. Висновки

У другому розділі було проаналізовано еволюцію, типи та функціональні особливості зовнішніх пристроїв, призначених для безпечного зберігання конфіденційної інформації. Дослідження показало, що розвиток зовнішніх носіїв інформації тісно пов’язаний із загальним прогресом інформаційних технологій, а також із зростаючими вимогами до захисту даних в умовах підвищених кіберзагроз і нормативного регулювання.

Ще система DLP є ключовим інструментом для забезпечення цілісності, конфіденційності та безпеки корпоративної інформації. Такі рішення, як Safetica ONE, дозволяють виявляти загрози, запобігати витоку даних, контролювати дії користувачів і відповідати вимогам міжнародних стандартів. Їх впровадження сприяє формуванню безпечного цифрового середовища на підприємстві та підвищує загальний рівень інформаційної безпеки.

Окрему увагу приділено характеристикам і класифікації сучасних пристроїв, серед яких найбільш ефективними з точки зору безпеки є USB-накопичувачі з апаратним шифруванням, захищені SSD, апаратні токени та HSM-модулі. Ці пристрої мають вбудовані механізми захисту, такі як криптографічні алгоритми AES-256, біометрична автентифікація, PIN-коди, самознищення даних, а також сертифікацію відповідно до міжнародних стандартів безпеки.

Було здійснено проєктування структурної та функціональної схеми системи безпечного зберігання конфіденційної інформації, яка поєднує апаратні та програмні засоби захисту. Запропонована модель системи охоплює ключові етапи: автентифікацію користувача, шифрування/дешифрування інформації, моніторинг активності, політики доступу та централізоване адміністрування. Важливу роль відіграють функції багаторівневого контролю доступу, логування подій, підтримка протоколів безпечного з’єднання та інтеграція з інфраструктурою довіри TPM.

3 РЕАЛІЗАЦІЯ СИСТЕМИ БЕЗПЕЧНОГО ЗБЕРІГАННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ НА ЗОВНІШНІХ ПРИСТРОЯХ

3.1 Програмно – апаратні засоби безпечного зберігання інформації

Серед сучасних програмних рішень, що використовуються для забезпечення захисту конфіденційної інформації на зовнішніх пристроях, важливе місце займають системи класу DLP. Основним завданням таких систем є запобігання витоку чутливої інформації за межі корпоративної мережі, зокрема через зовнішні носії даних.

DLP-системи реалізують контроль дій користувачів із зовнішніми пристроями, включаючи USB-флешки, зовнішні жорсткі диски, SD-карти та мобільні пристрої, що підключаються як накопичувачі. У рамках такого контролю здійснюється:

– моніторинг операцій копіювання та переміщення файлів;

– автоматичне блокування дій, що не відповідають політикам безпеки;

– ідентифікація типу переданих даних (наприклад, номери платіжних карт, ПІБ, комерційна інформація);

– ведення детального журналу подій і створення звітів для служби безпеки.

Впровадження DLP-систем дозволяє гарантувати високий рівень контролю за переміщенням інформації та запобігати витоку важливих даних через фізичні канали, що раніше були важко контрольованими. Це робить такі системи надзвичайно актуальними у процесі забезпечення інформаційної безпеки в сучасних організаціях.

Варто зазначити, що DLP може інтегруватися з антивірусами, SIEM-системами, засобами автентифікації, створюючи комплексну систему захисту. Таким чином, DLP — це не лише засіб виявлення загроз, а й активний інструмент запобігання несанкціонованому доступу до інформації.

Одним із яскравих прикладів ефективного програмного рішення у сфері захисту інформації є Safetica ONE — система, що забезпечує комплексний контроль за діями користувачів із даними та попереджає несанкціоновані дії з конфіденційною інформацією.

Safetica ONE дозволяє підприємствам:

– блокувати або дозволяти використання зовнішніх пристроїв залежно від політик безпеки;

– контролювати копіювання файлів на USB-накопичувачі, зокрема із застосуванням контекстного аналізу вмісту;

– виявляти порушення у режимі реального часу та оперативно реагувати на інциденти;

– створювати детальні звіти про дії користувачів з файлами, пристроями та інтерфейсами введення/виведення;

– застосовувати класифікацію даних з позначенням рівня їхньої критичності.

Важливою перевагою Safetica є її інтеграція з Active Directory, що дозволяє централізовано керувати політиками контролю доступу для конкретних працівників або груп користувачів.

Крім того, Safetica пропонує функціонал виявлення спроб обходу системи захисту, а також автоматичного шифрування файлів, які переміщуються на зовнішні носії. Це унеможливлює подальше використання таких файлів сторонніми особами у разі втрати або крадіжки носія.

Загалом Safetica ONE є ефективним інструментом для організацій, які прагнуть унеможливити витік критично важливої інформації через фізичні канали, зокрема через зовнішні накопичувачі. Використання цього рішення дозволяє сформувати надійну інфраструктуру інформаційної безпеки з мінімальними витратами на адміністрування.

Система безпечного зберігання конфіденційної інформації на зовнішніх пристроях має забезпечувати захист даних від спроб несанкціонованого доступу навіть у разі фізичної втрати або крадіжки носія. Основним принципом, який лежить в основі такої системи, є використання програмно-апаратного підходу, що поєднує шифрування, автентифікацію, контроль доступу, журналювання подій і реагування на загрози в режимі реального часу.

Розроблена система складається з кількох взаємопов’язаних модулів, які реалізують повний цикл захисту конфіденційної інформації:

1. Криптографічний модуль системи

Ключовим елементом захисту є криптографічний модуль, який реалізує алгоритми шифрування та дешифрування даних. Для захисту конфіденційної інформації використовуються сучасні криптографічні алгоритми, які забезпечують високий рівень безпеки при обробці та зберіганні даних. Одним із таких є AES-256, який є одним з найбільш надійних алгоритмів симетричного шифрування. AES-256 забезпечує шифрування даних за допомогою ключа довжиною 256 біт, що забезпечує достатній рівень захисту від атак перебору ключів brute force.

Модуль шифрування працює в режимі CBC**,** що дозволяє забезпечити високий рівень захисту даних за допомогою ідентифікаційного вектора IV, який генерується випадковим чином для кожної сесії. Це гарантує, що однакові дані при шифруванні будуть мати різний зашифрований вигляд, що робить їх менш уразливими до атак. Після шифрування даних для забезпечення цілісності інформації використовуються хеш-функції, зокрема SHA-256. Хеш-функція дозволяє визначити, чи не була змінена інформація, що зберігається, під час її обробки або передавання.

Перевагою такого підходу є те, що навіть при втраті чи крадіжці пристрою, збережена інформація залишатиметься захищеною від несанкціонованого доступу без відповідного ключа дешифрування.

2. Модуль автентифікації користувача

Для забезпечення доступу лише авторизованим користувачам використовується модуль автентифікації, який є важливою складовою частиною системи безпеки. Модуль відповідає за перевірку особи користувача за допомогою різних методів автентифікації, включаючи паролі**,** токени (апаратні або програмні) та біометричні дані (відбитки пальців, розпізнавання обличчя тощо). Це дозволяє реалізувати двофакторну автентифікацію, коли для доступу до системи потрібно ввести пароль та пройти додаткову перевірку, наприклад, за допомогою спеціального токена або біометрії.

Модуль автентифікації захищає від атак перебору паролів, обмежуючи кількість спроб введення неправильних даних. Також застосовуються механізми

затримки між спробами, щоб ускладнити здійснення атак методом brute-force. Після успішної автентифікації користувач отримує доступ до зашифрованого контейнера, в якому зберігаються конфіденційні дані.

3. Контейнер віртуального шифрованого диска

Всі дані зберігаються в спеціальному контейнері, що являє собою віртуальний шифрований диск. Такий контейнер є єдиним об’єктом, що містить зашифровані файли, та працює як окремий диск в операційній системі. Після монтування контейнера користувач може взаємодіяти з ним, як із звичайним диском, зберігаючи або зчитуючи файли. Однак ці файли насправді зберігаються в зашифрованому вигляді на носії.

Важливим є те, що всі дані в контейнері шифруються за допомогою алгоритму AES-256, а також для додаткового захисту можна використовувати методи цілісності наприклад, SHA-256, щоб упевнитися, що файли не були змінені або підроблені. Крім того, важливим є те, що після завершення роботи з контейнером його автоматично демонтують, а всі ключі та сесійні дані очищуються з оперативної пам’яті. Це знижує ризик доступу до конфіденційної інформації, навіть якщо пристрій потрапить у руки несанкціонованих осіб.

4. Модуль контролю доступу

Модуль контролю доступу є важливим інструментом, який перевіряє не тільки особу користувача, а й його права на доступ до конкретних даних. Для цього кожен користувач має певний рівень доступу, що визначає, які саме файли або функції доступні для перегляду, редагування чи видалення. Цей підхід дозволяє забезпечити політику мінімальних прав, коли користувачі мають доступ лише до тих ресурсів, які їм необхідні для виконання своїх функцій.

Контроль доступу може бути здійснено через рольову модель доступу (RBAC), де кожному користувачу або групі користувачів призначаються конкретні ролі та права доступу до файлів чи функцій системи. Такий підхід дозволяє забезпечити більш гнучкий контроль за використанням даних.

5. Модуль журналювання та аудиту

Для моніторингу активності користувачів і виявлення можливих спроб несанкціонованого доступу необхідно впровадити систему журналювання. Всі

важливі події, такі як успішні та неуспішні спроби автентифікації, підключення або відключення пристроїв, зміни налаштувань безпеки, записуються в спеціальний журнал. Цей журнал має бути зашифрований, щоб запобігти його підробці.

Завдяки модулю журналювання можна відстежувати діяльність користувачів, виявляти несанкціоновані спроби доступу або підозрілі операції та вчасно вжити заходів для запобігання витоку або пошкодження даних.

6. Апаратний детектор пристрою

Апаратний детектор пристрою є важливою складовою частиною системи, яка перевіряє ідентифікатор підключеного пристрою перед тим, як дозволити доступ до даних. Цей компонент перевіряє, чи є підключений USB-пристрій або інший зовнішній носій даних авторизованим. Пристрій ідентифікується за його унікальним серійним номером або іншим ідентифікатором, який записаний у системі як допустимий.

Якщо пристрій не відповідає жодному з відомих ідентифікаторів, система блокує доступ до даних і генерує сигнал тривоги. Це запобігає використанню несанкціонованих або підроблених пристроїв, що можуть бути використані для виведення даних або їх пошкодження.

7. Інтерфейс управління системою

Інтерфейс користувача є критично важливим для того, щоб користувач міг зручно та ефективно взаємодіяти з усіма функціями системи. Інтерфейс забезпечує зручний доступ до всіх функцій безпеки: автентифікація, моніторинг журналу подій, управління зашифрованими контейнерами, зміна налаштувань безпеки. Важливим є те, що користувач не має необхідності взаємодіяти з технічними аспектами шифрування, що спрощує використання системи. Всі процеси шифрування та дешифрування відбуваються на фоні, а користувач взаємодіє лише з віртуальним диском, що забезпечує безпечне зберігання даних.

У розробці було використано модель багаторівневого захисту, відповідно до якої доступ до інформації можливий лише після проходження кількох етапів ідентифікації та перевірки цілісності системи.

Загальна структурна схема рішення передбачає наявність наступних функціональних блоків:

1. Інтерфейс користувача – відображає всі дії, пов’язані з відкриттям доступу до зашифрованих даних, веденням логів та налаштуваннями користувача.

2. Модуль криптографічного захисту – відповідає за шифрування/дешифрування даних за допомогою алгоритму AES-256 у режимі CBC із випадковим IV.

3. Контейнер віртуального шифрованого диска – забезпечує логічне розмежування доступу, зберігає дані у вигляді одного зашифрованого файлу.

4. Модуль контролю доступу – перевіряє введений користувачем пароль або токен і дозволяє або забороняє монтування контейнера.

5. Журнальний модуль – фіксує усі спроби входу, зміни конфігурацій, підключення до зовнішнього носія тощо.

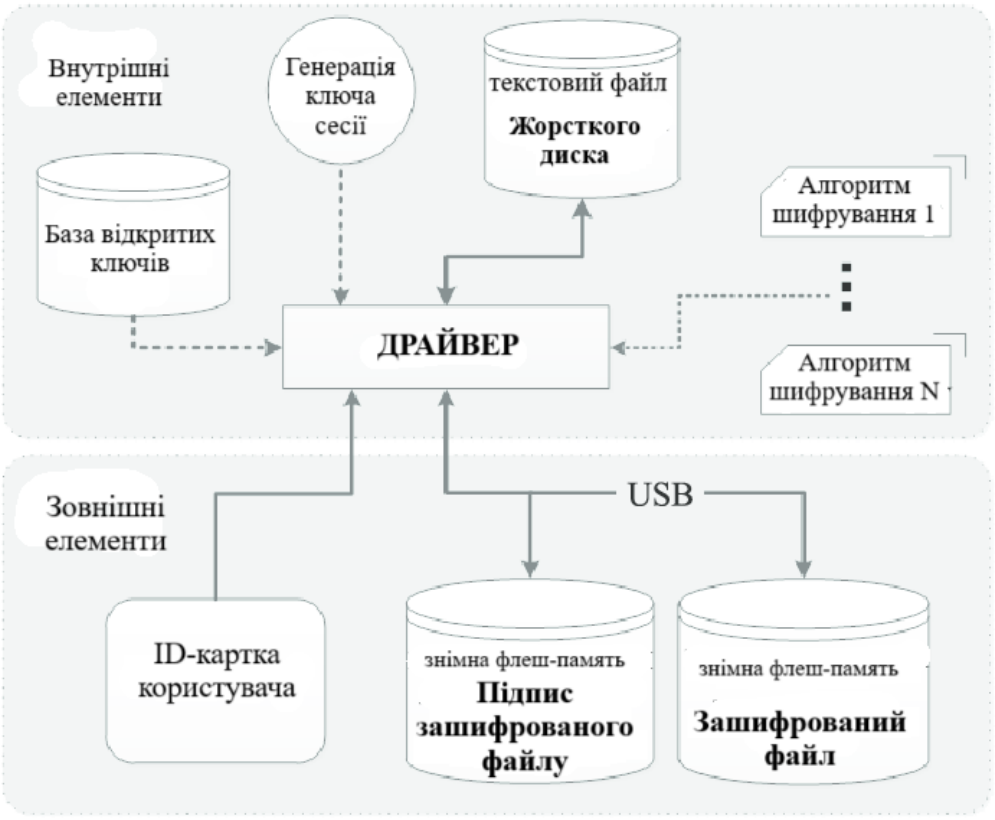


Рисунок 3.1 – Структурна схема взаємодії модулів системи [3]

Ця схема демонструє взаємодію між внутрішніми та зовнішніми компонентами системи захисту даних на зовнішньому носії. Вона ілюструє, як

дані шифруються та зберігаються, а також як здійснюється доступ до них через автентифікацію користувача.

Етап 1. Формування технічних вимог.

Спочатку було складено перелік функціональних та нефункціональних вимог. Серед основних вимог – безпечне зберігання, простота інтеграції з будь-якими USB-носіями, захист від фізичного доступу, наявність системи журналювання. Окремо було встановлено, що вся обробка даних має відбуватись локально без передачі через мережу.

Етап 2. Проєктування користувацького інтерфейсу.

Розроблено макети інтерфейсу з вікном авторизації, головною панеллю керування, формою перегляду логів, елементами керування файлами. Важливим аспектом стала реалізація простої взаємодії — користувач бачить лише віртуальний диск і не має справу з криптографічними параметрами (рис.3.2).

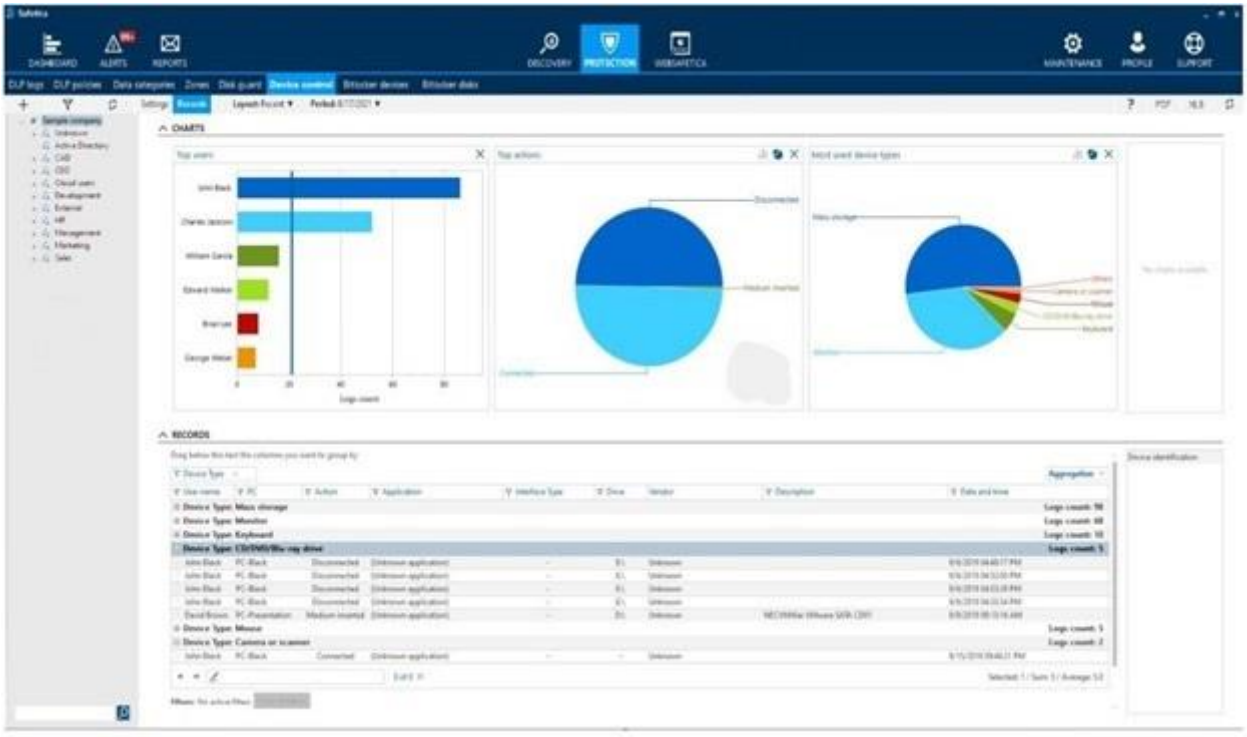


Рис. 3.2 – Інтерфейс консолі управління Safetica ONE

Цей макет ілюструє інтерфейс користувача програми для шифрування даних. Він включає вікно авторизації, панель управління файлами та журнал подій, що відповідає описаному в тексті інтерфейсу.

Етап 3. Побудова криптографічного модуля.

Ключ шифрування генерується на основі пароля користувача та сольового значення, яке зберігається на пристрої. Шифрування відбувається за стандартом AES-256 з ініціалізаційним вектором, який оновлюється кожного разу при новій сесії. Для забезпечення цілісності використовується SHA-256 хеш.

Етап 4. Побудова модуля роботи з контейнерами.

Було реалізовано механізм створення, монтування та демонтування зашифрованого контейнера. Контейнер представлений у вигляді одного файлу з розширенням .vault. При відкритті він монтується як окремий диск у системі, після завершення — демонтується, і всі ключі очищуються з оперативної пам’яті.

Етап 5. Реалізація журналювання.

Модуль журналу веде запис усіх дій користувача: вхід, вихід, помилки автентифікації, підключення носія, зміни налаштувань. Записи захищені від змін-зберігаються у зашифрованому файлі журналу з обмеженням прав доступу.

Таблиця 3.1 – Приклад журналу подій системи

№	Дата та час	Тип події	Користувач	Результат	Коментар
1	2025-04-10 08:45:12	Вхід у систему	Admin	Успішно	Виконано монтування контейнера
2	2025-04-10 08:46:55	Копіювання файлу	Admin	Успішно	Файл report.docx зашифровано
3	2025-04-10 08:47:33	Спроба зміни налаштувань	Admin	Відхилено	Доступ до конфігурації обмежений
4	2025-04-10 08:49:11	Введено неправильний пароль	Unknown	Помилка	1 спроба з 5
5	2025-04-10 08:50:01	Вихід із системи	Admin	Успішно	Контейнер демонтовано
6	2025-04-10 09:10:20	Підключення нового USB	Unknown Device	Заблоковано	Невідомий пристрій

Етап 6. Тестування модулів.

На завершальному етапі проведено модульне тестування кожного елементу системи. Оцінювалась стабільність роботи, швидкість шифрування, поведінка при неправильному введенні пароля, збої при несподіваному відключенні пристрою.

Звичайна сесія використання виглядає наступним чином:

1. Користувач підключає захищений накопичувач до комп'ютера.

2. Система автоматично перевіряє ідентифікатор пристрою.

3. Відкривається вікно авторизації.

4. Після проходження автентифікації монтується контейнер.

5. Користувач працює з файлами, як у звичайному провіднику.

6. По завершенні роботи диск демонтується, журнал оновлюється, а ключ знищується.

На рисунку зображено алгоритм роботи системи захисту даних, що включає етапи виявлення, шифрування/дешифрування даних (рис.3.3).

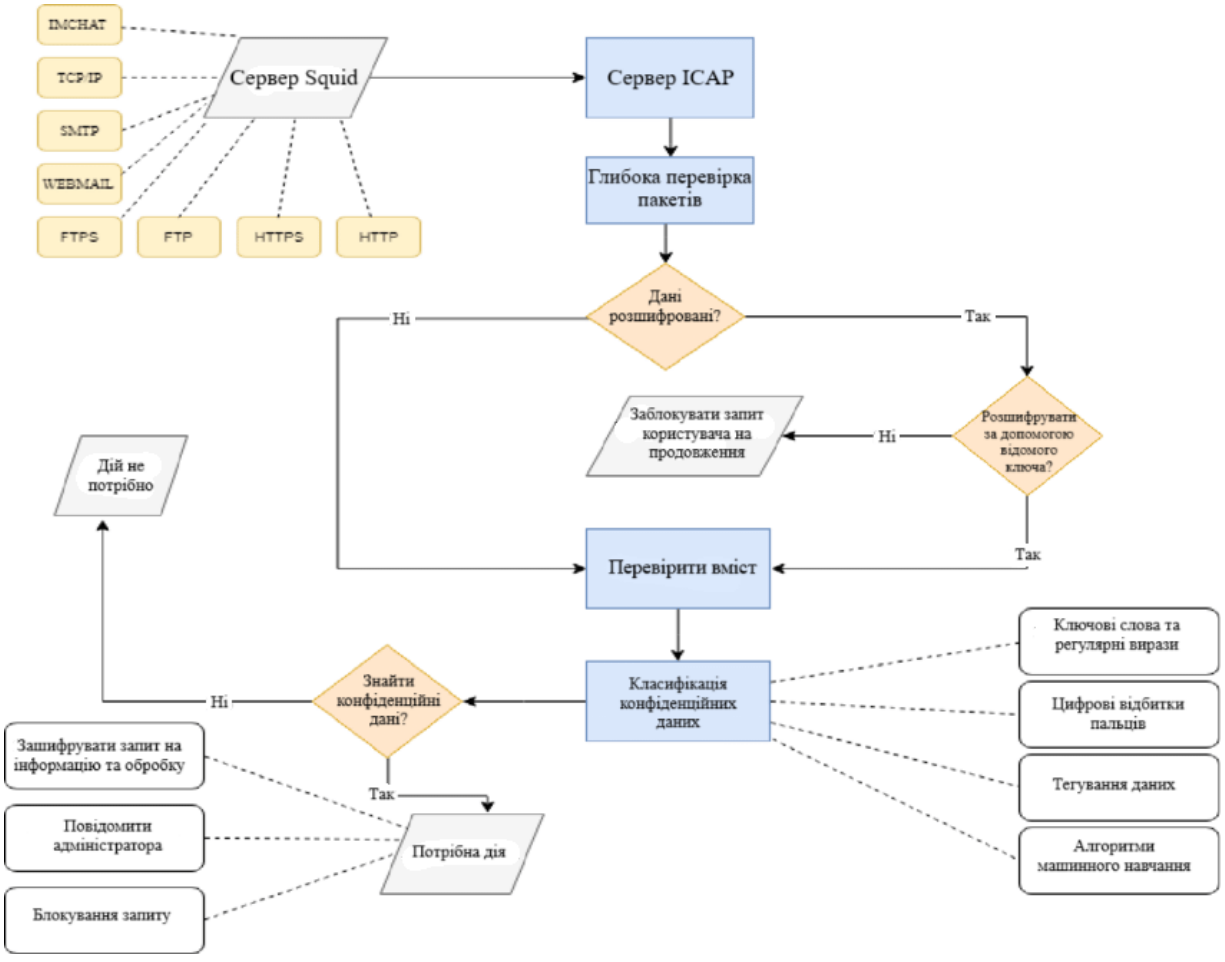


Рисунок 3.3 – Алгоритм роботи системи захисту даних

Ця блок-схема відображає послідовність дій у системі захисту даних, включаючи автентифікацію користувача, шифрування/дешифрування даних та ведення журналу подій.

3.2 Встановлення та налаштування програмного забезпечення

Safetica встановлюється за допомогою універсального інсталятора, який включає всі необхідні компоненти. Після його запуску можна вибрати один із двох способів інсталяції:

1. Автоматичну інсталяцію – автоматичне встановлення всіх компонентів на комп'ютер.

2. Інсталяція вручну (Експертна установка та витяг компонентів) – інсталяція окремих компонентів Safetica вручну.

Інсталяція вручну:

1. Перед інсталяцією потрібно перевірити, чи відповідає мережа умовам розгортання.

2. Встановити сервер на вибраних комп'ютерах. Під час інсталяції обрати, яка база даних буде використовуватися сервером для зберігання даних.

3. Встановити консоль управління або WebSafetica на ПК, з якого буде налаштоване управління Safetica.

4. Використовуючи консоль, підключити до сервера і виконати початкове налаштування Safetica.

5. Інсталювати агент на робочі станції.

6. Використавши консоль, щоб встановити клієнт на робочих станціях (встановлення клієнта через консоль можлива тільки на комп'ютерах з інстальованим агентом).

Після розгортання всіх компонентів та перевірки правильності встановлення, можна почати роботу з Safetica.

Автоматична інсталяція. Розглянемо лише автоматичну інсталяцію яка встановлює серверний компонент, адміністративні консолі, включаючи

WebSafetica, IIS вебсервер і сервер баз даних Microsoft SQL Server Express на цьому ПК. Клієнти встановлюються під час першого запуску Safetica після інсталяції. Необхідно переконатися, що комп'ютер має достатню обчислювальну потужність для роботи з базою даних, сервером, а також WebSafetica (Детальні умови стосовно вимог див. Install Manual на офіційному сайті Safetica One).

Після запуску універсального інсталятора Safetica необхідно виконати наступні дії:

1. Обрати мову інсталятора (рис.3.4).

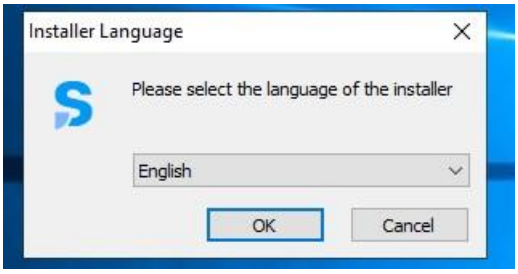


Рисунок 3.4– Вікно вибору мови інсталятора

2. Натиснути кнопку «Автоматична інсталяція» (рис.3.5).

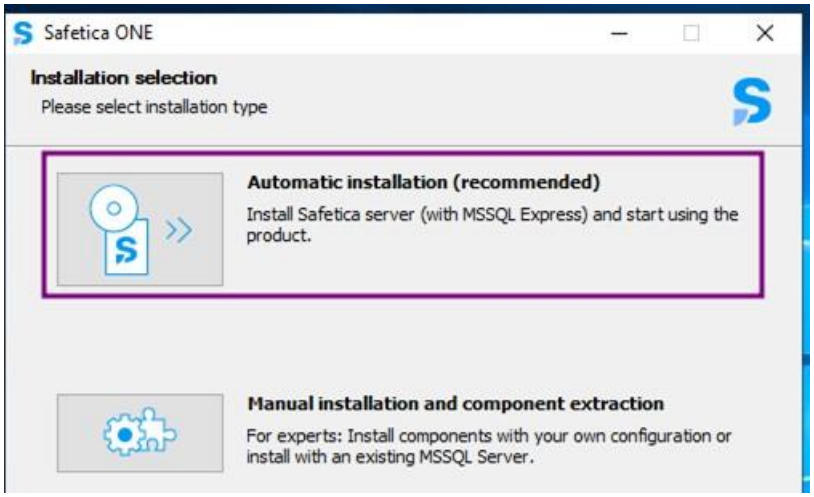


Рисунок 3.5– Вікно вибору Автоматичної інсталяції

3. Натиснути «Далі», щоб підтвердити, що обране середовище відповідає вимогам до апаратного забезпечення (рис.3.6).

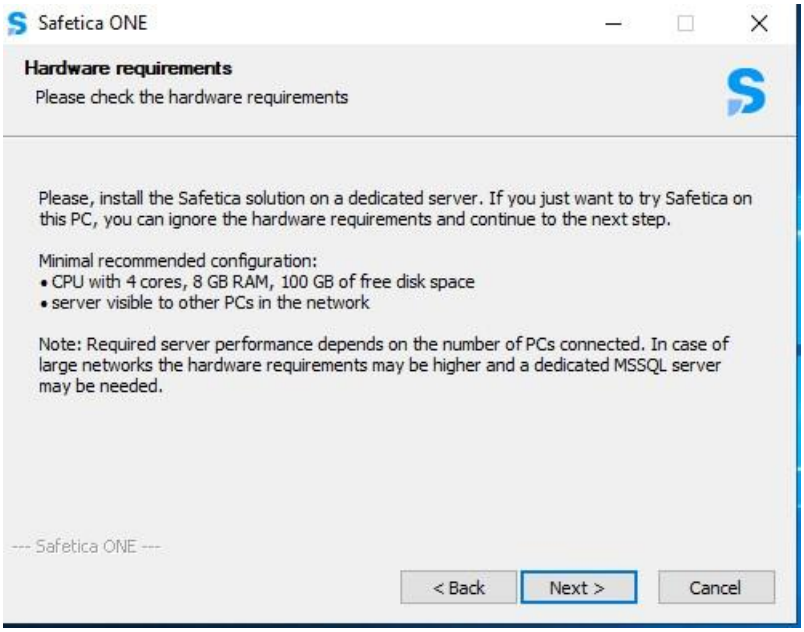


Рисунок 3.6– Вимоги апаратного забезпечення

4. Ввести пароль для облікового запису адміністратора. За замовчуванням пароль safetica. Підтвердіть умови ліцензійної угоди на сервері SQL і запустити інсталяцію, натиснувши кнопку «Інсталювати» (Install) (рис.3.7 – 3.11).

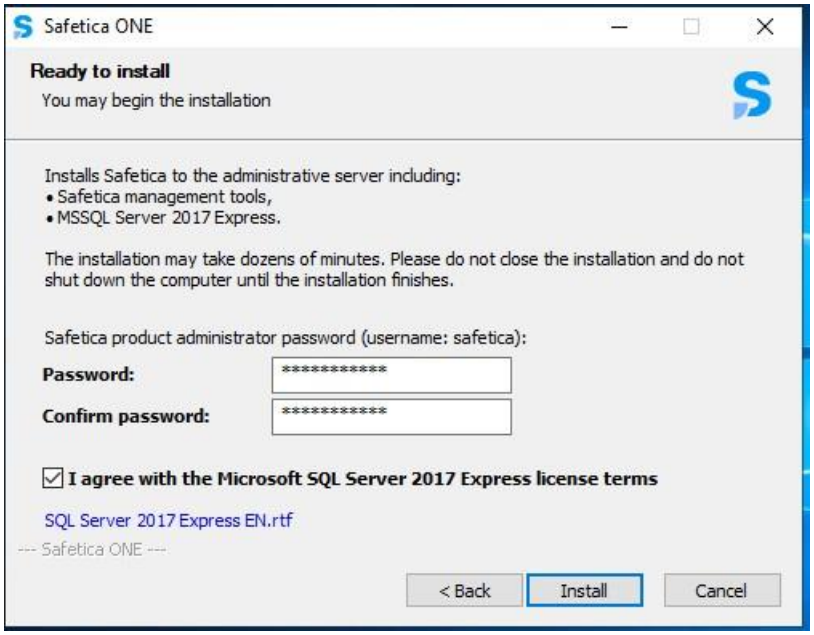


Рисунок 3.7– Вікно створення паролю адміністратора

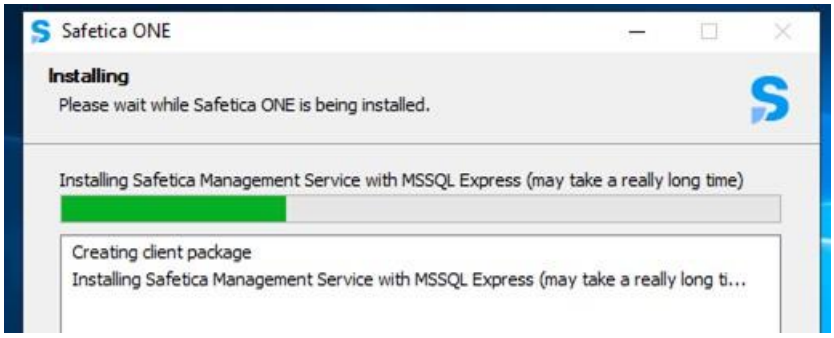


Рисунок 3.8– Вікно встановлення Safetica Management Service

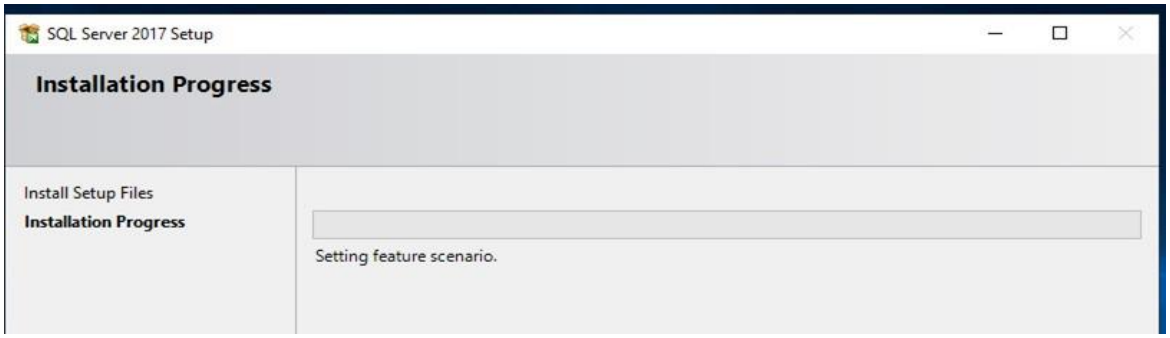


Рисунок 3.9 – Вікно встановлення SQL Server

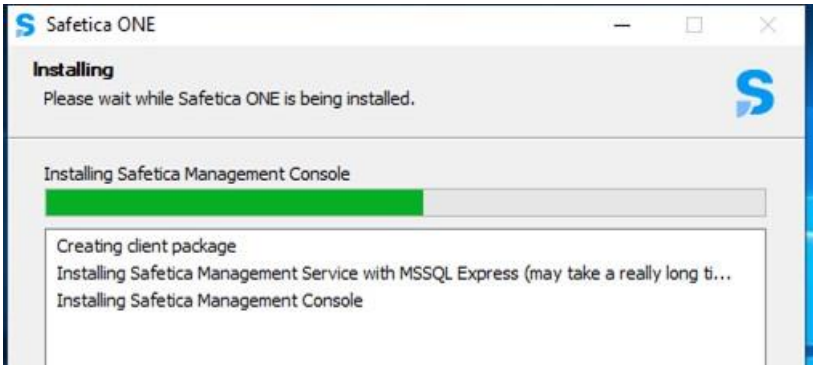


Рисунок 3.10 – Вікно встановлення Safetica Management Console

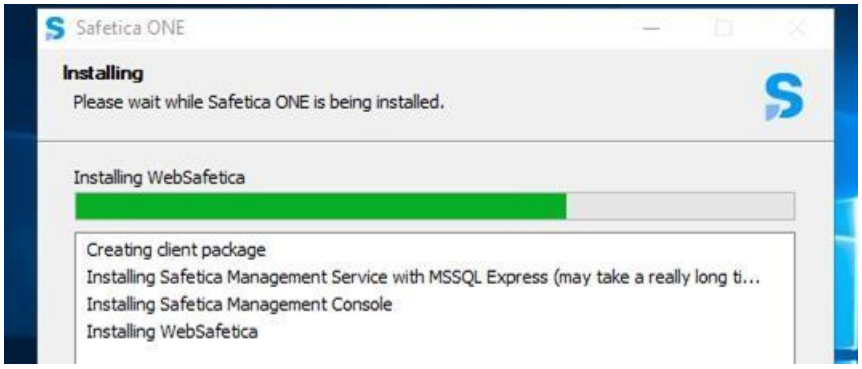


Рисунок 3.11 – Вікно встановлення WebSafetica

5. Щоб підтвердити успішну інсталяцію серверної частини натиснути «ОК» (рис.3.12).

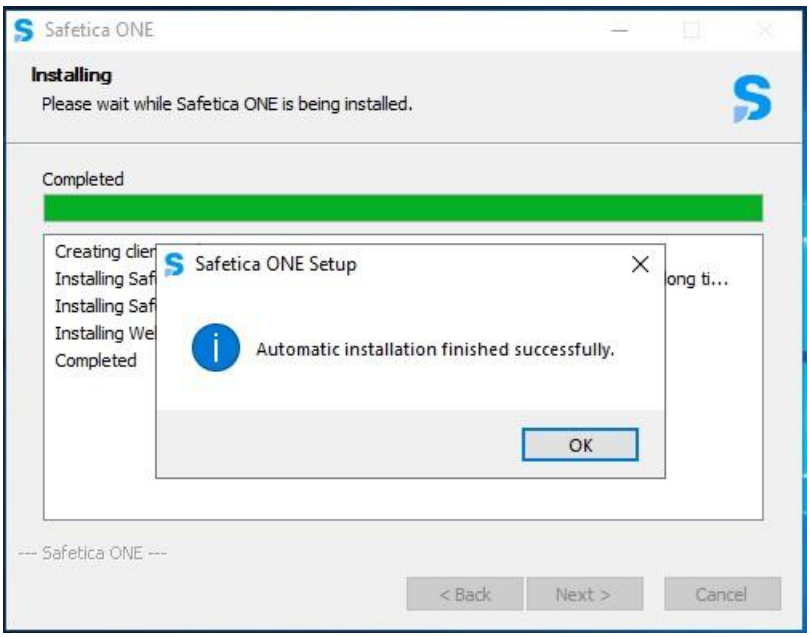


Рисунок 3.12 – Вікно підтвердження інсталяції

6. Після успішної інсталяції консолі управління Safetica та сервера, вся система повинна бути налаштована належним чином, перед тим як розпочати встановлення агента та клієнта Safetica на комп'ютерах. Управління та налаштування здійснюється за допомогою консолі управління Safetica (рис.3.13).

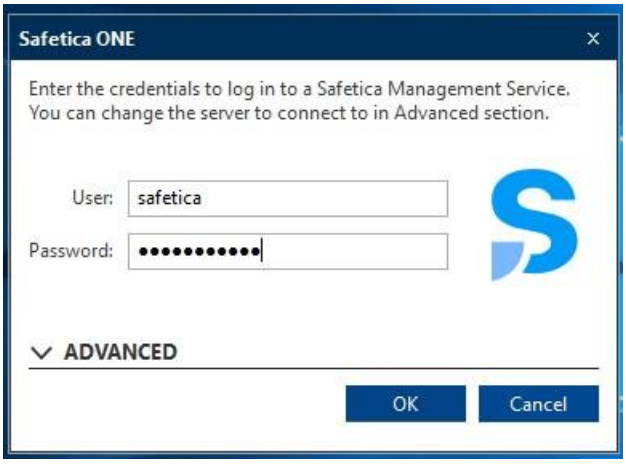


Рисунок 3.13 – Вікно входу в консоль управління

7. Після запуску консолі управління Safetica відкриється майстер початкового налаштування. Під час другого етапу можна додати сервер SMTP-сервер, на який Safetica буде надсилати сповіщення та звіти. Можна пропустити дане налаштування і вказати дані пізніше (рис.3.14).

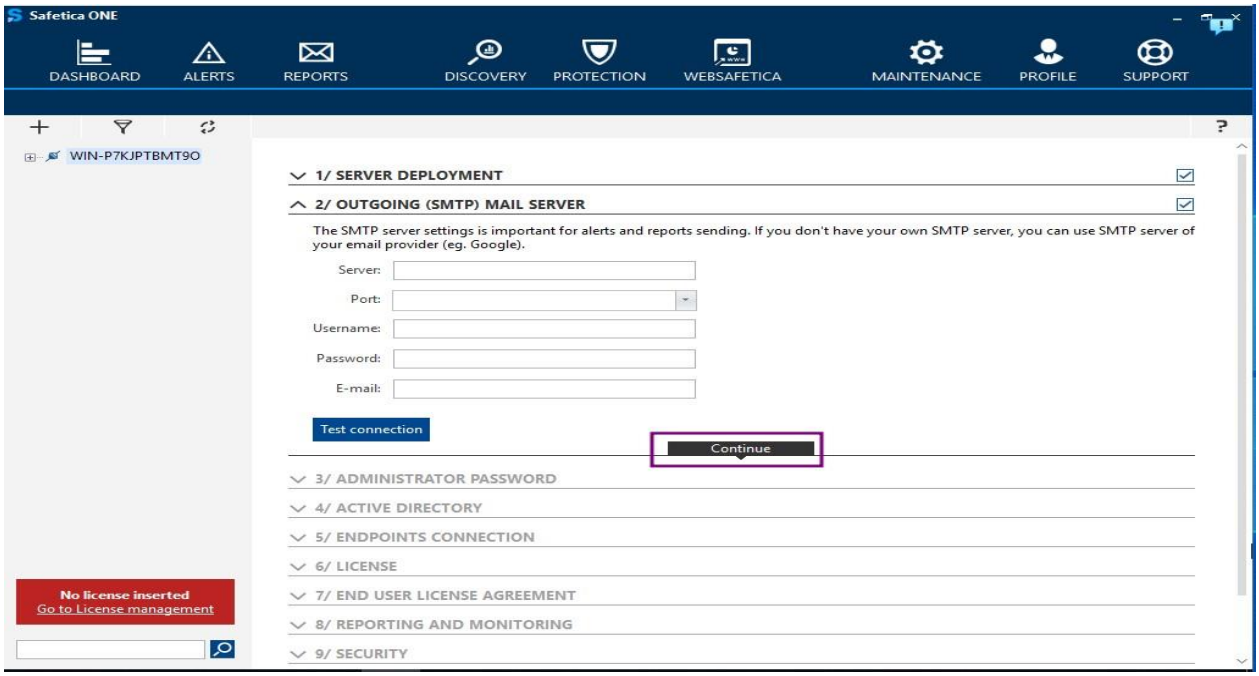


Рисунок 3.14 – Вікно налаштування підключення до поштового серверу

8. Під час наступного етапу можна імпортувати структуру Active Directory в компанії. Це можливо, якщо комп'ютер з сервером Safetica в домені (рис.3.15).

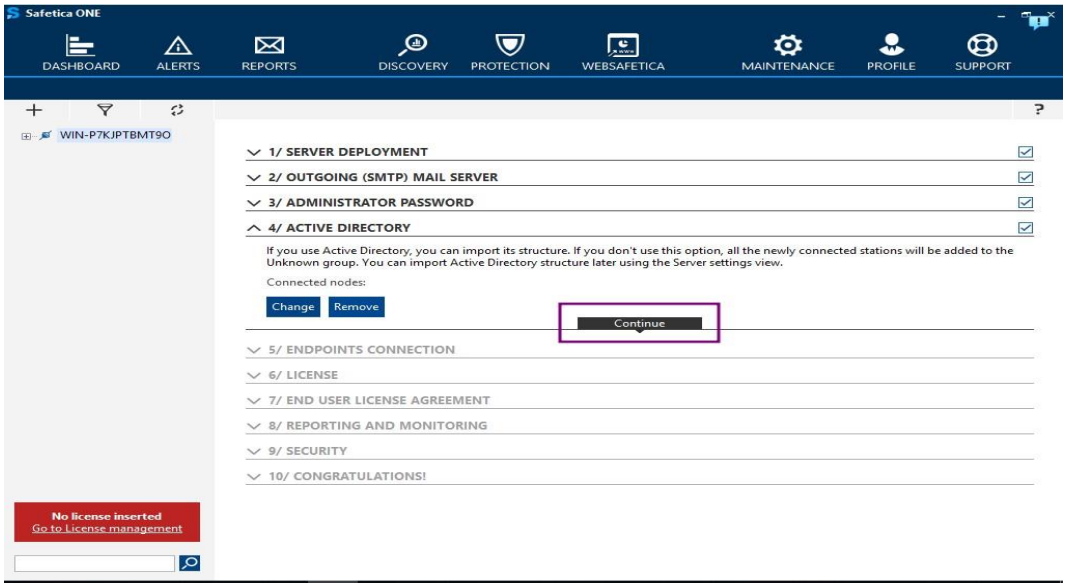


Рисунок 3.15 – Вікно налаштування підключення до Active Directory

9. Наступний крок — це завантаження агенту Safetica, щоб підключити робочі станції. Після натискання на кнопку «Get Downloader Agent» генерується файл інсталяції з агентом, який можна встановити на робочих станціях (рис.3.16).

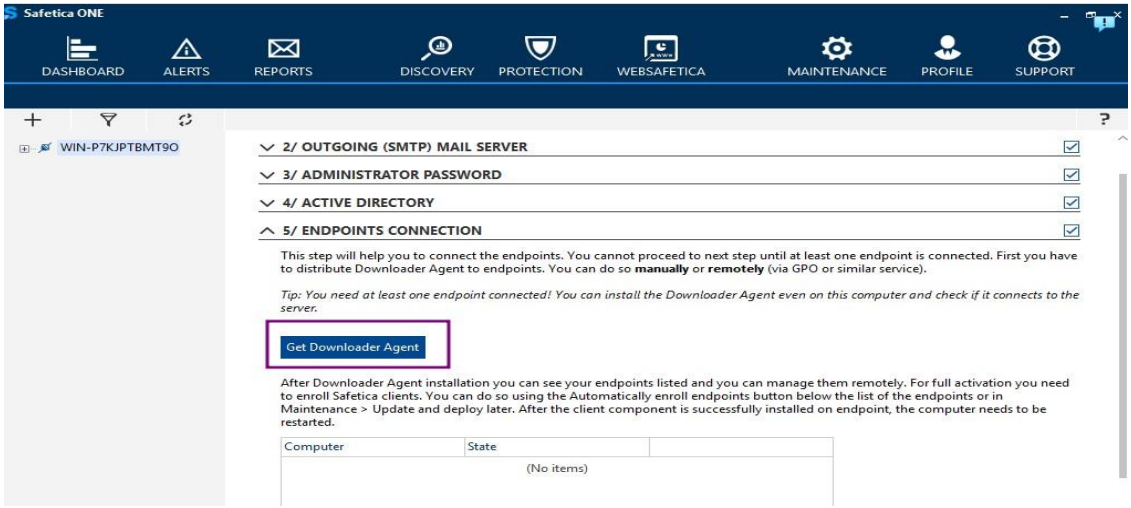


Рисунок 3.16 – Вікно для завантаження агента

10. Обираємо, куди завантажити інсталятор агента та натискаємо «Save» (рис.3.17 та рис.3.18).

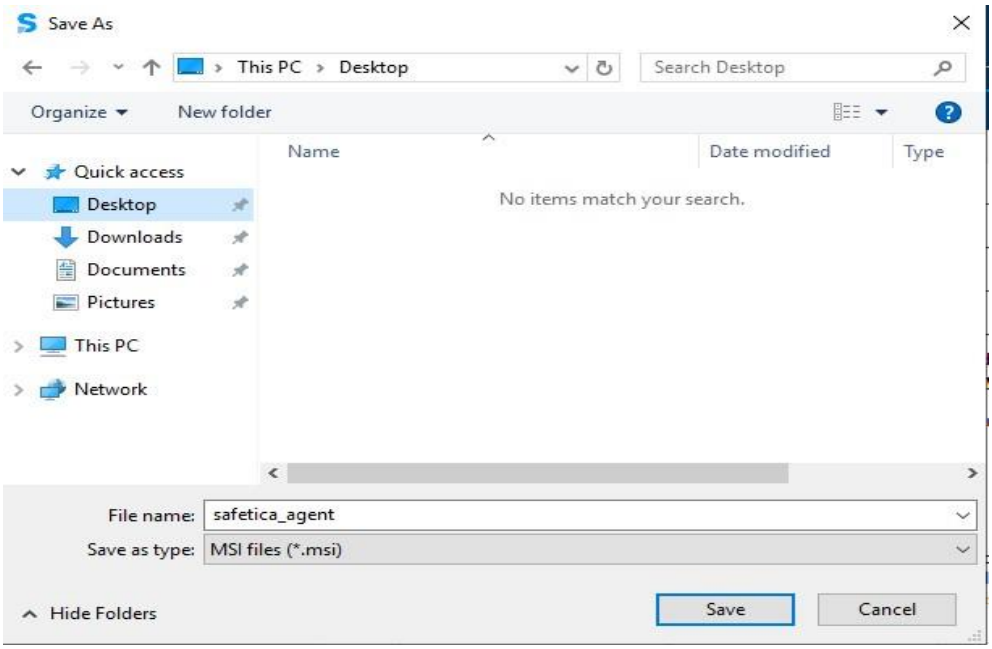


Рисунок 3.17 – Вікно вибору шляху завантаження

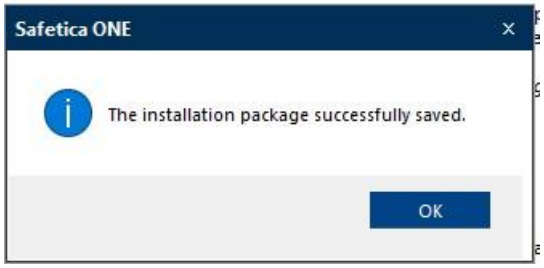


Рисунок 3.18 – Вікно успішного завантаження інсталятора агентам

11. Далі потрібно ввести ліцензійний ключ (рис.3.19).

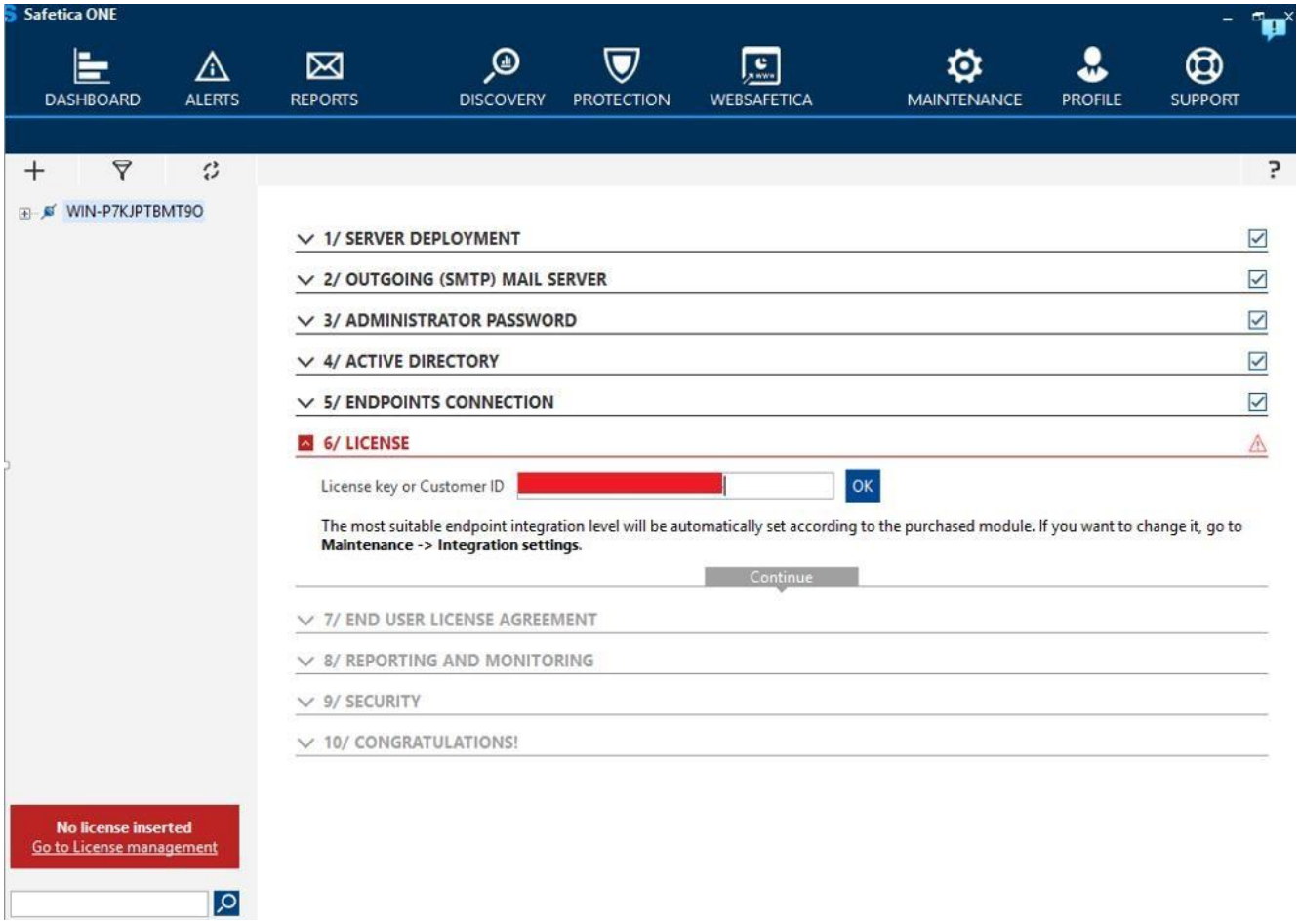


Рисунок 3.19 – Вікно вводу ліцензійного ключа

12. Вводимо дані адміністратора системи та погоджуємося з Safetica EULA (рис.3.20).

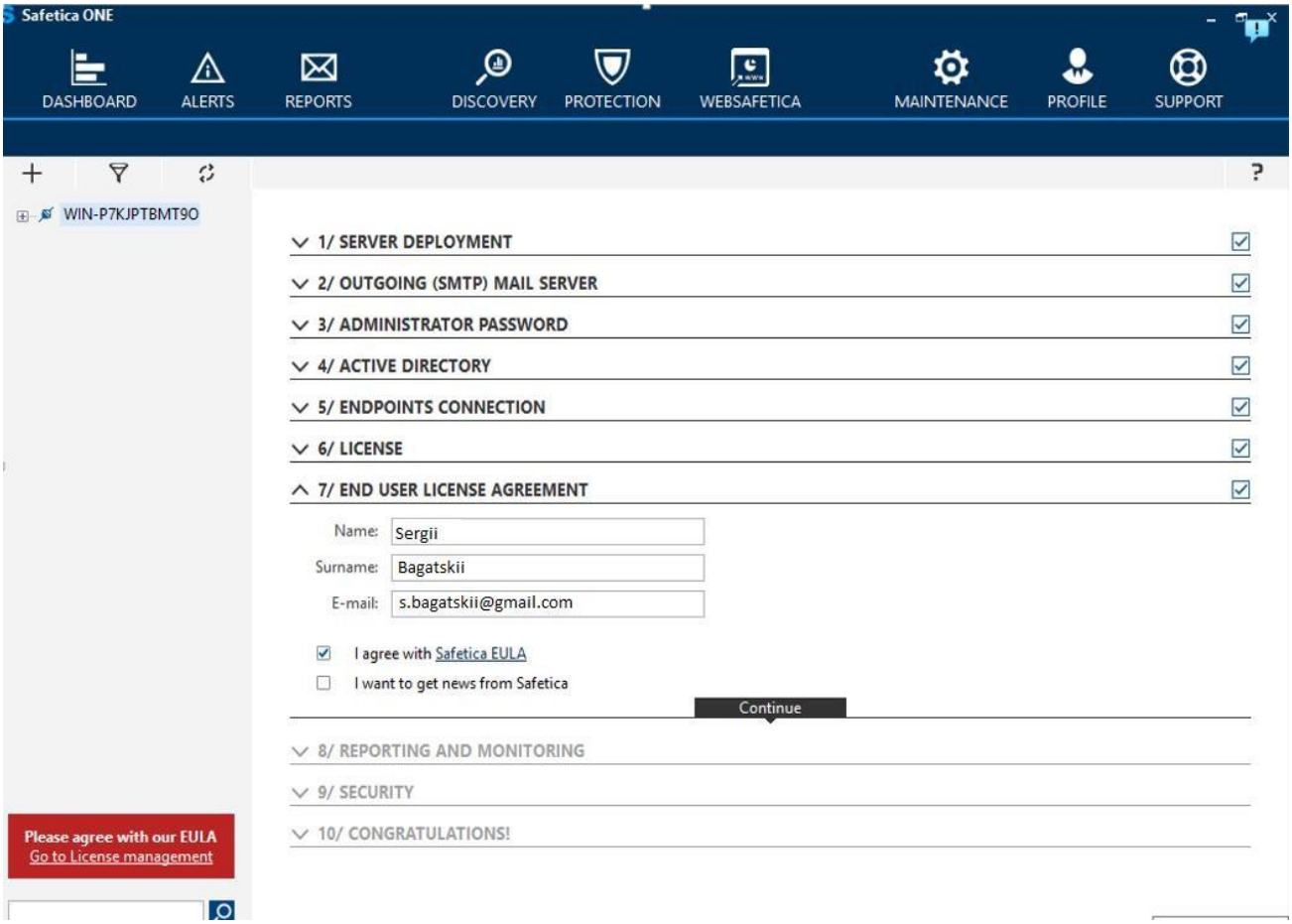


Рисунок 3.20 – Вікно вводу даних адміністратора

13. На даному етапі можна обрати доменну зону для електронної пошти компанії, встановити правила вмісту для опису конфіденційних даних. Після введення необхідної інформації натискаємо «Continue» (рис.3.21).

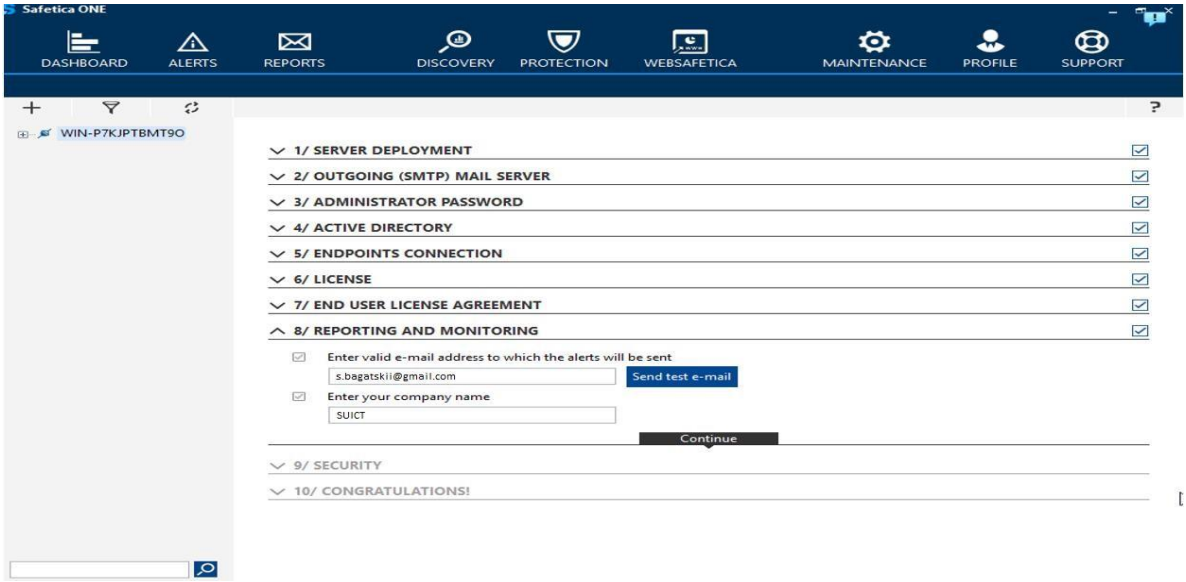


Рисунок 3.21 – Вікно для вводу назви компанії

14. Всі налаштування введені коректно, можна починати захист (рис. 3.22).

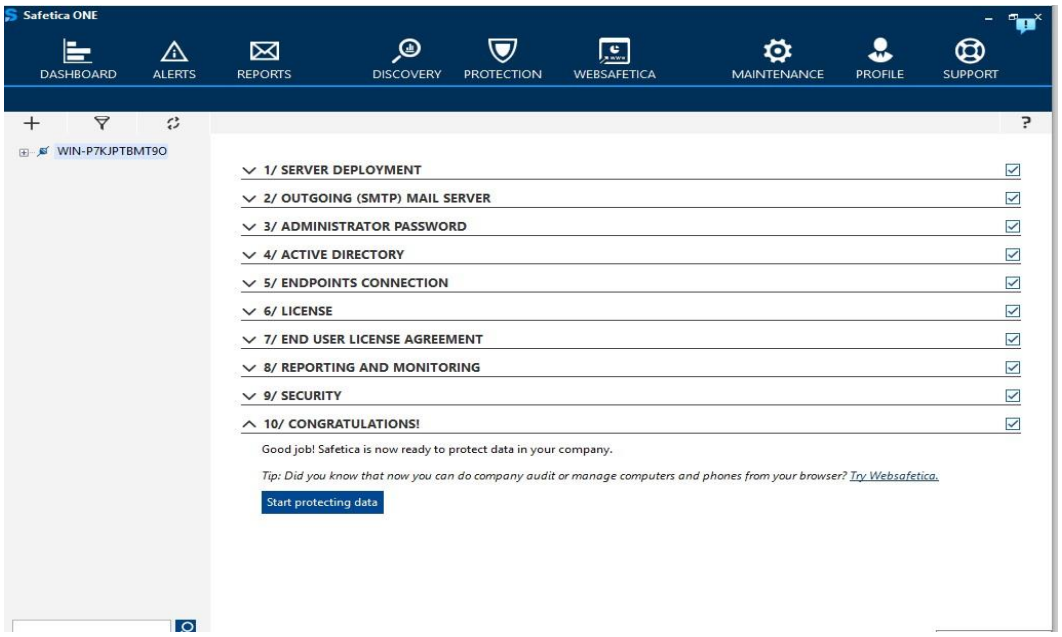


Рисунок 3.22 – Вікно підтвердження успішного налаштування системи

3.3 Розгортання системи

Зовнішні носії даних, такі як USB-накопичувачі, зовнішні жорсткі диски та інші портативні пристрої, часто використовуються для перенесення та зберігання інформації. Однак їх використання може становити серйозну загрозу для безпеки корпоративних даних у разі несанкціонованого доступу або втрати пристрою. Для запобігання таким ризикам необхідно впровадити ефективну систему контролю та захисту даних на зовнішніх носіях.

Налаштування політик контролю зовнішніх пристроїв у Safetica ONE

Safetica ONE надає можливість створення та впровадження політик контролю використання зовнішніх пристроїв. Це дозволяє обмежити або повністю заборонити копіювання конфіденційної інформації на незареєстровані носії.

Крок 1: Відкриття консолі керування Safetica ONE

Після входу в консоль керування перейдіть до розділу Protection.

Крок 2: Створення нової політики контролю пристроїв

У розділі Protection оберіть підрозділ DLP policies та натисніть кнопку New Policy для створення нової політики. (рис. 3.23)

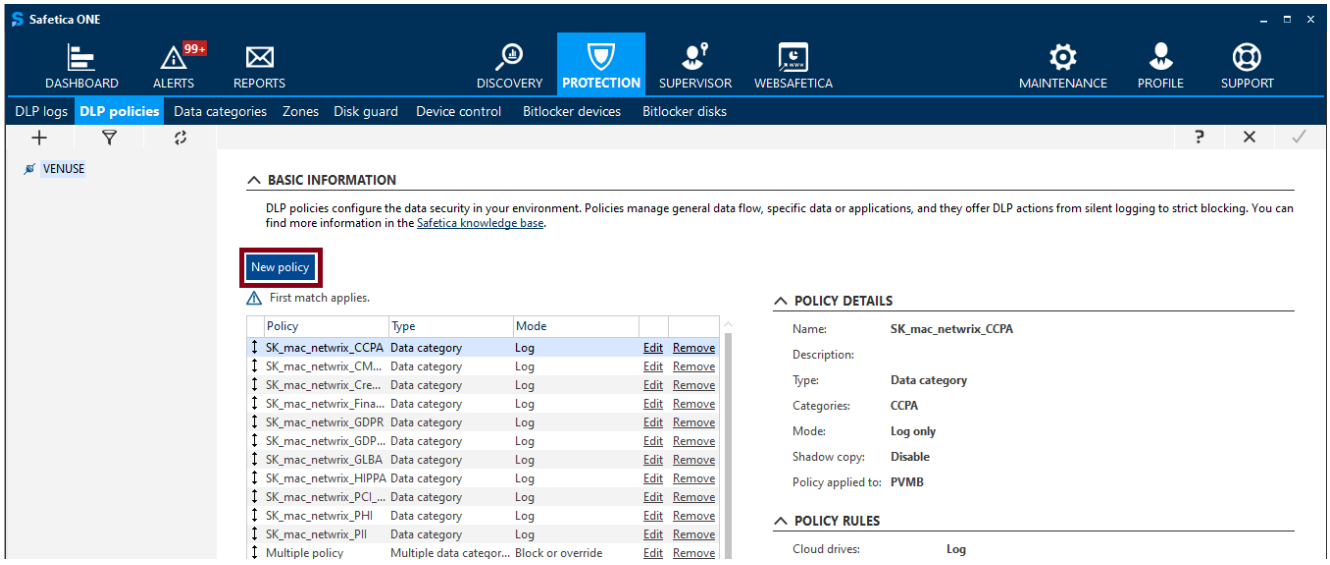


Рисунок 3.23 – Створення нової політики контролю пристроїв

Крок 3: Налаштування параметрів політики

У вікні налаштувань політики задайте такі параметри:

1. Назва політики: наприклад, "Контроль USB-пристроїв".

2. Тип пристрою: обрати "Removable Storage".

3. Після цього встановити вибірку "Block" для заборони використання незареєстрованих пристроїв або "Read-only" для дозволу лише читання.

Крок 4: Застосування політики до користувачів або груп

На цьому етапі обрати користувачів або групи, до яких буде застосована дана політика. Це дозволяє керувати доступом до зовнішніх пристроїв в залежності від ролі співробітника в організації.

Крок 5: Збереження та активація політики

Після завершення налаштувань натиснути кнопку Finish для збереження політики. Політика буде автоматично активована та застосована до обраних користувачів або груп.

Моніторинг та аудит використання зовнішніх пристроїв

Safetica ONE також надає можливість моніторингу та аудиту використання зовнішніх пристроїв. У розділі Dashboards можна переглядати звіти про

підключення пристроїв, спроби копіювання даних та інші дії користувачів. Це дозволяє швидко реагувати на потенційні загрози та порушення політик безпеки.

Цими діями продемонстровано як за допомогою Safetica ONE можна контролювати використання зовнішніх пристроїв та запобігати несанкціонованому витоку конфіденційної інформації. Впровадження таких політик є важливим кроком у забезпеченні комплексної безпеки даних в організації.

Створення та налаштування політик контролю зовнішніх пристроїв за допомогою Safetica ONE є важливим елементом захисту інформації в будь-якій організації. Крім безпосереднього контролю доступу до носіїв даних, система забезпечує всебічний моніторинг, що дозволяє виявляти аномальні дії та вчасно реагувати на потенційні загрози.

Застосування політик типу «Block» або «Read-only» дозволяє керувати рівнями доступу, адаптуючи їх під конкретні потреби бізнесу. Наприклад, для співробітників, що працюють з важливою інформацією, можна встановити повну заборону на копіювання даних, а для інших користувачів буде дозволено лише читання. Такий підхід мінімізує ризики витоку даних без істотного обмеження продуктивності праці.

Додатково Safetica ONE забезпечує централізоване управління та звітність, що полегшує роботу IT-відділу і сприяє дотриманню вимог нормативних актів щодо захисту інформації. Звіти про підключення та використання зовнішніх пристроїв допомагають відстежувати інциденти безпеки і вчасно приймати заходи.

Таким чином, впровадження системи Safetica ONE та налаштування політик контролю зовнішніх пристроїв значно підвищують рівень інформаційної безпеки в організації. Реалізація таких заходів потребує комплексного підходу, включаючи навчання персоналу, регулярний аудит та оновлення політик відповідно до змін у загрозах для підприємств.

Отже, розглянутий підхід до безпечного зберігання та контролю конфіденційної інформації на зовнішніх носіях є ефективним і рекомендованим

для впровадження у сучасних компаніях, які прагнуть захистити свої дані від несанкціонованого доступу та втрат.

3.4 Висновки

У третьому розділі було реалізовано систему безпечного зберігання конфіденційної інформації на зовнішніх пристроях, яка базується на програмно-апаратному підході. Основною складовою такої системи є застосування сучасних технологій захисту, зокрема криптографічних алгоритмів AES-256 у режимі CBC, модулів автентифікації користувачів, контролю доступу, журналювання подій та апаратного детектора пристроїв.

Було показано встановлення програми та впровадження DLP-систем, приклад Safetica ONE, демонструє ефективність комплексного контролю операцій із зовнішніми носіями, запобігання витоку інформації та оперативного реагування на потенційні загрози. Розроблена структурна схема забезпечує багаторівневий захист, що охоплює як технічні, так і організаційні аспекти безпеки даних.

Через поєднання шифрування, автентифікацію та контроль доступу забезпечується захист інформації навіть у випадку втрати або крадіжки носія. Система є зручною для користувачів завдяки інтуїтивному інтерфейсу та мінімальній необхідності взаємодії з технічними деталями захисту.

Таким чином, розроблена система відповідає сучасним вимогам безпеки конфіденційної інформації на зовнішніх пристроях і може ефективно застосовуватися в організаціях для мінімізації ризиків витоку даних.

ВИСНОВКИ

Впродовж виконання дипломної роботи було проведено комплексне дослідження засобів та методів захисту конфіденційної інформації на зовнішніх пристроях від несанкціонованого доступу. Було проаналізовано загрози, які виникають при використанні зовнішніх носіїв інформації, а також існуючі технології та алгоритми шифрування, які дозволяють мінімізувати ризики витоку даних.

Основна увага у роботі приділялась системам класу DLP (Data Loss Prevention), яка є ефективним інструментом контролю та захисту інформації. Детально було розглянуто програмне забезпечення Safetica ONE як приклад сучасного комплексного рішення для контролю доступу, моніторингу та запобігання несанкціонованому копіюванню конфіденційних даних на зовнішніх носіях. У роботі описано розгортання, налаштування політик безпеки, що показує практичну ефективність використання даної системи.

Побудова системи безпечного зберігання інформації на зовнішніх пристроях базується на поєднанні апаратних і програмних засобів захисту, що дозволяє забезпечити високий рівень конфіденційності та цілісності даних. Запропонована структурна та функціональна схема системи, а також покрокове розгортання засобів захисту у середовищі Safetica ONE, може бути використана як база для впровадження подібних систем у реальних організаціях.

Отже, результати дослідження підтверджують актуальність та необхідність застосування комплексних систем захисту інформації для запобігання витоку конфіденційних даних через зовнішні носії.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Костюк Ю. В., Складанний П. М., Гулак Г. М., Бебешко Б. Т., Хорольська К. В., Рзаєва С. Л. Системи захисту інформації. Київ: Київський столичний університет імені Бориса Грінченка, 2025. https://elibrary.kubg.edu.ua/51359/1/Kostiuk_Y_Skladannyi_P_Hulak_H_Bebeshko_B_Khorolska_K_Rzaieva_S_SZI_2025_FITM.pdf

2. Hypertec SP. «Безпека зберігання даних: Наскільки захищені ваші дані?». URL: https://hypertecsp.com/knowledge-base/data-storage-security/

3. Hypertec SP. "Data Storage Security - How Secure Is Your Data?" URL: https://hypertecsp.com/knowledge-base/data-storage-security/

4. Beyond20. "Cyber Security and External Storage Devices Risks" URL: https://www.beyond20.com/blog/external-storage-device-security/

5. ProfileTree. "Protecting User Data: Encryption & Secure Storage Techniques" URL: https://profiletree.com/protecting-user-data-and-secure-storage-techniques/

6. Складанний П. М., Гулак Г. М., Бебешко Б. Т., Хорольська К. В., Рзаєва С. Л. «Системи захисту інформації». Київ: Київський столичний університет імені Бориса Грінченка, 2025. URL: https://elibrary.kubg.edu.ua/51359/1/Kostiuk_Y_Skladannyi_P_Hulak_H_Bebeshko_B_Khorolska_K_Rzaieva_S_SZI_2025_FITM.pdf (дата звернення: 06.05.2025).

7. Гапак О. М., Балога С. І. «Захист інформації в комп’ютерних системах». Ужгород: Ужгородський національний університет, 2021. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/36506/1/ПІДРУЧНИК%20ІКС_2021.pdf (дата звернення: 06.05.2025).

8. CyberSecurity Handbook. «Безпечне зберігання даних». URL: https://cso.cyberhandbook.org/uk/topics/storing-data/bezpechne-zberihannya-danykh (дата звернення: 06.05.2025).

9. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу». Київ, 1999. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf (дата звернення: 06.05.2025).

10. Кононович В. Г. «Інформаційна безпека цифрових програмно-керованих автоматичних телефонних станцій». Одеса: ОНАЗ ім. О. С. Попова, 2013. URL: https://library.kre.dp.ua/Books/2-4%20kurs/Захист%20інформації/Рекомендовано%20МОНУ/Кононович_В.Г._Інформаційна_безпека_цифрових_АТС_ОНАЗ_Одеса_2013.pdf (дата звернення: 06.05.2025).

11. Лужицький В. М. «Основи організаційного захисту інформації». Вінниця: Вінницький національний технічний університет, 2005. URL: https://pdf.lib.vntu.edu.ua/books/2024/Luzhetskii_2005_148.pdf (дата звернення: 06.05.2025).

12. Конахович Г. Ф., Климчук В. П., Паук С. М., Потапов В. Г., Горбунов О. О. «Захист інформації в телекомунікаційних системах». Київ: НАУ, 2016. URL: https://tks.nau.edu.ua/wp-content/uploads/2016/05/Zahyst-informatsiyi-v-telekomunikatsijnyh-systemah.pdf (дата звернення: 06.05.2025).

13. Кононович В. Г. «Інформаційна безпека цифрових програмно-керованих автоматичних телефонних станцій». Одеса: ОНАЗ ім. О. С. Попова, 2013. URL: https://library.kre.dp.ua/Books/24%20kurs/Захист%20інформації/Рекомендовано%20МОНУ/Кононович_В.Г._Інформаційна_безпека_цифрових_АТС_ОНАЗ_Одеса_2013.pdf (дата звернення: 06.05.2025).

14. Кваліфікаційна робота (проект). Запорізький національний університет. URL: https://dspace.znu.edu.ua/jspui/bitstream/12345/4716/1/Диплом_Кан.pdf (дата звернення: 06.05.2025).

15. Конспект лекцій з управління інформаційною безпекою. КПІ ім. Ігоря Сікорського. URL: https://ela.kpi.ua/bitstream/123456789/43377/1/Konspekt-Lektsii_UIB.docx (дата звернення: 06.05.2025).

16. Kingston Technology Company. «Типи цифрових носіїв». URL: https://www.kingston.com/en/blog/pc-performance/types-of-digital-storage.

17. ForensicFocus. «Ідентифікація USB пристроїв у Windows системах». URL: https://www.forensicfocus.com/articles/identifying-usb-devices-on-windows-systems/.

18. Wikipedia. «Цифровий носій». URL: https://uk.wikipedia.org/wiki/Цифровий_носій.

19. Крук С. А. «Технічні засоби захисту інформації на зовнішніх носіях». Дніпропетровськ: НУ «Остромадський університет», 2018. URL: https://dspace.nlu.edu.ua/bitstream/123456789/12330/1/Krucka_301_305.pdf.

20. Вісник правових наук. «Методи захисту інформації в комп'ютерних мережах». URL: https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc5/56.pdf.

21. Kingston Technology Company. «Типи інтерфейсів для зберігання даних». URL: https://www.kingston.com/en/blog/pc-performance/data-interface-types.

22. Seagate Technology LLC. «Порівняння переносних і настільних зовнішніх жорстких дисків». URL: https://www.seagate.com/blog/portable-vs-desktop-external-hard-drives/.

23. Kaspersky. «Як зашифрувати USB флешку». URL: https://www.kaspersky.com/resource-center/preemptive-safety/how-to-encrypt-usb-drive.

24. CSO Online. «USB флешки та зростання вірусу Agent.btz». URL: https://www.csoonline.com/article/284501/usb-drives-and-the-rise-of-the-agent-btz-virus.html.

25. TechRadar. «Як хакери використовують USB пристрої для атак». URL: https://www.techradar.com/news/how-hackers-use-usb-devices-to-launch-attacks.

26. US-CERT. «Алерт TA17-130A: USB пристрої». URL: https://www.us-cert.cisa.gov/ncas/alerts/TA17-130A.

27. GeeksforGeeks. «Які ризики для безпеки існують при використанні USB флеш-накопичувачів?». URL: https://www.geeksforgeeks.org/what-are-the-security-risks-of-usb-drives/.

28. Wikipedia. «Безпека USB флеш-накопичувачів». URL: https://en.wikipedia.org/wiki/USB_flash_drive_security.

29. ManageEngine. «Найкращі практики використання USB пристроїв». URL: https://www.manageengine.com/data-security/best-practices/usb-drive-best-practices.html.

30. Kingston Technology Company. «Організації, що використовують зашифровані USB». URL: https://www.kingston.com/unitedkingdom/en/blog/data-security/organizations-using-encrypted-usb.

31. UpGuard. «Як захистити чутливі дані на USB флешці». URL: https://www.upguard.com/blog/secure-sensitive-data-on-a-usb-flash-drive.

32. UVic. «Інформаційна безпека при використанні USB пристроїв». URL: https://www.uvic.ca/systems/support/informationsecurity/datasecurity/usb.php.

33. Wired. «Китайські USB пристрої і шкідливі програми». URL: https://www.wired.com/story/china-usb-sogu-malware.

34. Honeywell. «Кібербезпека в 2024 році: USB пристрої залишаються серйозною загрозою». URL: https://www.honeywell.com/us/en/news/2024/04/cybersecurity-in-2024-usb-devices-continue-to-pose-major-threat.

35. BleepingComputer. «Атаки з використанням USB пристроїв знову зростають у першій половині 2023 року». URL: https://www.bleepingcomputer.com/news/security/usb-drive-malware-attacks-spiking-again-in-first-half-of-2023.

36. NIST. «FIPS 197: Advanced Encryption Standard (AES)». URL: https://csrc.nist.gov/publications/detail/fips/197/final.

37. OWASP. «Шифрування зберігання даних: Правила та найкращі практики».URL:https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html.

38. Computer History Museum. «Хронологія розвитку технології зберігання даних». URL: https://www.computerhistory.org/storage/timeline/.

39. Kingston Technology Company. «Історія USB флеш-накопичувачів». URL: https://www.kingston.com/en/blog/pc-performance/history-of-usb-flash-drives.

40. IBM. «Безпечні USB флешки». URL: https://www.ibm.com/security/secure-usb-flash-drive.

41. Apricorn. «USB пристрої з апаратним шифруванням». URL: https://apricorn.com/products/hardware-encrypted-storage/secure-usb-drives.html.

42. Kingston Technology Company. «Захищені USB пристрої IronKey». URL: https://www.kingston.com/en/usb/encrypted-secure/ironkey.

43. Western Digital. «SanDisk Extreme Pro USB 3.2 SSD». URL: https://www.westerndigital.com/products/usb-flash-drives/sandisk-extreme-pro-usb-3-2-ssd.

44. Rohde & Schwarz. «Зашифровані USB пристрої». URL: https://cybersecurity.rohde-schwarz.com/solutions/encrypted-usb-devices.

45. Kaspersky. «Шифрування даних». URL: https://www.kaspersky.com/resource-center/definitions/data-encryption.

46. ScienceDirect. «Аналіз безпеки зберігання даних на зовнішніх пристроях». URL: https://www.sciencedirect.com/science/article/abs/pii/S016740482100148X.

47. IBM. «Управління ключами». URL: https://www.ibm.com/topics/key-management.

48. Kingston Technology Company. «Переваги апаратно зашифрованих USB пристроїв». URL: https://www.kingston.com/en/blog/encrypted-usb/benefits-of-hardware-encrypted-usb.

49. Verbatim. «Захищені USB пристрої». URL: https://www.verbatim-europe.com/en/prod/secure-usb-drives/.

50. Intel. «Технологія Thunderbolt: Розробка для безпеки». URL: https://www.intel.com/content/www/us/en/io/thunderbolt/thunderbolt-technology-developer.html.

51. Microsoft. «Політика безпеки смарт-карт у Windows». URL: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-smart-card-removal-behavior.

52. Cisco. «Що таке кібербезпека». URL: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.

53. ISO. «ISO/IEC 27040: Безпека інформації — Керівництво з безпеки даних». URL: https://www.iso.org/standard/54534.html.

54. NCSC. «Вступ до безпеки хмар». URL: https://www.ncsc.gov.uk/collection/cloud-security/introduction.

55. IBM. «Безпека апаратних модулів для шифрування». URL: https://www.ibm.com/topics/hardware-security-module.

56. Microsoft. «Огляд модулю TPM (Trusted Platform Module)». URL: https://learn.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview.

57. Red Hat. «Що таке контроль доступу на основі ролей (RBAC)». URL: https://www.redhat.com/en/topics/security/what-is-role-based-access-control-rbac.

58. Microsoft. «Многофакторна автентифікація для бізнесу». URL: https://www.microsoft.com/en-us/security/business/identity/multifactor-authentication.

59. Lucidchart. «Діаграма потоку даних». URL: https://www.lucidchart.com/pages/data-flow-diagram.

60. ISO. «ISO/IEC 27001: Стандарт для систем управління інформаційною безпекою». URL: https://www.iso.org/standard/27001.

61. Informa TechTarget. «Технічні рішення для забезпечення кібербезпеки». URL: https://www.infosecurity-magazine.com.

62. eInfochips. «Оцінка кіберзагроз у організаціях». URL: https://www.einfochips.com.

63. Dspace UzhNU. «Аналіз інформаційних систем захисту даних». URL: https://dspace.uzhnu.edu.ua.

64. Рис. 1.1– Види зовнішніх цифрових носіїв інформації https://naurok.com.ua/urok-nosi-informaci-251409.html

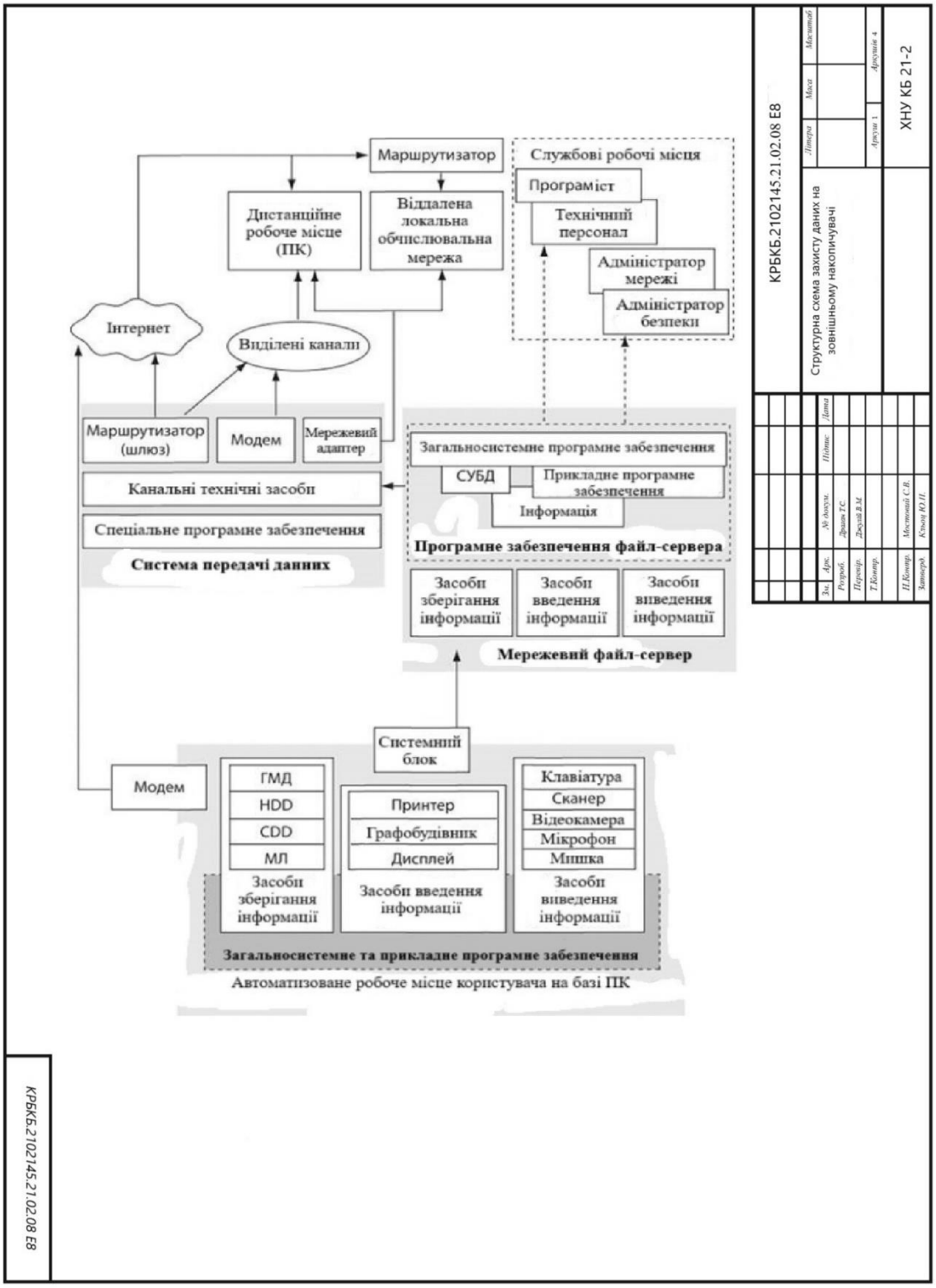
65. Рис. 1.2– Схема апаратного повного шифрування диску https://stud.com.ua/97437/informatika/kontseptsiya_zahischenih_virtualnih_privatnih_merezh

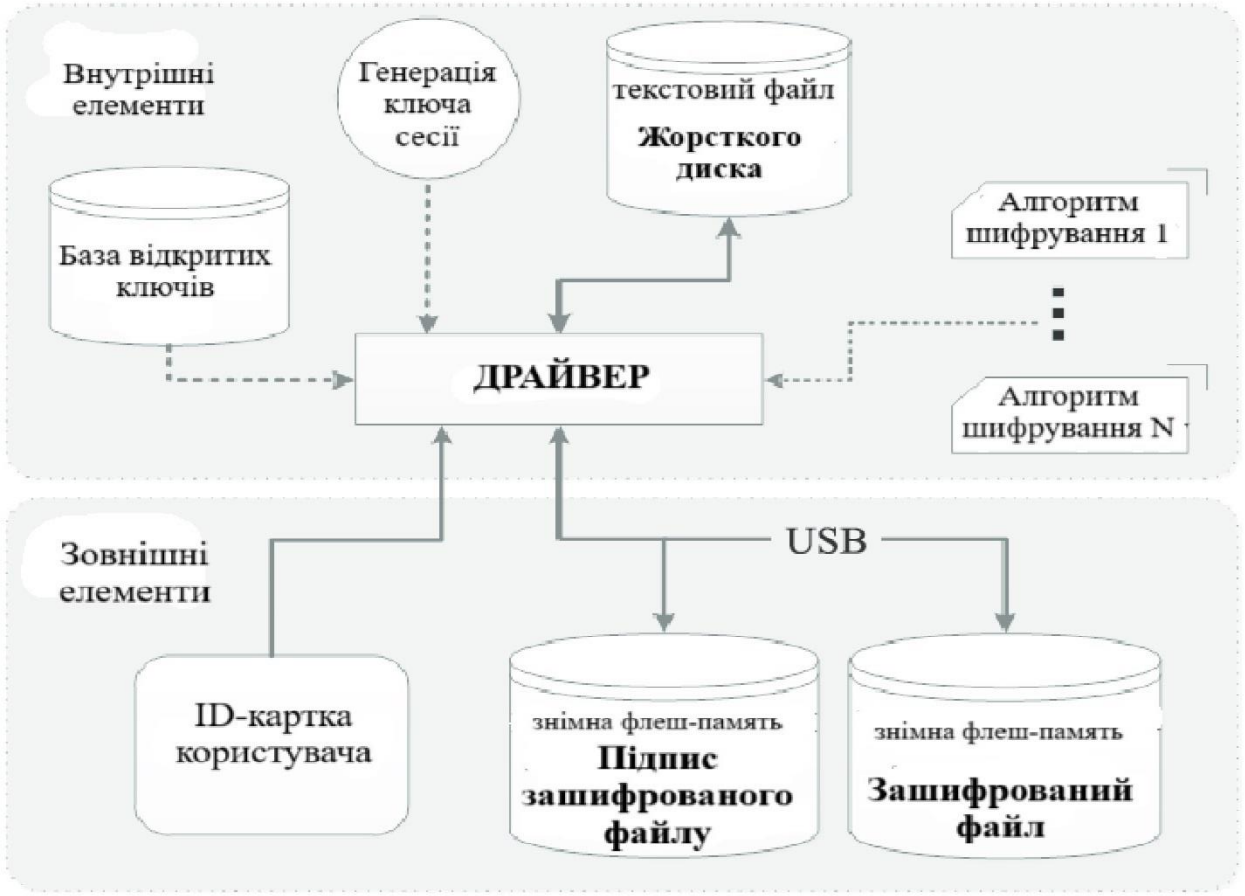
66. Рис. 2.1– Схема захисту даних на зовнішньому накопичувачі https://lektsii.org/16-74264.html?utm_source=

67. Рис. 3.1– Структурна схема взаємодії модулів системи https://stud.com.ua/164964/informatika/model_vzayemodiyi_program_sistem#google_vignette

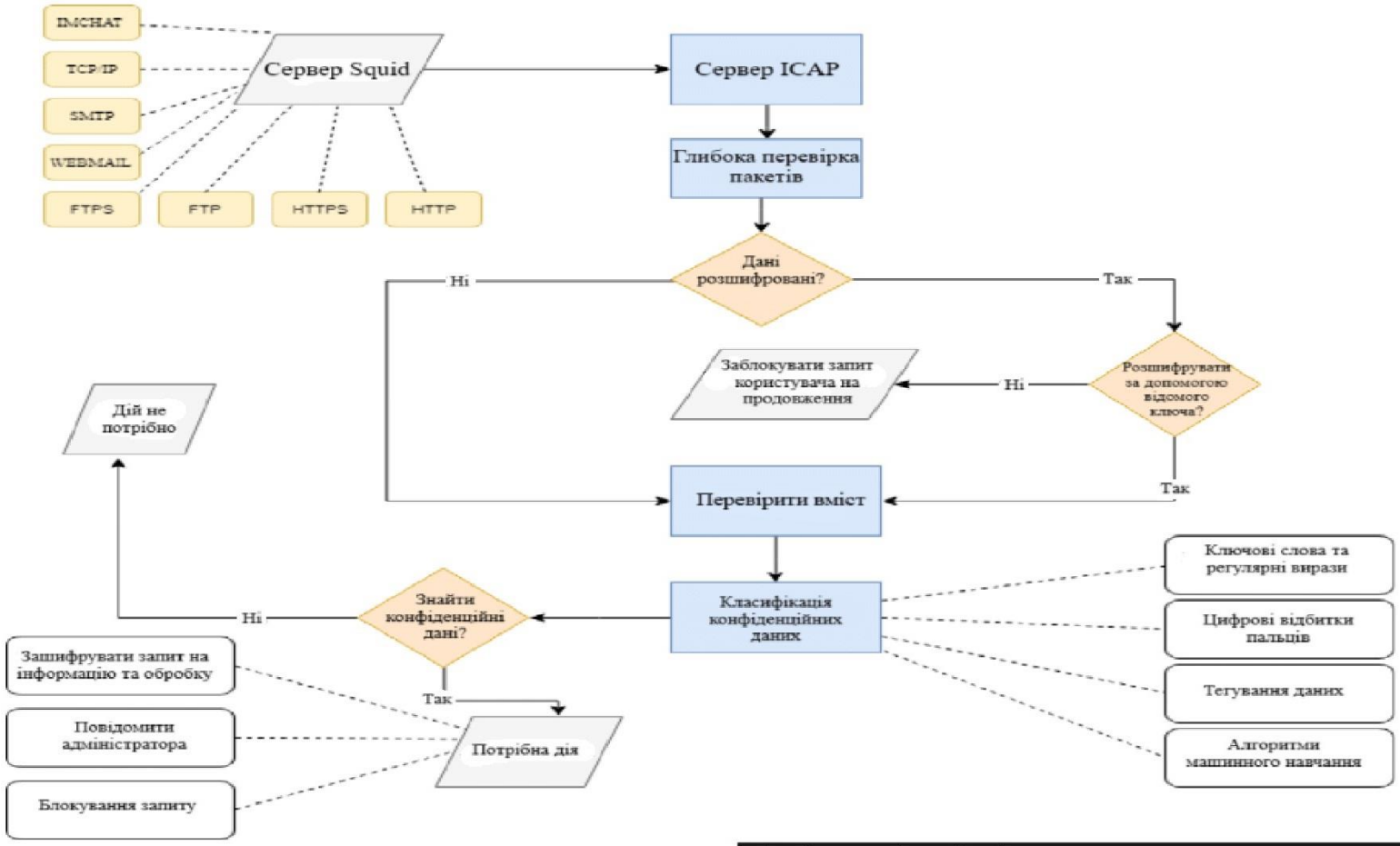
ДОДАТОК А

Копія графічної частини



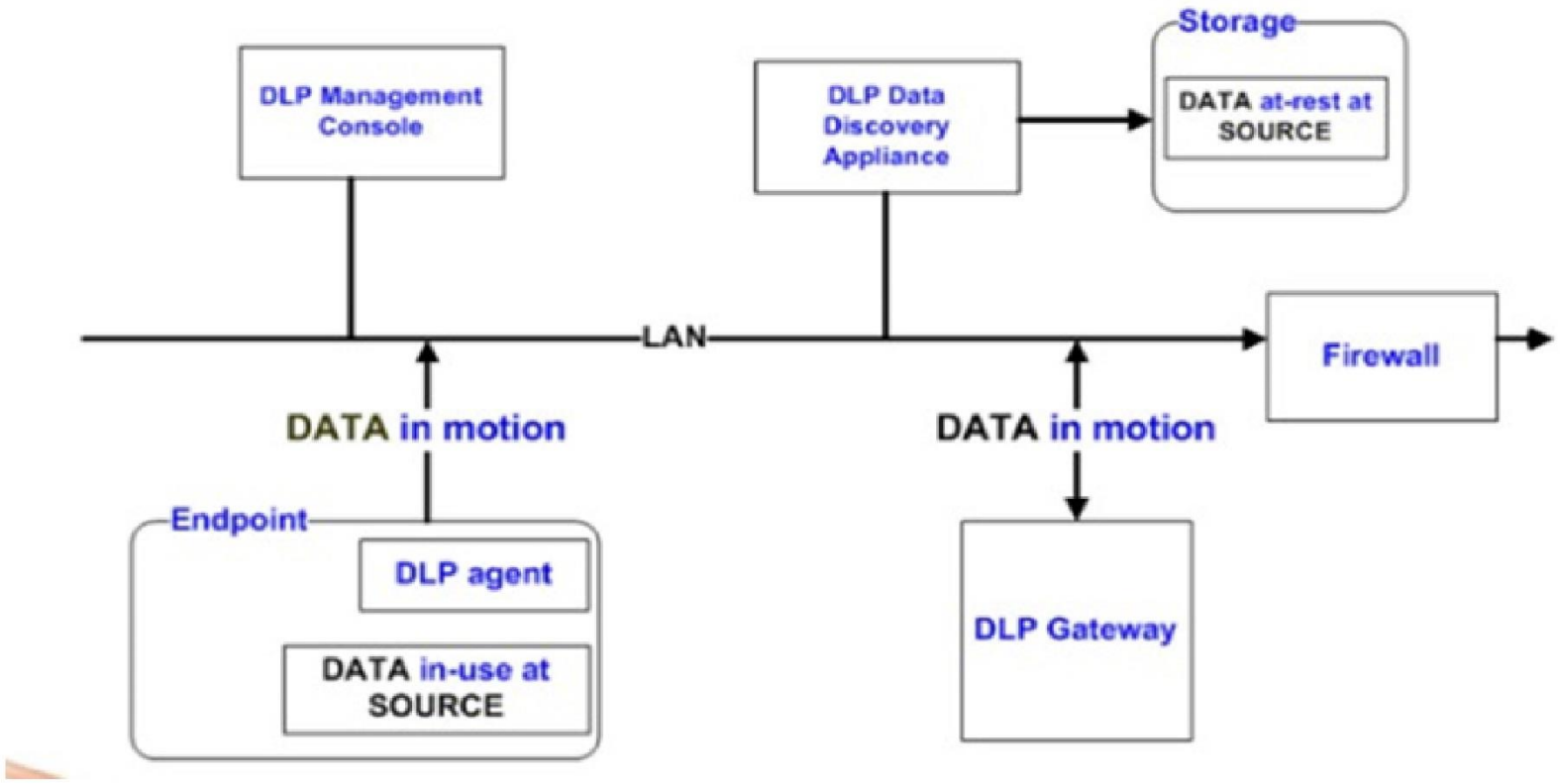


					КРБКБ.2102145.21.02.08 Е8
Зм.	Арк.	№ докум.	Підпис	Дата	Структурна схема системи захисту даних на зовнішньому носії
Розроб.		Драган Т.С.			Літера: — Маса: — Масштаб: —
Перевір.		Джулій В.М.			Аркуш 2 / Аркушів 4
Т.Контр.					
Н.Контр.		Мостовий С.В.			ХНУ КБ 21-2
Затверд.		Кльоц Ю.П.			



					КРБКБ.2102145.21.02.08 Е8	
					Алгоритм роботи системи захисту даних	Літера / Маса / Масштаб
Зм.	Арк.	№ докум.	Підпис	Дата		
Розроб.		Драган Т.С.				
Перевір.		Джулій В.М.				Аркуш 3 / Аркушів 4
Т.Контр.						
Н.Контр.		Мостовий С.В.				ХНУ КБ 21-2
Затверд.		Кльоц Ю.П.				

КРБКБ.2102145.21.02.08 Е8



					КРБКБ.2102145.21.02.08 Е8
Зм.	Арк.	№ докум.	Підпис	Дата	Типова архітектура DLP системи
Розроб.		Драган Т.С.			
Перевір.		Джулій В.М.			
Т.Контр.					
Н.Контр.		Мостовий С.В.			
Затверд.		Кльоц Ю.П.			

Літера	Маса	Масштаб
Аркуш 4	Аркушів 4	

ХНУ КБ 21-2

ДОДАТОК Б

Фрагмент програмного коду вузла контролю передачі конфіденційної інформації

```
import re
import os
import datetime
import mimetypes

# Шаблони для виявлення конфіденційних даних
SENSITIVE_PATTERNS = {
    "credit_card": r"\b(?:\d[ -]*?){13,16}\b",
    "email": r"[a-zA-Z0-9_.+-]+@[a-zA-Z0-9-]+\.[a-zA-Z0-9-.]+",
    "passport": r"\b[А-ЯІЇЄ]{2}\d{6}\b",  # приклад укр. паспорта
    "phone_number": r"\+?\d{10,13}"        # загальний шаблон телефону
}

# Журнал інцидентів
LOG_FILE = "security_log.txt"

def log_event(filepath, event_type, data_type=None):
    timestamp = datetime.datetime.now().strftime("%Y-%m-%d %H:%M:%S")
    log_entry = f"[{timestamp}] {event_type}: {filepath}"
    if data_type:
        log_entry += f" | Виявлено тип: {data_type}"
    with open(LOG_FILE, 'a', encoding='utf-8') as log:
        log.write(log_entry + "\n")
    print(log_entry)

# Перевірка розширення MIME-файлу (текстовий чи ні)
def is_text_file(filepath):
    mime_type, _ = mimetypes.guess_type(filepath)
    return mime_type is not None and mime_type.startswith("text")

# Функція перевірки вмісту на конфіденційні дані
def scan_file_for_sensitive_data(filepath):
    try:
        with open(filepath, 'r', encoding='utf-8', errors='ignore') as f:
            content = f.read()
            for data_type, pattern in SENSITIVE_PATTERNS.items():
                if re.search(pattern, content):
                    return True, data_type
    except Exception as e:
        log_event(filepath, "Помилка при скануванні")
        print(f"Помилка читання файлу: {e}")
    return False, None

# Блокування передачі файлу
def block_file_transfer(filepath, data_type):
```

```
    log_event(filepath, "Блокування передачі", data_type)
    print(f" Передача заблокована: виявлено конфіденційні дані типу '{data_type}'.")

# Основна функція моніторингу передачі
def monitor_external_device(file_to_transfer):
    print(f" Аналіз файлу: '{file_to_transfer}'")
    if not os.path.exists(file_to_transfer):
        print("Файл не знайдено.")
        return False

    if not is_text_file(file_to_transfer):
        log_event(file_to_transfer, "Пропущено: не текстовий файл")
        print(" Пропущено: тип файлу не підтримується для перевірки.")
        return True

    found, data_type = scan_file_for_sensitive_data(file_to_transfer)
    if found:
        block_file_transfer(file_to_transfer, data_type)
        return False
    else:
        log_event(file_to_transfer, "Передача дозволена")
        print("Файл не містить конфіденційних даних. Передача дозволена.")
        return True

# Тестування
if __name__ == "__main__":
    # Список файлів для тесту
    test_files = [
        "example_data.txt",
        "client_list.txt",
        "contract.docx",  # буде пропущено як не текстовий
        "passport_numbers.txt"
    ]
    for file in test_files:
        monitor_external_device(file)
```

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Драгана Тараса Сергійовича
ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КБ-21-2

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

01.06.25
дата

підпис

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Драган Тарас Сергійович

Співавтор:

Назва: Система безпечного зберігання конфіденційної інформації на зовнішніх пристроях

Науковий керівник:

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:2.2%

Коефіцієнт подібності 2:0.2%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-06-03 04:18:47.0

Після аналізу Звіту подібності констатую наступне:

☑ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

03.06.2025р.

Mon Jun 02 22:31:21 EEST 2025, Мостовий Сергій Володимирович, Хмельницький національний університет, ХНУ

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 1.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 8%**

	Document		Sum coincidence on the DB	
ID: 242998 Title: Система безпечного зберігання конфіденційної інформації на зовнішніх пристроях Added in a DB: 2025-06-02 Authors: Драган Тарас Сергійович Heads: Джулій В.М. Consultants: Opponents:	Symbols	Lexemes	Symbols	Lexemes
	96286	709	641 (1%)	8 (1%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система безпечного зберігання конфіденційної інформації на зовнішніх пристроях

Автор: Драган Тарас Сергійович

Спеціальність: 125 – Кібербезпека

Освітня програма: Кібербезпека

Науковий керівник: Володимир ДЖУЛІЙ, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 97.8%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism складає 99%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 24.09.2024, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100%, визначається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ Володимир ДЖУЛІЙ

Гарант ОП _____ Віктор Чешун

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Драган Тарас Сергійович

Тема Система безпечного зберігання конфіденційної інформації на зовнішніх пристроях

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 4; кількість сторінок записки 77.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі було досліджено питання захисту конфіденційної інформації при зберіганні на зовнішніх пристроях. Проведено аналіз загроз і методів захисту, розглянуто можливості DLP-систем, зокрема Safetica ONE. Реалізовано модель захищеного середовища, налаштовано контроль доступу до USB-пристроїв, що дозволяє ефективно запобігати витоку даних.

2. Висновок про відповідність кваліфікаційної роботи завданню. У кваліфікаційній роботі було виконано поставлене завдання як у теоретичній, так і в практичній частині. Зміст і результати дослідження підтверджують досягнення мети дипломної роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У кваліфікаційній роботі була виконана низка завдань, таких як наведення загальної характеристики задачі, визначення проблематики. У першому розділі проведено огляд цифрових носіїв інформації, загроз їх використання та сучасних методів захисту. У другому розділі здійснено обґрунтування вибору підходів до захисту даних, розроблено структурну та функціональну схему системи. Третій розділ присвячено практичній реалізації системи захисту на базі програмного продукту Safetica ONE, що відповідає сучасним підходам у сфері DLP та інформаційної безпеки. У роботі використано актуальні технології та сучасні методи контролю доступу до зовнішніх пристроїв.

4. Позитивні сторони роботи Проведено аналіз загроз, розроблено схему системи захисту, реалізовано її тестове впровадження з використанням Safetica ONE та налаштовано контроль доступу до зовнішніх носіїв. Тематика роботи має потенціал для подальшого розвитку та вдосконалення системи.

5. Негативні сторони роботи Розроблена система захисту базується на використанні Safetica ONE, що вимагає ліцензійного програмного забезпечення, що може бути фінансово недоступним для невеликих організацій. Впровадження системи потребує наявності кваліфікованих IT-фахівців для встановлення, налаштування та підтримки. Також існує ризик помилкових спрацювань або надмірного обмеження доступу, що може впливати на зручність роботи користувачів.

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення кваліфікаційної роботи відповідає темі роботи та виконане з дотриманням стандартів. У цілому графічне оформлення є якісним, а пояснювальна записка відповідає нормам оформлення.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки, оскільки весь матеріал роботи є структурованим, чітким та послідовним. Усі розділи роботи мають логічну послідовність, що сприяє зрозумінню викладеного матеріалу в рамках теми роботи. Графічний матеріал допомагає наочно продемонструвати доцільність та ефективність прийнятих рішень для досягнення мети.

8. Інші зауваження У переліку використаних джерел наявні посилання на популярні ресурси, такі як Вікіпедія. Такі джерела не рекомендовано використовувати при написанні кваліфікаційних робіт

9. Оцінка кваліфікаційної роботи Ураховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Бойко Юлій Миколайович,
доктор технічних наук, професор кафедри ТМІТ

« 10 » червня 2025. _____ (підпис)