

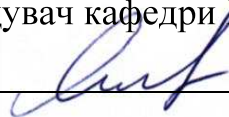
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут комп'ютерних наук та управління проектами
Кафедра інформаційних управляючих систем та технологій

"Допущений до захисту"

Завідувач кафедри ІУСТ



к.т.н, доц. Михелєв І.Л.

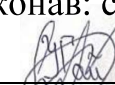
" ____ " _____ 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти "магістр"

**на тему: Дослідження технологій захисту корпоративних даних у
відкритих системах**

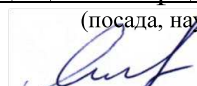
Виконав: студент групи 6141 мз



Гайдучок У. Т.
(підпис)

Керівник роботи:

доцент кафедри ІУСТ, к.т.н.,
(посада, науковий ступінь вчене звання)



Михелєв І. Л.
(підпис)

м. Миколаїв – 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут комп'ютерних наук та управління проектами

Кафедра інформаційних управляючих систем та технологій

Спеціальність 122 "Комп'ютерні науки"

Освітня програма "Комп'ютерні науки"

"ЗАТВЕРДЖУЮ"

Гарант освітньої програми

В. Ажищев

к.т.н, доц. Ажищев В.Ф.

" ____ " ____ 2025 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ на здобуття ступеня вищої освіти "магістр"

Студенту Гайдучок Уляні Тарасівній _____
(прізвище, ім'я, по батькові)

1. Тема роботи: «Дослідження технологій захисту корпоративних даних у відкритих системах» _____

Керівник роботи Михелєв Ігор Леонідович _____

Затверджені наказом ректора № 1355-уч. від "14" листопада 2025 року.

2. Термін подання роботи: 15 грудня 2025 р. _____

3. Вихідні дані до проєкту (роботи) ДСТУ щодо обробки інформації, літературні джерела, технічна документація на існуючі аналоги систем, матеріали наукового стажування _____

4. Перелік питань, що належать до розробки (найменування розділів)

Дослідження методів захисту даних корпоративних систем та постановка задачі;
Проектування інформаційної підсистеми захисту даних корпоративних систем;
Розробка інформаційної підсистеми захисту даних корпоративних систем;
Техніко-економічне обґрунтування розробки; Охорона праці; Охорона навколишнього середовища.

5. Перелік презентаційних матеріалів: електронна презентація. _____

6. Консультанти розділів роботи

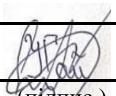
Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Михелєв І. Л.	05.09.2024	22.12.2024
2	Михелєв І. Л.	23.12.2024	15.06.2025
3	Михелєв І. Л.	15.06.2025	25.09.2025
4	Михелєв І. Л.	25.09.2025	14.11.2025
5	Михелєв І. Л.	25.09.2025	14.11.2025
6	Михелєв І. Л.	25.09.2025	14.11.2025

7. Дата видачі завдання 05 вересня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів роботи	Примітка
1	Дослідження та аналіз предметної галузі	22.12.2024	
2	Розробка концепції	15.03.2025	
3	Розділ з розробки проєктних рішень по системі (та її частинах)	15.06.2025	
4	Реалізація проєкту та розробка робочої документації	25.09.2025	
5	Обчислення економічної ефективності	14.11.2025	
6	Вирішення питань охорони праці та навколишнього середовища	14.11.2025	
7	Оформлення пояснювальної записки	14.11.2025	
8	Подання магістерської роботи на перевірку на плагіат	16.11.2025	
9	Подання магістерської роботи рецензенту	20.11.2025	
10	Подання магістерської роботи на державний захист	15.12.2025	

Студент


(підпис)

Гайдучок У.Т.

(ПІБ)

Керівник роботи


(підпис)

Михелєв І.Л.

(ПІБ)

АНОТАЦІЯ

Дану дипломну роботу присвячено Дослідженню технологій захисту корпоративних даних у відкритих системах.

Проведено аналіз сучасних загроз інформаційній безпеці та досліджено актуальні моделі й методи захисту даних, включаючи криптографічні алгоритми, механізми автентифікації та концепцію Zero Trust. Розроблено архітектуру інформаційної підсистеми, що забезпечує шифрування, захищене зберігання корпоративних даних та реєстрацію дій користувачів. Реалізовано програмний прототип клієнт-серверної системи з використанням технологій Python, Flask, SQLite та алгоритму AES.

Виконано техніко-економічне обґрунтування впровадження підсистеми, проаналізовано питання охорони праці та екологічної безпеки інформаційних технологій. Показано, що розроблена система може бути ефективно використана для підвищення безпеки корпоративних інформаційних ресурсів.

Роботу викладено на 111 сторінках машинописного тексту, містить 14 рисунків, 13 таблиць, 3 додатків та список використаної літератури з 35 найменувань.

Ключові слова: інформаційна безпека, захист даних, корпоративні системи, відкриті системи, шифрування, автентифікація, контроль доступу, конфіденційність, інформаційна підсистема, реєстрація дій користувачів, загрози безпеці, криптографія, безпечне зберігання даних.

ABSTRACT

This thesis is devoted to Research in Corporate Data Protection Technologies in Open Systems.

The work includes an analysis of modern information security threats and a study of current models and methods of data protection, including cryptographic algorithms, authentication mechanisms, and the Zero Trust concept. An architecture of the information security subsystem has been developed, providing data encryption, secure storage of corporate information, and user action recording. A software prototype of a client–server system has been implemented using Python, Flask, SQLite, and the AES encryption algorithm.

A techno-economic assessment of the subsystem’s implementation has been carried out, along with an analysis of occupational safety aspects and the environmental impact of information technologies. It has been demonstrated that the developed system can be effectively used to enhance the security of corporate information resources.

The thesis is presented on 111 pages of typescript, includes 14 figures, 13 tables, 3 appendices, and a list of references comprising 35 sources.

Keywords: information security, data protection, corporate systems, open systems, encryption, authentication, access control, confidentiality, information subsystem, user action recording, security threats, cryptography, secure data storage.

ЗМІСТ

ВСТУП

РОЗДІЛ 1. ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ДАНИХ КОРПОРАТИВНИХ СИСТЕМ ТА ПОСТАНОВКА ЗАДАЧІ

1.1. Аналіз предметної області щодо загроз інформаційній безпеці корпоративних систем

1.2. Огляд моделей інформаційних систем для захисту корпоративних даних

1.3 Розробка концепції інформаційної системи

1.4. Постановка задачі

Висновок до розділу 1

РОЗДІЛ 2. ПРОЄКТУВАННЯ ІНФОРМАЦІЙНОЇ ПІДСИСТЕМИ ЗАХИСТУ ДАНИХ КОРПОРАТИВНИХ СИСТЕМ

2.1 Загально системні рішення

2.2. Абстрактне представлення структури даних

2.3 Розробка бази даних

2.4 Діаграма послідовності для аналізу дослідження методів захисту даних корпоративних систем та аналіз предметної області

2.5 Математичне забезпечення розробки

Висновок до розділу 2

РОЗДІЛ 3. РОЗРОБКА ІНФОРМАЦІЙНОЇ ПІДСИСТЕМИ ЗАХИСТУ ДАНИХ КОРПОРАТИВНИХ СИСТЕМ

3.1. Діаграма розгортання

3.2 Технічні вимоги до системи

3.3 Програмні вимоги до системи

Висновок до розділу 3

РОЗДІЛ 4. ТЕХНІКО - ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ РОЗРОБКИ

4.1 Загальна характеристика роботи

4.2 Розрахунок витрат на проектування та впровадження системи визначено.

4.3 Розрахунок економічної ефективності розробки і впровадження системи

Висновок до розділу 4

РОЗДІЛ 5. ОХОРОНА ПРАЦІ

5.1 Вступ

5.2 Аналіз небезпечних і шкідливих факторів

5.3 Розрахунок освітленості робочого місця

5.4 Розробка заходів щодо зменшення впливу небезпечних і шкідливих факторів

Висновок до розділу 5

РОЗДІЛ 6. ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

6.1 Вступ

6.2 Загальні відомості про забруднення

6.3 Заходи щодо запобігання забруднення навколишнього середовища

Висновок до розділу 6

ВИСНОВКИ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Додаток А Інструкція користувача

Додаток Б Технічне завдання

Додаток В Фрагмент програмного коду.

ВСТУП

У сучасних умовах цифрової трансформації, коли інформація стала ключовим активом більшості підприємств, захист корпоративних даних набуває особливої важливості. З розвитком відкритих і розподілених інформаційних систем, а також активним впровадженням хмарних сервісів та мобільних платформ, істотно зростає рівень загроз для конфіденційності, цілісності та доступності корпоративних ресурсів. У таких умовах забезпечення комплексної інформаційної безпеки, зокрема захисту даних від зовнішніх і внутрішніх атак, несанкціонованого доступу та витоку, стає пріоритетним напрямом для сучасних організацій.

Особливе значення має питання захисту корпоративних даних у відкритих системах, де обмін інформацією відбувається через публічні мережі та міжрізними користувачами, пристроями і сервісами. Традиційні підходи до інформаційної безпеки виявляються недостатніми в умовах розподілених середовищ, що вимагає дослідження сучасних моделей захисту, адаптованих до новітніх архітектур і сценаріїв загроз. Це, зокрема, передбачає глибоке опрацювання методів шифрування, автентифікації, управління доступом, логування та моніторингу активності, що дозволяють створити надійну інформаційну підсистему для корпоративних потреб.

Метою цієї роботи є дослідження сучасних технологій захисту корпоративних даних у відкритих інформаційних системах, формування концепції надійної підсистеми безпеки та реалізація її програмного прототипу з урахуванням актуальних вимог до інформаційної безпеки. Об'єктом дослідження виступають корпоративні інформаційні системи, які функціонують у відкритому цифровому середовищі, а предметом – методи, засоби та технічні підходи до забезпечення цілісності, конфіденційності та контрольованості корпоративних даних.

Під час дослідження розглянуто актуальні загрози, пов'язані з роботою відкритих корпоративних систем, проведено аналіз існуючих методів захисту, розроблено власну концепцію безпечної інформаційної підсистеми та реалізовано її у вигляді програмного прототипу з підтримкою автентифікації, шифрування, контролю доступу й логування дій користувачів. Окрема увага приділяється техніко-економічному обґрунтуванню розробки та питанням охорони праці і захисту довкілля в процесі впровадження.

РОЗДІЛ 1. ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ДАНИХ КОРПОРАТИВНИХ СИСТЕМ ТА ПОСТАНОВКА ЗАДАЧІ

1.1. Аналіз предметної області щодо загроз інформаційній безпеці корпоративних систем

Із розвитком цифрових технологій та зростанням обсягів оброблюваної інформації корпоративні системи опинилися в центрі постійно зростаючої кількості кіберзагроз. Особливо уразливими стають ті середовища, що працюють у відкритих мережах, де взаємодія з численними зовнішніми сервісами, пристроями та користувачами супроводжується ризиками порушення конфіденційності, цілісності та доступності даних. Загрози інформаційній безпеці прийнято класифікувати за кількома основними напрямками, що охоплюють як зовнішні технічні атаки, так і внутрішні недбалі дії користувачів.

На рисунку 1.1 зображено основні типи загроз, що виникають у корпоративних системах, із деталізацією причин і потенційних вразливостей. Як видно зі схеми, до технічних загроз належать мережеві атаки, серед яких домінують DDoS-атаки, перехоплення трафіку, використання експлойтів і zero-day вразливостей. Ці атаки здебільшого спрямовані на недоліки в інфраструктурі, такі як застаріле програмне забезпечення або неправильна конфігурація систем захисту. Технічні вразливості, зокрема відкриті порти, слабкі механізми автентифікації та відсутність сучасних протоколів шифрування, створюють умови для реалізації широкого спектру атак, особливо у відкритих інформаційних середовищах.

Соціальні загрози, які представлені фішингом та прийомами соціальної інженерії, також займають значну частку у загальній структурі ризиків. Вони ґрунтуються на маніпуляціях із поведінкою персоналу та дозволяють зловмисникам отримати доступ до конфіденційних відомостей без необхідності технічного втручання. Водночас внутрішні загрози, пов'язані з людським

фактором, заслуговують на не меншу увагу. Недбалість співробітників у дотриманні політик безпеки, зокрема застосування слабких паролів або використання відкритих каналів зв'язку, може стати причиною витоку критично важливих даних. Іще більш небезпечними є навмисні дії з боку інсайдерів, що мають доступ до інформаційних систем, адже вони здатні обходити засоби захисту зсередини.



Рисунок 1.1 – Класифікація загроз інформаційній безпеці корпоративних систем

У моделі, що представлена на рисунку 1.1, також відображено криптографічні вразливості. Серед них – використання застарілих алгоритмів шифрування (наприклад, MD5, SHA-1), відсутність HTTPS-протоколів для передавання даних, а також ігнорування обов'язкового шифрування резервних копій. Не менш критичним є й блок, присвячений проблемам автентифікації. У багатьох компаніях досі використовуються паролі у відкритому вигляді без обов'язкового впровадження двофакторної аутентифікації, що значно підвищує ризик компрометації облікових записів.

Корпоративні системи зазнають впливу як зовнішніх, так і внутрішніх факторів ризику. Зовнішні загрози зазвичай виникають через Інтернет або IoT-

пристрої, які недостатньо захищені й можуть бути використані як точка входу до корпоративного середовища. Внутрішні інциденти часто пов'язані або з випадковими помилками співробітників, або з навмисними діями осіб, що мають прямий або непрямий доступ до системи.

Серед технічних вразливостей найбільш поширеними є застарілі версії програмного забезпечення, що більше не отримують оновлень безпеки, а також конфігурації, які не відповідають рекомендаціям з кібергігієни. Окремої уваги заслуговує відсутність належного логування та аудиту дій користувачів, що унеможлиблює вчасне виявлення вторгнень або аномальної активності. Усі перелічені фактори створюють сприятливе середовище для впровадження зловмисного програмного забезпечення, особливо шкідливих програм-шифрувальників, які здатні паралізувати діяльність організації.

Типовими сценаріями реалізації кіберзагроз можуть бути перехоплення даних у незашифрованому каналі, що вимагає впровадження VPN-тунелів та використання протоколів TLS; компрометація облікових даних через витік паролів, що вирішується шляхом застосування багатофакторної автентифікації; а також масове зараження систем через шкідливе ПЗ, яке потребує використання актуального антивірусного захисту та ізольованих середовищ для роботи з підозрілими файлами.

1.2. Огляд моделей інформаційних систем для захисту корпоративних даних

Формування ефективної системи інформаційної безпеки в умовах відкритих мережевих середовищ передбачає використання апробованих моделей захисту, які забезпечують організаціям високий рівень захищеності. Зростання обсягів даних, що обробляються в корпоративному середовищі, збільшує потребу в структурованих підходах до проектування систем безпеки. Саме тому у

практиці застосовується низка концептуальних моделей, які є основою для побудови захищених інформаційних систем.

Однією з найбільш відомих є модель довірчого обчислення, яка ґрунтується на створенні контрольованого середовища, де взаємодія апаратного й програмного забезпечення регулюється спеціалізованими механізмами, зокрема апаратними модулями типу TPM. Такий підхід дозволяє гарантувати захист операційної системи від несанкціонованих змін і підтримувати криптографічну цілісність програмного коду. Ця модель знайшла широке застосування в критично важливих сферах, зокрема у фінансовому секторі, де довіра до інфраструктури має першочергове значення.

Іншою універсальною моделлю є триєдина концепція CIA, що передбачає забезпечення конфіденційності, цілісності та доступності даних. Цей підхід є базовим і вбудовується в більшість сучасних стандартів інформаційної безпеки, включаючи ISO/IEC 27001. Він застосовується у всіх типах організацій як концептуальна основа для побудови політик безпеки.

Багатошаровий підхід реалізується в моделі захисту за глибиною, яка передбачає наявність послідовно вибудованих рубежів безпеки: від мережевого фільтрування до захисту фізичного доступу. Поєднання технічних, організаційних та адміністративних засобів дає змогу стримувати навіть складні атаки, які використовують кілька векторів одночасно. Водночас така модель потребує значних ресурсів для впровадження та підтримки, тому найчастіше реалізується у великих корпораціях або державних установах.

У контексті розвитку хмарних технологій особливої популярності набуває модель нульової довіри. У ній жоден користувач або пристрій не вважається довіреним за замовчуванням, незалежно від того, чи перебуває він у внутрішній мережі, чи за її межами. Кожен запит доступу проходить повторну перевірку, а автентифікація та авторизація здійснюються динамічно з урахуванням контексту.

Такий підхід ефективно працює в умовах віддаленої роботи, однак може створювати додаткове навантаження на системи доступу.

Ще однією широко вживаною моделлю є модель управління доступом на основі ролей (RBAC). У ній контроль реалізується шляхом призначення ролей, що мають наперед визначені права доступу до ресурсів. Це значно спрощує адміністрування, особливо у великих організаціях з великою кількістю працівників. Проте така модель менш чутлива до змін у контексті поведінки користувача, наприклад до нетипових дій, що вимагають контекстної перевірки.

Для зіставлення ключових характеристик описаних моделей доцільно звернутися до таблиці 1.1, у якій наведено порівняльний аналіз переваг та недоліків кожної концепції захисту корпоративних даних.

Таблиця 1.1 – Порівняльний аналіз моделей інформаційної безпеки

Модель	Переваги	Недоліки
Trusted Computing	Висока надійність, апаратний рівень захисту	Потребує спеціалізованого обладнання, складність реалізації
CIA Triad	Універсальність, простота концепції	Відсутність конкретних механізмів реалізації
Defense-in-Depth	Багатошаровий захист, адаптація до складних атак	Висока вартість впровадження
Zero Trust	Постійний контроль, підходить для хмарних середовищ	Може знижувати продуктивність через часті перевірки
RBAC	Простота управління доступом, масштабованість	Не враховує динамічні аспекти, наприклад, контекст дій користувача

Узагальнюючи, варто зазначити, що вибір моделі захисту залежить від особливостей бізнес-процесів, рівня ризику та доступних ресурсів. Найбільш ефективним підходом є комбінування кількох моделей, що дозволяє створити

багаторівневу систему безпеки, здатну адаптуватися до динамічних умов середовища та нових типів загроз.

1.2.1. Дослідження потенційних методів для вирішення поставлених задач

Побудова ефективної системи захисту корпоративних даних у відкритих середовищах вимагає комплексного аналізу сучасних технологічних рішень. Одним із ключових напрямів є впровадження надійних методів аутентифікації та авторизації, які дозволяють точно ідентифікувати користувачів і забезпечувати контрольований доступ до інформаційних ресурсів. Зокрема, широко використовується багатофакторна аутентифікація, яка поєднує кілька незалежних способів підтвердження особи, таких як пароль, мобільний пристрій або біометричні дані. Це значно знижує ймовірність несанкціонованого доступу, хоча й потребує додаткового технічного оснащення або відповідного рівня підготовки користувачів.

У більш складних середовищах застосовується контекстна авторизація, яка враховує не лише ідентичність користувача, але й такі фактори, як місце розташування, час доступу або тип пристрою. Цей підхід забезпечує динамічну гнучкість і дає змогу обмежити доступ у разі нетипової поведінки, однак його впровадження вимагає значних обчислювальних ресурсів та ретельної попередньої конфігурації політик безпеки.

Ще одним важливим аспектом є використання криптографічних методів, які реалізуються за допомогою різних схем шифрування. Найбільш поширеним у корпоративних системах є симетричне шифрування, де для зашифрування та розшифрування даних використовується один і той самий ключ. Такий підхід забезпечує високу швидкість обробки, що особливо важливо при роботі з великими обсягами інформації. Проте симетричні методи потребують надійного

захищеного каналу для обміну ключами між сторонами, що не завжди можливо в умовах відкритого середовища.

Асиметричне шифрування, натомість, дозволяє уникнути проблеми безпечного обміну ключами завдяки використанню пари ключів – відкритого для шифрування і закритого для розшифрування. Цей підхід ідеально підходить для захисту передачі даних, хоча й поступається за продуктивністю симетричним алгоритмам. Його застосування найчастіше спостерігається в електронному документообігу, підписуванні даних та захищеному спілкуванні через Інтернет.

Окрему нішу займає гомоморфне шифрування, яке дозволяє виконувати обчислення над зашифрованими даними без необхідності їхнього розшифрування. Це відкриває широкі можливості для обробки чутливої інформації у хмарних середовищах, наприклад, у сфері фінансів чи охорони здоров'я. Водночас такий підхід супроводжується значними обчислювальними витратами, що обмежує його масове застосування у корпоративному секторі.

Аналіз показує, що жоден із розглянутих методів не може гарантувати повну безпеку корпоративної інформації у відкритих системах самостійно. Найбільш ефективним підходом є поєднання кількох технологій у межах єдиної архітектури безпеки. Таке комбінування дозволяє враховувати специфіку загроз, ресурси організації та типову поведінку користувачів. Застосування багаторівневих стратегій, у яких об'єднуються криптографічні засоби, контроль доступу, політики безпеки та підготовка персоналу, дозволяє створити гнучку й надійну систему захисту корпоративних даних у відкритих середовищах.

1.2.2. Методи шифрування для захисту даних

Шифрування становить один із найбільш надійних засобів забезпечення інформаційної безпеки корпоративних систем. Воно дозволяє гарантувати

конфіденційність, цілісність та захищеність даних як у процесі їх зберігання, так і під час передавання. У сучасних умовах застосовуються різноманітні методи шифрування, кожен з яких має власну специфіку, переваги та технічні обмеження.

Найбільш поширеним підходом є симетричне шифрування, у якому один і той самий ключ використовується як для шифрування, так і для розшифрування інформації. До прикладу, алгоритм AES забезпечує високу швидкість обробки даних та стійкість до відомих типів атак, що зумовило його широке впровадження у промислових і державних інформаційних системах. Водночас його головним обмеженням є потреба у безпечному розповсюдженні ключа, що може створювати додаткові вектори ризику.

Асиметричне шифрування, яке базується на використанні пари ключів – відкритого і закритого – дозволяє мінімізувати ризики, пов'язані з передаванням ключів. Наприклад, алгоритми RSA або ECC активно використовуються для захисту комунікацій у мережі Інтернет, а також для підписування документів у цифровому середовищі. Однак порівняно з симетричними, такі алгоритми мають нижчу швидкість обробки даних і вимагають більших обчислювальних потужностей.

Компромісом між цими двома підходами стало гібридне шифрування, у якому асиметричні методи використовуються для безпечного передавання симетричних ключів, а симетричні – для подальшої обробки інформації. Такий підхід лежить в основі більшості сучасних захищених протоколів, включно з TLS та HTTPS, що забезпечують безпечний обмін даними між клієнтами та серверами в мережі.

Сучасні завдання інформаційної безпеки вимагають і нових підходів до шифрування, серед яких виділяється гомоморфне шифрування. Його особливістю є можливість виконання обчислень над зашифрованими даними без їхнього попереднього розшифрування. Це відкриває перспективи для обробки

конфіденційної інформації у хмарних середовищах, де власник даних не може повністю контролювати інфраструктуру. Попри значні переваги в контексті конфіденційності, такі алгоритми залишаються ресурсоємними та малопридатними для задач, де потрібна висока продуктивність у реальному часі.

Окрім принципів шифрування, важливо також враховувати тип побудови алгоритмів. Блочні шифри, які працюють із фіксованими блоками даних, добре підходять для шифрування великих масивів інформації, баз даних і архівів. У той же час, потокові шифри, які оперують з даними послідовно, ідеально справляються з завданнями шифрування мережевого трафіку, де важлива мінімальна затримка.

Як видно з таблиці 1.2, кожен із розглянутих підходів має свою нішу застосування, і вибір відповідного алгоритму визначається вимогами до продуктивності, захищеності, простоти інтеграції та вартості впровадження.

Таблиця 1.2 – Порівняльна характеристика основних методів шифрування

Метод шифрування	Принцип роботи	Переваги	Недоліки	Сфери застосування
Симетричне	Один ключ для шифрування і дешифрування	Висока швидкість, простота реалізації	Проблема обміну ключами	Захист великих обсягів даних
Асиметричне	Пара ключів: відкритий і закритий	Безпечний обмін ключами, цифрові підписи	Низька швидкість, високе навантаження на систему	Електронні підписи, передача ключів
Гібридне	Комбінація симетричного та асиметричного шифрування	Висока безпека та швидкодія	Ускладнена реалізація	Протоколи TLS, HTTPS
Гомоморфне	Обчислення над зашифрованими даними	Максимальна конфіденційність при обробці	Висока обчислювальна складність	Хмарні сервіси, обробка чутливих даних
Блочне шифрування	Розбиття на блоки та послідовне шифрування	Надійність, стійкість до атак	Повільніше в реальному часі	Файлові системи, БД

Метод шифрування	Принцип роботи	Переваги	Недоліки	Сфери застосування
Потокове шифрування	Шифрування по одному біту або символу	Швидка обробка потоків даних	Чутливість до помилок в реалізації	Мережевий трафік, мобільний зв'язок

1.2.3. Методи аутентифікації та контролю доступу

Захист корпоративних даних неможливий без ефективних засобів ідентифікації користувачів та управління їхнім доступом до інформаційних ресурсів. В умовах постійного зростання кількості кібератак, а також з огляду на складність сучасних інформаційних систем, компанії повинні впроваджувати комплексні рішення, які забезпечують автентичність суб'єктів доступу та обмежують доступ лише до тих ресурсів, які необхідні для виконання функціональних обов'язків.

Традиційним засобом ідентифікації залишаються паролі та PIN-коди. Вони базуються на знанні певної інформації користувачем, проте мають значні недоліки – низький рівень безпеки при поганій практиці користування, вразливість до атак перебором, фішингу або витоку через ненадійне зберігання. Політики використання складних паролів, їх регулярна зміна та обмеження кількості спроб входу частково знижують ці ризики, але сам по собі цей метод є недостатнім для сучасних умов.

Біометрична аутентифікація набирає популярності завдяки високій надійності та зручності використання. Унікальні фізіологічні або поведінкові характеристики людини, такі як відбитки пальців, структура обличчя або голос, дозволяють точно ідентифікувати користувача. Цей підхід широко впроваджено в мобільних пристроях, платіжних системах і корпоративному ПЗ. Проте біометричні дані мають певну вразливість до імітацій, а також є незмінними, що ускладнює їх "перегенерацію" у разі витоку.

Ефективним і поширеним методом залишається використання фізичних пристроїв: смарт-карток, токенів або USB-ключів. Вони зберігають ключі шифрування або одноразові паролі, не передаючи їх безпосередньо в систему, що знижує ризик перехоплення. Але фізичну втрату або крадіжку таких пристроїв важко виключити, тож найкращим варіантом вважається поєднання цього методу з іншими – наприклад, з паролем чи біометрією.

Важливим елементом сучасної цифрової безпеки є багатофакторна аутентифікація. Вона дозволяє перевірити особу за кількома незалежними ознаками: знання (пароль), володіння (пристрій) та біометрія. Цей підхід вважається найбільш надійним і дає змогу значно знизити ймовірність компрометації навіть у випадку злому одного з факторів. Незважаючи на це, надмірне ускладнення процесу входу може викликати невдоволення користувачів, тому важливо дотримуватись балансу між безпекою та зручністю.

Контроль доступу реалізується через політики, що визначають повноваження користувачів. Найбільш поширеною є модель контролю на основі ролей (RBAC), що дозволяє надавати права доступу до ресурсів не окремим користувачам, а їхнім ролям у системі. Це полегшує адміністрування, особливо у великих організаціях. Розширенням цього підходу є модель ABAC – контроль доступу на основі атрибутів, яка дозволяє враховувати не лише роль, а й контекст доступу: час, місце, пристрій, рівень ризику.

Контекстна аутентифікація є новітнім підходом, який дозволяє додатково перевіряти поведінкові або мережеві особливості під час спроби входу. Наприклад, якщо вхід виконується з незвичного місця, у незвичний час, або з нового пристрою, система може вимагати додаткову перевірку. Такий підхід добре поєднується з моделлю нульової довіри.

Модель Zero Trust, яка полягає у відсутності апріорної довіри до будь-якого пристрою чи користувача, вимагає постійної перевірки всіх запитів, незалежно від того, чи походять вони з внутрішньої, чи з зовнішньої мережі. Реалізація цієї

концепції включає багатофакторну аутентифікацію, мікросегментацію мережі, інтелектуальний аналіз запитів та повне логування.

У таблиці 1.3 наведено порівняння основних методів аутентифікації та контролю доступу за критеріями безпеки, зручності використання, вартості впровадження та придатності до масштабування.

Таблиця 1.3 – Порівняння методів аутентифікації та контролю доступу

Метод	Безпека	Зручність	Вартість впровадження	Масштабованість
Паролі / PIN-коди	Низька	Висока	Низька	Висока
Біометрія	Висока	Висока	Середня / Висока	Середня
Фізичні токени	Висока	Середня	Висока	Середня
Багатофакторна аутентифікація	Дуже висока	Середня	Середня / Висока	Висока
RBAC	Висока	Висока	Низька / Середня	Висока
ABAC	Висока	Середня	Висока	Висока
Контекстна аутентифікація	Дуже висока	Висока	Висока	Висока
Zero Trust	Дуже висока	Середня	Висока	Висока

1.2.4. Методи логування та моніторингу

Ефективне забезпечення інформаційної безпеки неможливе без надійних механізмів логування та моніторингу. Ці інструменти відіграють важливу роль у виявленні порушень, розслідуванні інцидентів, а також у забезпеченні відповідності чинним нормативам та внутрішнім політикам компанії. Їхнє впровадження дозволяє створити прозору картину діяльності системи, забезпечити безперервне спостереження за поведінкою користувачів і компонентів мережі, а також вчасно реагувати на потенційні загрози.

Суть логування полягає в автоматичному фіксуванні подій, що відбуваються у системі: починаючи від звичайних дій користувачів і завершуючи критичними змінами в конфігурації або спробами несанкціонованого доступу. Якість логування визначається низкою принципів. По-перше, повнота передбачає, що всі ключові події повинні бути зафіксовані, включаючи як успішні, так і невдалі дії. По-друге, точність вимагає чіткої ідентифікації події, із зазначенням часу, користувача, IP-адреси та інших атрибутів. По-третє, забезпечення цілісності логів є обов'язковим для недопущення їхньої модифікації, а доступність – для швидкого доступу уповноважених осіб.

Типи логів можуть бути класифіковані залежно від джерела інформації. Системні журнали містять інформацію про роботу ОС і апаратних засобів. Мережеві журнали фіксують дії на рівні з'єднань, запити DNS, звернення до фаєрволів тощо. Додатково, логи прикладного рівня відображають поведінку програмного забезпечення, включно з доступом до баз даних чи помилками виконання. Особливе місце займають аудиторські журнали, які фіксують дії користувачів щодо обробки конфіденційної інформації або змін у критичних конфігураціях.

У тісному зв'язку з логуванням працює моніторинг – постійне спостереження за станом системи. Його мета – виявлення аномалій у поведінці користувачів або компонентів ще до того, як ці дії призведуть до серйозного порушення безпеки. Моніторинг може бути проактивним – з акцентом на передбачення загроз, або реактивним – зосередженим на аналізі вже скоєних інцидентів. Сучасні інструменти забезпечують моніторинг у реальному часі, що дозволяє оперативно виявляти та нейтралізувати загрози.

Інструменти логування та моніторингу представлені широким спектром програмних рішень. SIEM-платформи, такі як IBM QRadar або Splunk, забезпечують збір, зберігання, кореляцію подій та виявлення аномалій. Для аналізу мережевих даних використовуються системи Wireshark, Zabbix або

Nagios. Важливу роль відіграють лог-сервери, зокрема Graylog чи стек ELK, які забезпечують централізоване управління логами. Інструменти на основі машинного навчання, як-от Darktrace чи Vectra, дозволяють виявляти нетипову поведінку, яка може свідчити про приховані атаки або внутрішні загрози.

Важливою умовою ефективності системи логуювання та моніторингу є правильна конфігурація. Необхідно чітко визначити критичні точки контролю, автоматизувати збір і збереження даних, а також організувати регулярний аудит логів. Логи мають зберігатися в зашифрованому вигляді у захищеному середовищі, доступ до якого мають виключно уповноважені особи.

У таблиці 1.4 представлено узагальнене порівняння основних типів логуювання та моніторингу, з урахуванням їхніх ключових характеристик та прикладів застосування.

Таблиця 1.4 – Порівняльна характеристика типів логуювання та моніторингу

Тип або метод	Призначення	Основні переваги	Приклади інструментів
Системні логи	Фіксація подій ОС, адміністрування	Діагностика та аудит	Windows Event Viewer, syslog
Мережеві логи	Моніторинг трафіку, з'єднань, фаєрволів	Виявлення аномалій у мережі	Wireshark, Zabbix, pfSense
Логи додатків	Відображення роботи програмного забезпечення	Аналіз програмних збоїв	Log4j, AppDynamics
Аудиторські логи	Облік дій користувачів з привілейованим доступом	Відстеження критичних змін	SIEM-системи, auditd
SIEM-системи	Комплексна обробка та кореляція логів	Централізований контроль і аналітика	Splunk, IBM QRadar, ArcSight
Моніторинг у реальному часі	Негайне виявлення інцидентів	Швидке реагування	Kibana, Prometheus

Тип або метод	Призначення	Основні переваги	Приклади інструментів
Машинне навчання	Виявлення нетипової поведінки	Профілактика прихованих загроз	Darktrace, Vectra AI

1.3 Розробка концепції інформаційної системи

Розробка концепції інформаційної системи захисту корпоративних даних є ключовим етапом, який визначає загальну архітектуру, функціональні можливості та рівень безпеки системи. Її основною метою є формування цілісного підходу до забезпечення конфіденційності, цілісності та доступності корпоративної інформації в умовах відкритих і потенційно вразливих середовищ.

Концепція інформаційної безпеки базується на реалізації багаторівневого захисту, що враховує різні сценарії атак та потенційні загрози. Система має бути здатною реагувати як на зовнішні, так і на внутрішні виклики, використовуючи сучасні технології захисту, включно з автентифікацією, шифруванням, сегментацією мережі та системами виявлення вторгнень. На практиці це означає, що кожен рівень доступу повинен бути захищеним незалежно, навіть якщо інші ланки ланцюга будуть скомпрометовані.

Ключовим підходом до побудови такої системи є модульне проєктування, яке дозволяє розділити функціональність на окремі компоненти – керування доступом, шифрування, моніторинг, аналіз, захист мережі. Це забезпечує можливість масштабування та оновлення окремих частин без ризику для функціонування всієї інфраструктури. З огляду на зростаюче використання хмарних платформ і мобільних пристроїв, доцільним є впровадження моделі нульової довіри (Zero Trust), де кожен запит доступу проходить обов’язкову перевірку, незалежно від джерела.

Для візуалізації структури майбутньої системи нижче наведено схему ключових її компонентів (рисунок 1.2). У центрі концепції знаходяться чотири

основні блоки: **управління доступом, захист мережі, моніторинг і аналітика**, а також **шифрування**.

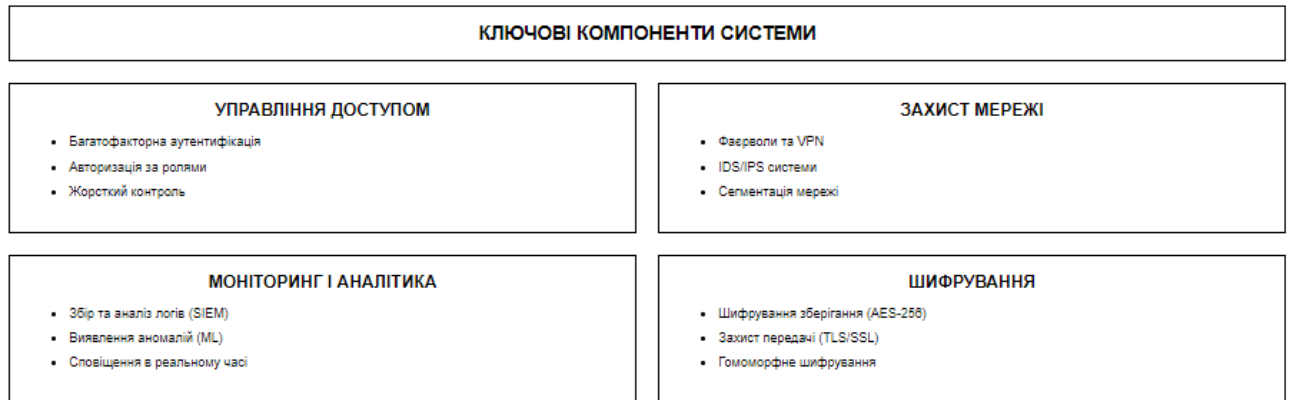


Рисунок 1.2 – Ключові компоненти інформаційної системи захисту корпоративних даних

Кожен із компонентів виконує окрему роль у загальному ланцюгу безпеки. Управління доступом охоплює реалізацію багатофакторної автентифікації, авторизацію за ролями та контроль над підозрілими активностями. Засоби захисту мережі, включаючи фаєрволи, VPN, системи IDS/IPS та сегментацію, забезпечують ізоляцію критичних ресурсів від потенційних загроз. Компонент моніторингу й аналітики відповідає за збір логів, виявлення аномалій (зокрема за допомогою алгоритмів машинного навчання), а також формування сповіщень у режимі реального часу. Шифрування відіграє вирішальну роль як на рівні зберігання (наприклад, AES-256), так і на етапі передавання даних (TLS/SSL), а також підтримує гомоморфні механізми для обробки конфіденційної інформації без її розшифрування.

Не менш важливим елементом концепції є резервне копіювання. Воно забезпечує захист від втрати даних у разі збоїв, атак або катастроф, передбачаючи регулярне створення зашифрованих копій зберігання у віддалених географічних точках.

Загалом процес впровадження системи охоплює кілька етапів. Спочатку здійснюється аналіз вимог та оцінка ризиків. Далі формується архітектура, обираються відповідні технології й визначається взаємодія між компонентами. Після технічної реалізації проводиться тестування на відповідність політикам безпеки й здатність протистояти атакам. Завершальним етапом стає навчання персоналу, що забезпечує правильну експлуатацію системи та своєчасне реагування на інциденти.

1.3.1. Розробка концепції застосунку для захисту корпоративних даних

Метою створення такого застосунку є забезпечення комплексного централізованого захисту корпоративної інформації на основі сучасних методів багатофакторної аутентифікації, криптографічного захисту, систем аналітики та гнучкого управління правами доступу. Серед ключових завдань, що вирішує система, можна виділити забезпечення захищеного доступу до внутрішніх сервісів компанії, незалежно від фізичного розташування працівників, реалізацію надійного шифрування даних як під час зберігання, так і в процесі передавання, впровадження механізмів виявлення загроз у режимі реального часу, а також надання адміністраторам інструментів для централізованого керування користувачами та політиками безпеки.

Застосунок має реалізовувати сучасні засоби автентифікації, що включають багатофакторні механізми з можливістю використання біометричних параметрів, таких як відбитки пальців або розпізнавання обличчя. Авторизація має враховувати контекстні фактори, серед яких – тип пристрою, місце доступу або час доби. Додатково впроваджуються механізми OTP для підтвердження доступу. У контексті захисту даних передбачено використання симетричного шифрування на основі алгоритму AES-256, підтримку безпечної передачі

інформації через протоколи TLS/SSL, а також реалізацію функцій резервного копіювання із багаторівневим шифруванням і можливістю автоматичного знищення даних у разі втрати чи компрометації пристрою.

Моніторинг реалізується як у реальному часі, так і на основі періодичного аналізу логів. Застосунок генерує сповіщення при фіксації атипових подій, таких як спроби входу з невідомих пристроїв або з незвичних локацій. Важливою функцією є інтеграція з зовнішніми SIEM-системами для підвищення рівня обробки подій. Передбачено також управління пристроями, що включає їхню попередню реєстрацію, перевірку відповідності вимогам безпеки, можливість віддаленого блокування, очищення та встановлення обмежень для підозрілих або незахищених середовищ.

Розділ аналітики забезпечує формування детальних звітів щодо поведінки користувачів, зокрема, спроб доступу, змін конфігурацій і дій із чутливими даними. Візуалізація інформації дозволяє виявляти тенденції, що можуть свідчити про поступову ескалацію загроз. Передбачено автоматизоване реагування на інциденти шляхом передачі даних до спеціалізованих платформ.

Архітектура запропонованого рішення включає клієнтську частину, серверну інфраструктуру, систему зберігання й модулі аналітики. Клієнтська частина охоплює мобільні застосунки, десктопні програми та веб-інтерфейс для адміністративного керування. Серверна частина включає модулі автентифікації, шифрування, API для взаємодії з іншими системами та служби моніторингу. Сховище даних повинно бути захищене, підтримувати реплікацію для підвищення відмовостійкості та відповідати високим стандартам конфіденційності. Аналітичні компоненти базуються на обробці логів і алгоритмах виявлення аномалій із застосуванням машинного навчання.

Модель розгортання передбачає три можливих варіанти. Хмарне розміщення забезпечує гнучкість та масштабованість, локальне – підвищену конфіденційність і незалежність від зовнішніх факторів, а гібридна модель

поєднує переваги обох підходів, дозволяючи оптимізувати витрати та ефективно розподіляти ресурси.

У контексті технологій для серверної логіки рекомендовано використовувати фреймворки на основі Python або Node.js із базами даних PostgreSQL або MongoDB. Для реалізації криптографічних функцій ефективним є застосування бібліотеки OpenSSL. Клієнтська частина може базуватися на React або Angular, а мобільні застосунки – на Flutter, Swift або Java. Моніторинг реалізується за допомогою стеку Elasticsearch + Kibana, а для побудови моделей виявлення аномалій можуть використовуватись TensorFlow або PyTorch.

1.3.2. Побудова моделей обміну інформацією в рамках застосунку

Забезпечення надійного обміну інформацією в межах корпоративного застосунку є ключовим аспектом захисту даних, що передаються між компонентами системи. У межах розробки розглядається модель взаємодії, яка гарантує конфіденційність, цілісність і автентичність інформації за допомогою сучасних механізмів шифрування, авторизації та контролю доступу.

Основою архітектури взаємодії між клієнтами та сервером є класична клієнт-серверна модель, у якій обмін повідомленнями відбувається через захищене програмне API. Для забезпечення безпечного передавання використовується шифрування на двох рівнях – під час зберігання даних застосовується симетричний алгоритм AES-256, а під час передавання – протоколи TLS/SSL, що дозволяють протистояти перехопленню інформації у відкритих мережах.

Кожен запит користувача до сервера супроводжується токеном автентифікації, сформованим за допомогою технології JSON Web Token (JWT).

Це дозволяє уніфікувати обмін даними, водночас зберігаючи можливість ідентифікації користувача на кожному етапі.

Процес обміну починається з автентифікації користувача: клієнт надсилає на сервер свої облікові дані, які проходять перевірку. У разі успішного підтвердження особи, сервер генерує токен, що містить зашифровану інформацію про користувача та термін дії. Надалі клієнт додає цей токен у заголовки кожного запиту, забезпечуючи безперервну перевірку прав доступу. Сервер, перевіряючи автентичність токена, відповідає відповідними зашифрованими даними.

Для реалізації цього підходу застосовується стек сучасних технологій. На серверній стороні використовується фреймворк Flask у зв'язці з бібліотекою PyJWT. Ця конфігурація дозволяє створити компактну, але ефективну систему автентифікації з мінімальними витратами обчислювальних ресурсів. На клієнтській стороні застосовується мова JavaScript та бібліотека Axios, яка дозволяє легко налаштувати запити до API із додаванням авторизаційних заголовків. У ролі прикладу реалізовано два етапи – отримання токена та надсилання захищеного запиту з цим токеном.

Особливу увагу приділено захисту вмісту запитів, зокрема конфіденційної інформації. Доцільно перед передаванням даних реалізовувати локальне шифрування, використовуючи бібліотеки на зразок Cryptography для Python. В основі лежить алгоритм симетричного шифрування на базі ключа, який може генеруватися й передаватися окремим зашифрованим каналом.

Нижче наведено узагальнену характеристику основних елементів побудованої моделі, представлену у вигляді таблиці 1.5.

Таблиця 1.5 – Ключові компоненти моделі обміну інформацією

Компонент	Призначення
TLS/SSL	Шифрування даних під час передавання через мережу
AES-256	Симетричне шифрування збережених даних
JWT (JSON Web Token)	Формування токенів для автентифікації користувача
Flask + PyJWT (Python)	Обробка запитів, перевірка облікових даних, генерація токенів на сервері
Axios (JavaScript)	Надсилення HTTP-запитів до серверу з токенами автентифікації
Cryptography (Python)	Локальне шифрування/розшифрування повідомлень перед передачею

Розроблена модель інформаційного обміну дозволяє не лише захистити дані від зовнішнього втручання, але й гнучко масштабувати систему, додаючи нові рівні перевірки, механізми аудиту або елементи аналітики. Такий підхід забезпечує відповідність стандартам інформаційної безпеки (зокрема, GDPR та ISO/IEC 27001), а також адаптивність до змін у зовнішньому середовищі загроз. У підсумку модель є надійною основою для побудови корпоративних застосунків із високим рівнем захищеності.

1.4. Постановка задачі

У сучасному цифровому середовищі зростає потреба у забезпеченні надійного захисту корпоративних даних, особливо в умовах активного використання хмарних рішень, мобільного доступу та дистанційної роботи. У зв'язку з цим виникає необхідність створення програмного забезпечення, яке

забезпечує як зберігання конфіденційної інформації, так і її захист на рівні доступу, моніторингу та контролю дій користувачів.

Метою даного програмного продукту є розробка застосунку для захищеного керування корпоративними даними, який дозволяє здійснювати автентифікацію користувачів, зберігати зашифровані відомості та вести аудит усіх дій у системі. Кінцевий результат – компіляція у вигляді виконуваного файлу (main.exe), який реалізує повноцінний інтерфейс користувача для взаємодії з базою даних, що зберігається локально.

Для досягнення поставленої мети потрібно реалізувати такі функціональні можливості:

- Реєстрація та автентифікація користувачів, із використанням хешування паролів (таблиця users);
- Збереження та перегляд корпоративних даних, пов'язаних із конкретним користувачем (таблиця corporate_data);
- Журналювання дій, зокрема запис операцій, що виконуються користувачами, із фіксацією часу (таблиця user_logs);
- Забезпечення конфіденційності інформації, з урахуванням механізмів шифрування та безпечного зберігання облікових даних;
- Мінімалістичний графічний інтерфейс, який дозволяє зручно працювати з обліковими записами, даними та журналами.

Висновок до розділу 1

У першому розділі було здійснено комплексне дослідження сучасних підходів до захисту корпоративних даних у відкритих інформаційних системах. Встановлено, що в умовах динамічного зростання обсягів даних, хмарних обчислень і віддаленої роботи питання конфіденційності, цілісності й

доступності інформації стає критично важливим для будь-якої організації. Визначено, що захист даних має охоплювати як технічні аспекти, пов'язані з криптографією, аутентифікацією та моніторингом, так і організаційні заходи, зокрема політики контролю доступу та моделі довіри.

У підрозділах розглянуто ключові технології шифрування даних, серед яких окрему увагу приділено симетричним та асиметричним алгоритмам, зокрема AES і RSA, що широко використовуються в корпоративних системах. Проаналізовано методи автентифікації, зокрема багатофакторні, біометричні та токен-орієнтовані, а також моделі контролю доступу – RBAC, ABAC та Zero Trust. Також розглянуто важливість логування та моніторингу подій для оперативного виявлення загроз і аналізу інцидентів, що є невід'ємною складовою сучасної стратегії кіберзахисту.

На основі вивчених теоретичних підходів була сформульована концепція інформаційної системи для захисту корпоративних даних. Зокрема, обґрунтовано архітектуру застосунку, що поєднує фронт-енд і бек-енд частини, систему управління доступом, механізми шифрування, інструменти моніторингу та аналізу. Модель обміну інформацією базується на сучасних технологіях API, JWT-токенах, TLS/SSL та AES-шифруванні, що дозволяє гарантувати безпечну взаємодію користувача з системою.

РОЗДІЛ 2. ПРОЄКТУВАННЯ ІНФОРМАЦІЙНОЇ ПІДСИСТЕМИ ЗАХИСТУ ДАНИХ КОРПОРАТИВНИХ СИСТЕМ

Сучасні корпоративні системи зберігають та обробляють великі обсяги конфіденційної інформації, що потребує надійного захисту від несанкціонованого доступу, витоків та модифікації. З розвитком інформаційних технологій значна частина корпоративних процесів переходить у відкриті системи, зокрема у хмарні середовища, що збільшує ризики інформаційної безпеки. Основними загрозами є атаки на аутентифікацію, перехоплення даних, компрометація облікових записів та зовнішнє втручання в систему.

Проектowana інформаційна підсистема покликана забезпечити захист корпоративних даних у відкритих системах шляхом реалізації механізмів безпечного зберігання, контролю доступу та шифрування інформації. Основою підсистеми є веб-додаток, побудований на мікрофреймворку Flask, який забезпечує взаємодію між користувачами та базою даних. Система використовує криптографічний алгоритм шифрування AES (Fernet) для захисту збережених даних, що унеможливорює їх прочитання без відповідного ключа.

Розроблена підсистема включає механізм аутентифікації користувачів, який дозволяє ідентифікувати суб'єктів доступу до корпоративних записів. Користувачі можуть додавати, переглядати та видаляти власні зашифровані дані, що зберігаються у базі даних. Завдяки розподіленій моделі доступу, кожен користувач бачить лише свої записи, а адміністратори мають можливість здійснювати аудит безпеки системи.

Запропоноване рішення відповідає сучасним вимогам безпеки інформаційних систем та може бути використане у корпоративних середовищах для забезпечення конфіденційності та захисту даних від потенційних загроз.

2.1 Загально системні рішення

Сучасні інформаційні системи в корпоративному середовищі зазнають численних загроз, пов'язаних із безпекою збереження, обробки та передачі даних. Захист корпоративної інформації стає критично важливим завданням, оскільки організації обробляють великі обсяги конфіденційної інформації, що може містити комерційні, фінансові та особисті дані. У зв'язку з цим розробка ефективної інформаційної підсистеми захисту даних потребує комплексного підходу та використання передових методів криптографічного захисту, аутентифікації та контролю доступу.

Проектована система має відповідати вимогам інформаційної безпеки, що передбачає забезпечення таких основних принципів:

- Конфіденційність – дані мають бути доступні лише авторизованим користувачам, а їх перегляд третіми особами повинен бути унеможливлений.
- Цілісність – інформація не повинна зазнавати несанкціонованих змін або модифікацій без відповідного дозволу.
- Доступність – користувачі системи повинні мати можливість отримувати доступ до даних відповідно до своїх прав та ролей.

Одним із ключових аспектів захисту корпоративних даних є використання методів криптографічного шифрування, що дозволяє зберігати інформацію у вигляді, непридатному для читання без спеціального дешифрувального ключа. У розробленій інформаційній підсистемі використовується алгоритм AES (Fernet), який гарантує безпечне збереження даних, оскільки навіть у разі компрометації бази даних зломисники не зможуть отримати доступ до вихідної інформації без відповідного ключа.

Система передбачає обов'язкову ідентифікацію та аутентифікацію користувачів перед отриманням доступу до корпоративної інформації. Реєстрація

користувачів здійснюється через веб-інтерфейс із подальшим збереженням захешованих паролів у базі даних. Для аутентифікації використовується захищене з'єднання, що унеможливлює перехоплення облікових даних.

Розроблена система базується на клієнт-серверній архітектурі, що дозволяє забезпечити гнучкість та масштабованість. Серверна частина побудована на основі фреймворку Flask, який забезпечує ефективне оброблення запитів та інтеграцію з базою даних. База даних SQLite використовується як основне сховище для збереження зашифрованих корпоративних записів.

Система підтримує механізм шифрування та дешифрування інформації в реальному часі, що дозволяє користувачам безпечно працювати з даними, не ризикуючи їх компрометацією. Окремий модуль ведення журналу подій дозволяє відстежувати дії користувачів, що підвищує рівень безпеки.

Запропоновані загальносистемні рішення забезпечують комплексний підхід до захисту корпоративних даних, підвищуючи стійкість до потенційних загроз та атак. Використання передових криптографічних методів у поєднанні з механізмами аутентифікації та контролю доступу дозволяє гарантувати надійну конфіденційність і безпеку інформації у відкритих системах.

2.2. Абстрактне представлення структури даних

У процесі розробки інформаційної підсистеми захисту корпоративних даних у відкритих системах важливим етапом є проєктування структури даних. Вона визначає спосіб зберігання, обробки та маніпуляції інформацією, забезпечуючи ефективний доступ до неї та відповідний рівень безпеки.

Розглянута система має модульну архітектуру, що складається з основних сутностей, пов'язаних між собою відносинами. Основними компонентами є користувачі, зашифровані корпоративні дані та журнал дій, які відображають операції, що здійснювалися в системі.

Користувач (User) – основна сутність, яка містить інформацію про користувачів системи. Кожен користувач має унікальний ідентифікатор, ім'я користувача та захешований пароль для безпечної аутентифікації.

Зашифровані дані (CorporateData) – містять інформацію, що зберігається в базі даних у зашифрованому вигляді. Кожен запис прив'язаний до власника (користувача), що забезпечує контроль доступу.

Журнал дій (UserLog) – відстежує активність користувачів, фіксуючи події, такі як вхід у систему, шифрування або видалення даних. Це дозволяє здійснювати аудит безпеки та моніторинг роботи системи.

Для формального представлення структури даних використовується концепція реляційної бази даних, у якій кожна сутність представлена у вигляді окремої таблиці з визначеними атрибутами та зв'язками (табл 2.1 – 2.3)

Таблиця 2.1 - User (Користувачі)

Поле	Тип даних	Опис
id	INTEGER (PK)	Унікальний ідентифікатор користувача
username	TEXT UNIQUE	Унікальне ім'я користувача
password_hash	TEXT	Захешований пароль користувача

Таблиця 2.2 - CorporateData (Зашифровані дані)

Поле	Тип даних	Опис
id	INTEGER (PK)	Унікальний ідентифікатор запису
data	TEXT	Зашифрований вміст
owner_id	INTEGER (FK)	Власник запису (зв'язок із User.id)

Таблиця 2.3 - UserLog (Журнал дій)

Поле	Тип даних	Опис
id	INTEGER (PK)	Унікальний ідентифікатор запису
user_id	INTEGER (FK)	Ідентифікатор користувача (User.id)
action	TEXT	Опис дії (наприклад, "зашифрував дані")
timestamp	DATETIME	Час виконання операції

При реєстрації нового користувача створюється запис у таблиці User, зберігаючи ім'я користувача та хеш пароля. Під час додавання зашифрованих даних користувачем створюється відповідний запис у таблиці CorporateData, прив'язаний до User.id. Усі дії, такі як авторизація, створення чи видалення даних, фіксуються у таблиці UserLog, що дозволяє здійснювати аудит роботи системи.

Браузер бази даних – це зручний інструмент для перегляду, редагування та управління даними. Він дозволяє швидко переглядати структуру таблиць, їхні поля та зв'язки між ними. Також за допомогою браузера можна додавати, змінювати або видаляти записи без написання SQL-запитів.

На зображенні рис.2.1. видно структуру нашої бази даних, що містить три основні таблиці:

- users – для збереження облікових записів користувачів;
- corporate_data – для зберігання зашифрованих корпоративних даних;
- user_logs – журнал дій користувачів.

Цей інструмент допомагає контролювати роботу з базою даних та аналізувати інформацію, що зберігається у системі.

Имя	Тип	Схема
Таблицы (3)		
corporate_data		CREATE TABLE corporate_data (id INTEGER NOT NULL, data TEXT NOT NULL, owner_id INTEGER NOT NULL)
id	INTEGER	"id" INTEGER NOT NULL
data	TEXT	"data" TEXT NOT NULL
owner_id	INTEGER	"owner_id" INTEGER NOT NULL
user_logs		CREATE TABLE user_logs (id INTEGER NOT NULL, user_id INTEGER NOT NULL, action VARCHAR(255) NOT NULL, timestamp DATETIME)
id	INTEGER	"id" INTEGER NOT NULL
user_id	INTEGER	"user_id" INTEGER NOT NULL
action	VARCHAR(255)	"action" VARCHAR(255) NOT NULL
timestamp	DATETIME	"timestamp" DATETIME
users		CREATE TABLE users (id INTEGER NOT NULL, username VARCHAR(50) NOT NULL, password_hash VARCHAR(255) NOT NULL)
id	INTEGER	"id" INTEGER NOT NULL
username	VARCHAR(50)	"username" VARCHAR(50) NOT NULL
password_hash	VARCHAR(255)	"password_hash" VARCHAR(255) NOT NULL
Индексы (0)		
Представления (0)		
Триггеры (0)		

Рисунок 2.1. структура БД в браузері

2.3 Розробка бази даних

Процес розробки бази даних передбачає створення логічної структури для ефективного зберігання та обробки даних, що гарантує високий рівень безпеки корпоративної інформації. Проєктована база даних є реляційною і містить основні сутності, що забезпечують функціональність системи: користувачі, зашифровані корпоративні дані та журнал дій.

Концептуальна модель бази даних розроблена відповідно до вимог безпеки та принципів захисту даних. Використання реляційного підходу дозволяє підтримувати зв'язність між об'єктами та реалізовувати контроль доступу на рівні запитів до бази. Головним елементом системи є користувач, який має унікальні ідентифікатори та облікові дані, що дозволяють йому взаємодіяти з системою. Кожен користувач має можливість додавати зашифровані корпоративні записи, які асоціюються з його обліковим записом.

Окрім основних операцій із шифруванням та розшифруванням інформації, у системі передбачено ведення журналу подій, що дозволяє відстежувати дії кожного користувача. Записи у журналі містять інформацію про авторизацію, додавання, видалення та перегляд корпоративних даних. Таким чином, система

забезпечує не тільки збереження конфіденційної інформації, а й дозволяє проводити аудит безпеки.

При створенні бази даних було обрано технологію **SQLite**, яка відповідає вимогам проєкту завдяки своїй легкості, простоті використання та підтримці транзакцій. Реалізація таблиць здійснюється за допомогою ORM (Object-Relational Mapping) у Flask через SQLAlchemy, що дозволяє ефективно працювати з даними у Python-додатку.

Відповідно до концептуальної моделі було створено три основні таблиці: `users`, `corporate_data` та `user_logs`. Кожна з них має унікальні атрибути та пов'язані між собою через зовнішні ключі.

Загальна структура бази даних представлена на **Рисунку 2.2**.

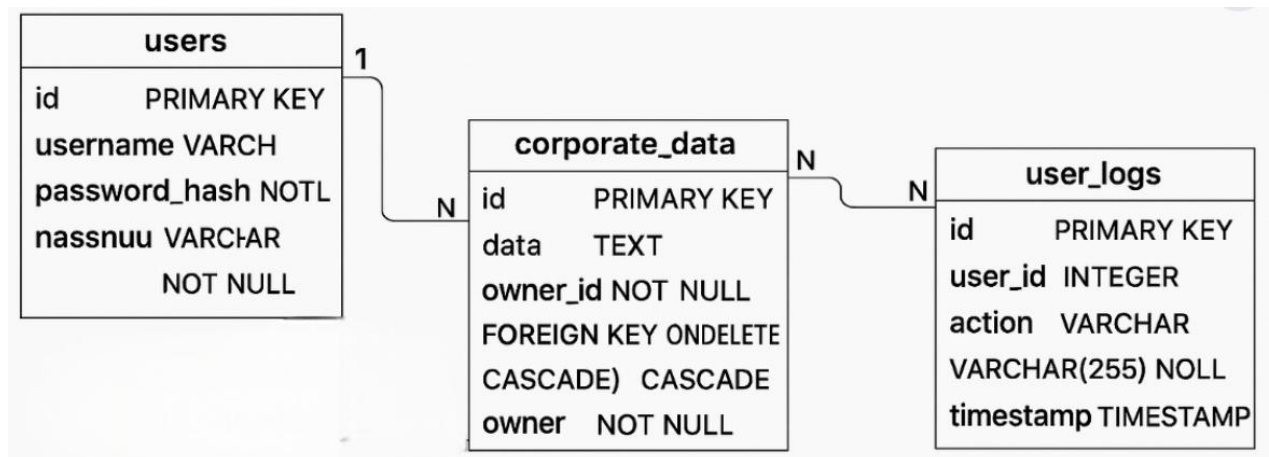


Рисунок 2.2 – Схема бази даних

Реалізація бази даних забезпечує захист корпоративних даних завдяки використанню шифрування перед збереженням, аутентифікації користувачів та веденню історії змін. При додаванні нового запису він одразу шифрується за допомогою алгоритму AES, що гарантує конфіденційність.

Структура бази дозволяє масштабувати систему без зміни основної логіки, додаючи нові функціональні можливості, такі як додаткові рівні доступу або

підтримка розширених методів аутентифікації. Таким чином, розроблена база даних є основою для безпечного збереження корпоративної інформації та забезпечує ефективний контроль доступу у відкритих системах.

2.4 Діаграма послідовності для аналізу дослідження методів захисту даних корпоративних систем та аналіз предметної області

Процес захисту корпоративних даних у відкритих системах включає кілька етапів, що забезпечують конфіденційність, цілісність та доступність інформації. Для візуалізації взаємодії між користувачем та системою застосовується діаграма послідовності (Sequence Diagram), яка відображає основні кроки роботи з системою.

У нашому випадку діаграма послідовності моделює процес автентифікації користувача, шифрування даних та ведення журналу дій рис 2.3. Основні учасники взаємодії включають:

- Користувача – ініціатора взаємодії з системою.
- Сервер (Flask) – обробник запитів користувача.
- Базу даних (SQLite) – сховище зашифрованих даних.
- Криптографічний модуль (Fernet AES) – механізм шифрування та дешифрування.

Приклад діаграми послідовності демонструє, як користувач входить у систему, додає зашифрований запис, переглядає свої дані та як ці дії фіксуються у журналі активності.

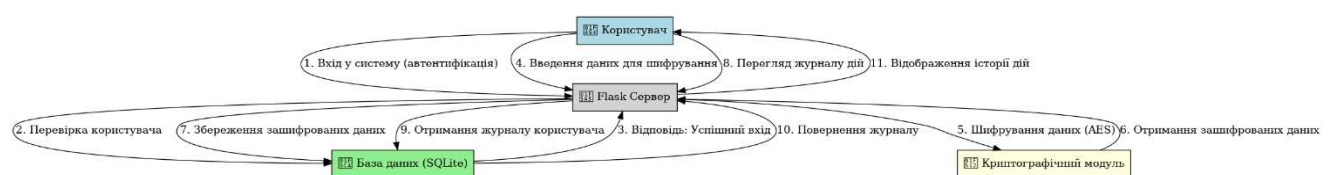


Рисунок 2.3. Діаграма послідовності

Для підтвердження функціональності розробленої системи та аналізу дослідження методів захисту корпоративних даних представлено кілька основних екранів програми. Вони демонструють роботу ключових механізмів: **автентифікацію користувача, управління зашифрованими даними та ведення журналу дій.**

Сторінка входу користувача – процес автентифікації рис 2.4.

Ця сторінка є початковим етапом взаємодії користувача із системою. Вона містить форму входу, де користувач вводить свій логін та пароль. Після успішної автентифікації він отримує доступ до основного функціоналу. Якщо введені дані неправильні, система виводить відповідне повідомлення про помилку рис 2.5.

Захист корпоративних даних у відкритих системах

Реєстрація Вхід

Вхід

Електронна пошта

Пароль

☐ Показати пароль

Увійти

[Зареєструватися як новий користувач](#)

© 2025 Захист корпоративних даних
Безпека інформації та конфіденційність у відкритих системах

Рисунок 2.4. Сторінка входу користувача

Вхід

Невірні дані для входу.

Електронна пошта

Пароль

☐ Показати пароль

Увійти

[Зареєструватися як новий користувач](#)

Рисунок 2.5. Повідомлення про помилку

Після входу користувач потрапляє на **головну сторінку рис 2.6**, де відображається список усіх зашифрованих записів, що належать йому. Таблиця містить такі поля, як **розшифровані дані**, **зашифрований текст** та **кнопка для видалення запису**.

Захист корпоративних даних у відкритих системах

Вихід

Головна

Шифрування даних

Налаштування

Дані успішно зашифровані та збережені!

Ваші зашифровані дані

Дані	Зашифровані дані	Дії
Зашифровані дані	gAAAAABn2zR1hvxxHxbqTBIYdq5cs_7_J3VJ2G50Knqem3CapTYDMZ7thEpxVKtEsXOhZUSnRXj2Lla0Fx6ZMQFN15ZxC5mwPoovjL7x_EIF9o-4EtcY8jE=	Видалити
Тест	gAAAAABn2zSA-KPLmQQyLOYzfQYmTfrO9m-zao9v59bxSoMU_HlrsfMrSJNGHp-9NIwfr8eGaS83wmkSkpHgxeV1589g1KTslg==	Видалити

© 2025 Захист корпоративних даних

Безпека інформації та конфіденційність у відкритих системах

Рисунок 2.6 Головна сторінка

Форма шифрування даних – введення та збереження конфіденційної інформації рис.2.7. На цій сторінці користувач вводить текстові дані, які хоче зашифрувати, після чого система перетворює їх у захищений формат і зберігає в базі даних. Доступ до цих даних можливий лише через автентифікацію та за допомогою вбудованого механізму розшифрування.

The screenshot shows a web application titled "Захист корпоративних даних у відкритих системах" (Protection of corporate data in open systems). The interface includes a sidebar with navigation links: "Головна" (Home), "Шифрування даних" (Data Encryption), and "Налаштування" (Settings). The main content area is titled "Шифрування даних" (Data Encryption) and contains the instruction "Введіть дані для шифрування" (Enter data for encryption). Below this is a large text input field. At the bottom of the input area is a blue button labeled "Зашифрувати та зберегти" (Encrypt and save). The footer of the application contains the copyright notice "© 2025 Захист корпоративних даних" and the tagline "Безпека інформації та конфіденційність у відкритих системах" (Security of information and confidentiality in open systems).

Рисунок 2.7 Форма шифрування даних

Форма зміни пароля дозволяє користувачеві оновити свої облікові дані рис.2.8. Для цього необхідно ввести **старий пароль**, після чого система перевіряє його на відповідність. Якщо перевірка успішна, користувач вводить **новий пароль**, який буде збережений у **захешованому вигляді**.

У розробленій системі реалізовано механізм **шифрування даних перед збереженням у базі**, що забезпечує їх конфіденційність та захист від несанкціонованого доступу. Використовується **алгоритм AES (Fernet)**, який гарантує, що навіть у разі отримання доступу до бази даних сторонніми особами, інформація залишатиметься у зашифрованому вигляді без можливості її розшифрування без відповідного ключа.

Захист корпоративних даних у відкритих системах

Головна

Шифрування даних

Налаштування

Зміна пароля

Поточний пароль

Новий пароль

Підтвердження пароля

Змінити пароль

Рисунок 2.8 Форма зміни пароля

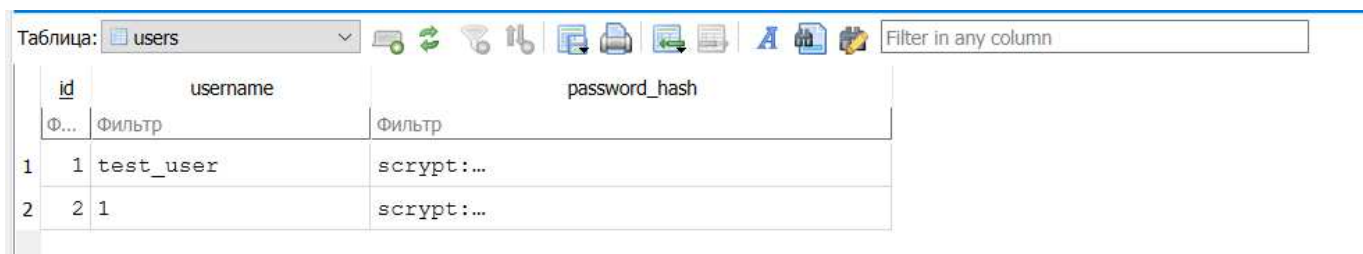
На зображенні 2.9 представлено вміст таблиці `corporate_data`, де видно, що дані збережені у зашифрованому вигляді та не можуть бути прочитані без використання спеціального дешифрувального механізму. Це унеможливило перегляд конфіденційної інформації, навіть якщо база буде скомпрометована.

Таблиця: corporate_data			Filter in any column		
id	data			owner_id	
Ф...	Фильтр			Фильтр	
1	6	gAAAAABn2xLrPMTTeLgYFR2MtTe0brOf7T2gRRGSOnboIER4UgchA57A...			1
2	7	gAAAAABn2xOn0Y__fUXb6-kRE-DvLGo8e4i4qyAOos45bizVQKa-...			1
3	8	gAAAAABn2xPDuM8MG7v6TnmN7bW1Xz40cJjgI1fhbbhg3tA_yfoMdF3m...			1
4	9	gAAAAABn2xPF393F-...			1
5	10	gAAAAABn2xPITzyOIZk_OrM-m5ST-...			1
6	11	gAAAAABn2xPM59ZwFyXScYmCumyPXgE1VJ3Kg6TOgaBduJok4I81V6R0...			1
7	12	gAAAAABn2xQNTLVbx_bcVq_XuGYnzvag0GMrIeOYXemzj2WfkpKj-...			1

Рисунок 2.9. Дані збережені у зашифрованому вигляді

Друге зображення 2.10 демонструє таблицю `users`, де зберігаються облікові записи користувачів. Паролі також не зберігаються у відкритому вигляді, а

проходять через **алгоритм хешування Scrypt**, що забезпечує їх захист від підбору та компрометації. Таким чином, навіть адміністратор бази даних не має доступу до реальних паролів користувачів, що підвищує рівень безпеки системи.



Таблиця: users		
	id	username
	Ф...	Фильтр
1	1	test_user
2	2	1

Рисунок 2.10. Зберігання облікових записів

2.5 Математичне забезпечення розробки

Розробка інформаційної підсистеми захисту корпоративних даних базується на використанні криптографічних алгоритмів та методів захисту інформації. Основним завданням математичного забезпечення є реалізація механізмів **шифрування, хешування та контролю доступу**, що забезпечують конфіденційність, цілісність і захист від несанкціонованого доступу.

Для захисту корпоративних даних використовується **симетричний алгоритм шифрування AES (Advanced Encryption Standard)** у режимі **Fernet**. Цей алгоритм працює на основі **математичних операцій над бітовими блоками фіксованої довжини**.

Формально процес шифрування можна описати так:
Нехай:

- P – відкритий текст (корпоративні дані),
- K – секретний ключ довжиною 32 байти,
- $E_K(P)$ – функція шифрування AES з ключем K ,

- C – зашифрований текст.

Тоді процес шифрування описується рівнянням:

$$C = E_K(P)$$

Розшифрування виконується за допомогою зворотної функції:

$$P = D_K(C)$$

де D_K – функція дешифрування, яка застосовується до зашифрованого тексту з використанням того ж ключа K .

Для збереження паролів використовується алгоритм **Scrypt**, який належить до категорії криптографічних хеш-функцій та ґрунтується на обчислювально складних операціях, що ускладнюють атаку методом перебору.

Хешування паролів виконується за формулою:

$$H = \text{Scrypt}(\text{password}, \text{salt}, N, r, p)$$

де:

- password – вхідний пароль користувача,
- salt – випадкове значення, що додається для запобігання однаковим хешам для однакових паролів,
- N, r, p – параметри алгоритму, що впливають на складність обчислень,
- H – отриманий хеш, який зберігається у базі даних.

Цей метод дозволяє зменшити ризик атак типу "brute force" та "rainbow table", оскільки кожен пароль має унікальний хеш.

Контроль доступу базується на системі **ідентифікації та аутентифікації користувачів**, де кожен користувач має унікальний ідентифікатор та рівень доступу. Дії користувачів фіксуються у **журналі логів**, що реалізовано через математичну функцію часової мітки:

$$L = (U, A, T)$$

де:

- U – користувач, який виконав дію,
- A – тип дії (вхід, шифрування, видалення даних тощо),
- T – час виконання дії.

Ця модель дозволяє здійснювати аудит безпеки та виявляти потенційні загрози.

Математичне забезпечення розробленої системи ґрунтується на **криптографічних алгоритмах AES та Scrypt**, що гарантують високий рівень захисту даних. Також використання **моделі логування дій** дозволяє відстежувати активність користувачів та контролювати можливі загрози безпеці. Запропоновані математичні методи забезпечують надійність, стійкість до атак та безпеку інформаційної підсистеми.

Висновок до розділу 2

У другому розділі було розглянуто процес проектування інформаційної підсистеми для захисту корпоративних даних у відкритих системах. Було проведено аналіз предметної області, визначено ключові вимоги до бази даних та реалізовано її структуру, що дозволяє ефективно керувати зашифрованими записами та контролювати доступ користувачів.

Розроблена система базується на реляційній моделі даних, що включає три основні таблиці:

- Users – для збереження облікових записів користувачів та їхніх паролів у захищеному вигляді.
- CorporateData – для зберігання конфіденційних даних, зашифрованих за допомогою AES (Fernet).
- UserLog – для ведення журналу активності користувачів, що дозволяє здійснювати аудит безпеки.

Було реалізовано механізми автентифікації, шифрування та логування дій користувачів, що забезпечує конфіденційність, цілісність та захист від несанкціонованого доступу.

Окрім теоретичної моделі, було розроблено графічний інтерфейс, що включає:

- Сторінку входу – для авторизації користувачів.
- Головну сторінку – для перегляду зашифрованих записів.
- Форму шифрування – для введення та збереження даних у захищеному вигляді.
- Журнал дій – для моніторингу активності користувачів.
- Форму зміни пароля – для безпечного оновлення облікових даних.

Математичне забезпечення системи включає використання криптографічних алгоритмів AES (Fernet) для шифрування даних та Scrypt для хешування паролів, що гарантує їх захист від атак.

Загалом, у цьому розділі було розроблено концептуальну модель системи, реалізовано базу даних та алгоритми захисту інформації, що є основою для подальшого впровадження та тестування програмного забезпечення.

РОЗДІЛ 3. РОЗРОБКА ІНФОРМАЦІЙНОЇ ПІДСИСТЕМИ ЗАХИСТУ ДАНИХ КОРПОРАТИВНИХ СИСТЕМ

3.1. Діаграма розгортання

У процесі створення інформаційної підсистеми захисту корпоративних даних важливим етапом є побудова діаграми розгортання. Вона відображає фізичну структуру системи, її основні пристрої, логічні компоненти та зв'язки між ними. Таке графічне подання дозволяє не лише узагальнити архітектуру рішення, а й проаналізувати особливості його реалізації з погляду безпеки, масштабованості та доступності.

Система побудована на основі клієнт-серверної моделі з додатковим використанням хмарних сервісів і спеціалізованого моніторингового обладнання. Центральною ланкою у взаємодії виступає сервер застосунку, на якому реалізовано основну логіку автентифікації користувачів, розмежування доступу та шифрування інформації. Усі запити, що надходять від клієнтів, обробляються саме цим сервером, після чого відбувається звернення до бази корпоративних даних або до хмарного сховища, якщо йдеться про резервне копіювання.

На стороні користувача розміщується клієнтський комп'ютер із встановленим застосунком, що забезпечує інтерфейс для взаємодії із системою. Всі звернення до сервера здійснюються через захищений канал з використанням протоколу HTTPS та прикладного інтерфейсу API. Таким чином гарантується захищеність переданої інформації навіть у відкритих мережах.

База даних корпоративної системи функціонує на окремому сервері, з яким взаємодія організована через захищене SQL-з'єднання з використанням TLS. Це дозволяє не тільки розмежувати обчислювальні ресурси, а й створити додатковий рівень захисту інформації завдяки фізичній ізоляції серверів.

Задля забезпечення надійного зберігання резервних копій у разі втрати доступу до локальної інфраструктури або виникнення аварійної ситуації

передбачено підключення до хмарного сховища. Взаємодія з ним реалізується за допомогою API із застосуванням TLS-шифрування. Перед передачею дані додатково обробляються модулем шифрування, що інтегрований у сервер застосунку, завдяки чому зберігається високий рівень конфіденційності навіть у хмарному середовищі.

Моніторинг роботи системи реалізується через окремий сервер, на якому встановлено SIEM-рішення. Сервер моніторингу приймає лог-файли із сервера застосунку, бази даних та хмарної інфраструктури, обробляє їх за допомогою аналітичних алгоритмів та інформує адміністратора у разі виявлення підозрілих дій або аномалій. У системі застосовано метод прямої пересилки журналів (Log Forwarding), що дає змогу передавати дані в реальному часі з мінімальними затримками. Аналітична підсистема побудована з урахуванням здатності до виявлення нетипової поведінки, що дозволяє реагувати на загрози ще до того, як вони призведуть до серйозних наслідків.

На рисунку 3.1 наведено діаграму розгортання розробленої інформаційної системи. У центрі зображено сервер застосунку, до якого підключено як клієнтську частину, так і сервер бази даних. Усі обміни між цими компонентами відбуваються за зашифрованими протоколами. Також зображено взаємодію з хмарним сховищем, у межах якого відбувається резервне копіювання за допомогою відповідного компонента. Праворуч на діаграмі розміщено сервер моніторингу, який приймає журнали подій із різних джерел і аналізує їх за допомогою вбудованої системи SIEM. Компоненти системи згруповані відповідно до їхнього розміщення: на клієнтському комп'ютері, сервері застосунку, сервері бази даних, у хмарному середовищі та на сервері моніторингу. Кожне логічне з'єднання підписано відповідним протоколом або типом обміну, що забезпечує прозорість і зрозумілість загальної архітектури.

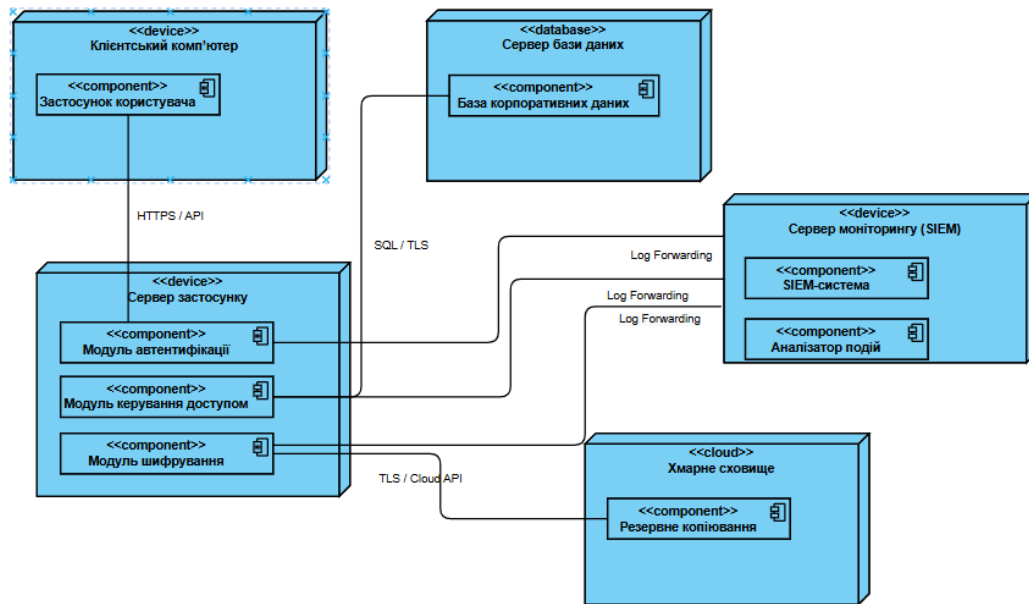


Рисунок 3.1 – Діаграма розгортання інформаційної підсистеми захисту корпоративних даних

Загалом представлена діаграма демонструє структуровану, багаторівневу архітектуру, що відповідає сучасним принципам побудови безпечних ІТ-систем. Розподіл ролей між компонентами, використання незалежних каналів зв'язку та впровадження засобів моніторингу дозволяють не лише ефективно захищати корпоративну інформацію, а й своєчасно виявляти загрози та реагувати на них. Такий підхід відповідає вимогам щодо створення надійних інформаційних систем для організацій, діяльність яких пов'язана з обробкою чутливих даних.

3.2 Технічні вимоги до системи

Технічні вимоги до інформаційної підсистеми захисту корпоративних даних є ключовим етапом її проєктування та реалізації. Від правильності їх формування залежить не лише функціональна спроможність системи, а й її стійкість до загроз, масштабованість, продуктивність, надійність і зручність

використання. Усі вимоги поділяються на функціональні, які визначають очікувану поведінку системи, та нефункціональні, що встановлюють обмеження й характеристики, пов'язані з експлуатацією.

Функціональні вимоги передбачають підтримку автентифікації користувачів із можливістю багатофакторної перевірки, що може включати пароль, токен, біометричні дані або інші чинники. Система має забезпечувати динамічне управління ролями, надання та скасування доступу до ресурсів відповідно до політик організації. Також необхідна підтримка шифрування як у процесі зберігання даних, так і під час їх передачі між компонентами системи. Очікується, що взаємодія із хмарними сервісами відбуватиметься через захищені інтерфейси з обов'язковою авторизацією. Вбудовані механізми моніторингу мають забезпечувати виявлення підозрілої активності та автоматичне повідомлення адміністратора. Усі ці елементи мають бути логічно об'єднані в єдину систему, що працює безперебійно у реальному часі.

Що стосується нефункціональних вимог, особливу увагу слід приділити надійності та безвідмовності роботи, особливо з огляду на критичність корпоративної інформації. Підсистема має забезпечувати відновлення після збоїв, зокрема через створення резервних копій і автоматичну реплікацію. Висока продуктивність є необхідною умовою для збереження швидкості обробки запитів незалежно від кількості одночасних користувачів. Сумісність з операційними системами Windows та Linux є бажаною, оскільки дозволяє розгортати рішення в гетерогенному середовищі. Безпека інформації повинна гарантуватись через дотримання стандартів шифрування, ізоляцію середовищ, захист API та ведення логів.

Для ефективного управління розвитком системи всі вимоги до апаратного забезпечення, програмного середовища та мережевої інфраструктури зведено у таблицю 3.1. Вона дозволяє систематизувати технічні характеристики відповідно до функціонального призначення кожного компонента.

Таблиця 3.1 – Технічні вимоги до інформаційної підсистеми захисту
корпоративних даних

Компонент системи	Апаратні вимоги	Програмні вимоги	Мережеві вимоги
Клієнтський комп'ютер	Процесор ≥ 2 ядра, 4 ГБ RAM, SSD ≥ 64 ГБ	ОС Windows 10/11, веббраузер із підтримкою HTTPS	Інтернет-з'єднання ≥ 10 Мбіт/с
Сервер застосунку	4 ядра, 16 ГБ RAM, SSD ≥ 256 ГБ	ОС Ubuntu Server, Python 3.10+, Django, Gunicorn	Підтримка TLS 1.2+, відкр. порти 443, 80
Сервер бази даних	4 ядра, 32 ГБ RAM, SSD ≥ 512 ГБ	PostgreSQL 14+, реплікація та резервне копіювання	Внутрішнє з'єднання з сервером застосунку
Хмарне сховище	Необмежене сховище, георезервування	Підтримка Cloud API (AWS, Azure, Google), TLS 1.3	VPN або TLS-з'єднання з сервером
Сервер моніторингу (SIEM)	8 ядер, 64 ГБ RAM, SSD ≥ 1 ТБ	SIEM-система (наприклад, Wazuh, Splunk), Elasticsearch	Пряме з'єднання із серверами, Log Forwarding
Адміністративна консоль	Будь-який ПК зі стабільним інтернетом	Вебінтерфейс, інтеграція з сервером моніторингу	HTTPS-доступ до внутрішньої мережі

Апаратні ресурси мають забезпечувати безперебійну роботу всіх компонентів навіть у пікові навантаження. Наприклад, сервер моніторингу повинен мати достатньо оперативної пам'яті та накопичувачів для зберігання великих обсягів логів і виконання аналітичних операцій. Сервер бази даних, у свою чергу, має бути оптимізований під виконання запитів великої кількості користувачів, що одночасно працюють із різними сегментами інформації. Для

хмарної частини важливо, щоб провайдер підтримував стандарти ISO/IEC 27001, а також функції автоматичного масштабування, які дозволяють адаптуватися до зростання обсягів даних.

З боку програмного забезпечення, система має базуватися на сучасних і стабільних технологіях з активною підтримкою спільноти або постачальника. Наприклад, використання фреймворку Django у поєднанні з Gunicorn дозволяє забезпечити гнучкість, безпеку та розширюваність серверної частини. Застосування PostgreSQL як основи для бази даних гарантує масштабованість і підтримку складних транзакцій, що особливо актуально для корпоративного середовища. SIEM-сервер із аналітичним модулем дозволяє не лише збирати події, а й корелювати їх у реальному часі, завдяки чому вдається виявити складні атаки.

Мережеві вимоги передбачають підтримку сучасних протоколів захищеного з'єднання, включаючи HTTPS, TLS 1.3 і внутрішні API із перевіркою автентичності. Усі внутрішні з'єднання повинні бути ізольованими від публічних каналів шляхом використання VPN або приватних VLAN. Також важливо забезпечити фільтрацію трафіку, використання міжмережевих екранів, а також інструментів контролю доступу на рівні мережі.

Узагальнюючи, технічні вимоги до підсистеми захисту корпоративних даних мають на меті не лише визначити базові характеристики, але й задати орієнтир для розгортання, тестування та подальшої експлуатації системи. Врахування вимог на ранньому етапі дозволяє уникнути неузгодженостей при реалізації, зменшити витрати на адаптацію та забезпечити високий рівень безпеки корпоративного середовища.

3.3 Програмні вимоги до системи

У процесі розробки інформаційної підсистеми захисту корпоративних даних програмні вимоги відіграють визначальну роль, оскільки саме вони задають рамки вибору мов програмування, фреймворків, бібліотек, операційних систем і служб, що формують єдине функціональне середовище. Головним завданням при визначенні програмних вимог є забезпечення надійності, сумісності, масштабованості та підтримки сучасних стандартів безпеки, які є критично важливими для обробки конфіденційної інформації у корпоративному середовищі.

Програмне забезпечення системи охоплює серверну, клієнтську, мережеву та допоміжну складові, кожна з яких виконує свої функції в межах розгортання системи. Серверна частина є ядром логіки застосунку, забезпечує автентифікацію, контроль доступу, шифрування, взаємодію з базами даних та інтеграцію з зовнішніми API. Вона повинна реалізовуватись за допомогою мов програмування високого рівня, таких як Python, що забезпечує ефективність розробки та активну підтримку сучасних засобів безпеки. Фреймворк Django, що побудований на архітектурі MVC, дає можливість швидко створити масштабований сервер із чітким розділенням функцій.

Клієнтська частина включає застосунок користувача, який може бути реалізований як десктопна, мобільна або вебверсія. Основною вимогою до неї є підтримка захищеної взаємодії з сервером через HTTPS-протокол, відображення візуального інтерфейсу та забезпечення автентифікації користувача. Реалізація фронтенду може здійснюватися з використанням фреймворків React, Vue або Angular, що дозволяє створити адаптивний інтерфейс з високим рівнем інтерактивності. Мобільна версія може реалізовуватись за допомогою Flutter або React Native, що дозволяє одночасно підтримувати Android і iOS.

Особливої уваги потребують вимоги до програмного забезпечення, пов'язаного з обробкою логів та моніторингом. У системі передбачається використання SIEM-серверу з вбудованими модулями обробки подій безпеки. Доцільно застосовувати платформу Wazuh або Splunk, яка підтримує розподілену обробку даних і дозволяє будувати зв'язки між подіями, формуючи повну картину безпекової ситуації. У випадку аналітики, спрямованої на виявлення аномалій, слід включити бібліотеки машинного навчання, такі як Scikit-learn або PyTorch, які можуть бути інтегровані до окремого модуля аналітики на сервері.

Інфраструктурне забезпечення вимагає наявності систем віртуалізації або контейнеризації. Зокрема, передбачено використання Docker для ізоляції сервісів, а також інструментів CI/CD на основі GitHub Actions або GitLab CI, що дозволяє забезпечити контроль за змінами коду, автоматизоване тестування й розгортання. Система має підтримувати інтеграцію з хмарними сервісами, зокрема AWS або Azure, для забезпечення резервного копіювання та масштабування. Також необхідною є підтримка REST API з чітко визначеним форматом обміну даними (JSON або XML), що дозволяє інтегрувати зовнішні системи.

Для повнішого представлення вимог усі ключові елементи програмного середовища наведено у таблиці 3.2. Це дозволяє систематизувати інформацію щодо кожного модуля системи та визначити їхні залежності.

Таким чином, сформовані програмні вимоги забезпечують комплексний підхід до реалізації системи, де кожен компонент має чітко окреслену роль, технічні залежності та стандарти взаємодії. Особливе значення мають сумісність та стандартизація, оскільки вони дають змогу розширювати систему в майбутньому без необхідності повної перебудови її архітектури. Також варто зазначити, що при впровадженні таких вимог значно підвищується безпекова стійкість та продуктивність системи, що робить її придатною до роботи в умовах

підвищених ризиків та динамічного середовища корпоративної інформаційної інфраструктури.

Таблиця 3.2 – Програмні вимоги до підсистеми захисту корпоративних даних

Компонент системи	Програмне середовище	Опис функціональності та залежностей
Серверна частина	Python 3.10+, Django, Gunicorn	Реалізація бізнес-логіки, маршрутизації, контролю доступу
База даних	PostgreSQL 14+, pgAdmin, SQLAlchemy	Зберігання користувачів, політик, журналів доступу
Модуль автентифікації	Django REST, JWT, OAuth2	Підтримка MFA, генерація токенів, контроль сесій
Модуль шифрування	OpenSSL, Cryptography (Python)	Шифрування даних AES-256, TLS, генерація ключів
Модуль логування	Wazuh, Logstash, Elasticsearch	Збір подій, аналіз аномалій, індексація логів
Інтерфейс користувача	React / Angular / Vue	Вебінтерфейс доступу до функцій системи
Мобільний додаток	Flutter / React Native	Адаптивність, доступ до функцій через API
Система контейнеризації	Docker, Docker Compose	Ізоляція сервісів, гнучке розгортання
CI/CD	GitHub Actions / GitLab CI	Автоматизація тестування, оновлень, доставки коду
Хмарні сервіси	AWS S3 / Azure Blob Storage	Резервне копіювання, масштабоване зберігання
API	REST, JSON, TLS	Безпечний обмін між модулями та зовнішніми системами

Висновок до розділу 3

У межах третього розділу було здійснено послідовне формування основних підходів до розробки інформаційної підсистеми захисту корпоративних даних, яка відповідає сучасним вимогам щодо безпеки, масштабованості та функціональної повноти. В результаті опрацювання архітектури системи побудовано діаграму розгортання, що дозволяє візуалізувати логіку взаємодії між ключовими компонентами: клієнтським застосунком, сервером застосунку, сервером бази даних, хмарним сховищем і сервером моніторингу. У кожному блоці чітко виділено функціональні модулі, такі як автентифікація, управління доступом, шифрування, резервне копіювання, аналітика подій тощо. Структура взаємодії відображає логіку розмежування обов'язків між рівнями системи та демонструє підтримку стандартів захищеної комунікації, включаючи HTTPS, TLS, SQL API та Log Forwarding.

Подальший аналіз технічних вимог дозволив встановити апаратні передумови, необхідні для стабільної роботи системи. Було визначено оптимальні параметри для серверної та клієнтської частин, засоби захищеної передачі даних, наявність засобів віддаленого керування, можливість масштабування та відповідність архітектури обраним сценаріям експлуатації. Особлива увага була приділена тому, щоб системні вимоги залишались реалістичними для впровадження в умовах малого або середнього підприємства, водночас забезпечуючи достатній рівень продуктивності та безпеки.

Програмні вимоги, які було сформульовано у наступному підрозділі, охоплюють усе програмне середовище, необхідне для функціонування підсистеми. Це включає вибір мов програмування, фреймворків, баз даних, інструментів обробки журналів, криптографічних бібліотек, модулів машинного навчання та інструментів віртуалізації. Застосування таких засобів, як Python, Django, PostgreSQL, React, Docker, Wazuh і AWS, забезпечує відповідність

проєкту сучасним інженерним підходам та спрощує підтримку, супровід і подальший розвиток системи.

Отже, на основі розробленої архітектури, визначених технічних і програмних вимог було створено ґрунтовну основу для подальшої реалізації підсистеми, що дозволяє забезпечити надійний захист корпоративної інформації в умовах зростаючих загроз. Результати цього розділу безпосередньо лягають в основу практичного впровадження рішень у наступному етапі роботи.

РОЗДІЛ 4. ТЕХНІКО - ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ РОЗРОБКИ

4.1 Загальна характеристика роботи

Розробка інформаційної підсистеми захисту корпоративних даних є відповіддю на сучасні виклики цифрової безпеки, зумовлені зростаючою кількістю кіберзагроз, підвищеними вимогами до конфіденційності інформації та нормативним тиском з боку міжнародних і локальних стандартів. В умовах цифрової трансформації підприємств і активного використання віддалених технологій значення захисту даних значно зросло. Внаслідок цього компанії потребують гнучких, надійних і ефективних програмних рішень, здатних забезпечити як захист внутрішніх ресурсів, так і безпечну взаємодію з зовнішніми користувачами, контрагентами чи сервісами.

Розроблена в межах даного проєкту система має на меті комплексне забезпечення інформаційної безпеки корпоративного середовища. До складу проєкту входять засоби багаторівневої автентифікації, управління ролями та доступами, моніторинг системної активності, зберігання журналів дій, шифрування інформації при передачі та зберіганні, механізми резервного копіювання, а також аналітичні модулі, здатні виявляти загрози в реальному часі.

З огляду на потреби компаній різних масштабів, система була спроектована із урахуванням гнучкості у розгортанні. Її можна реалізувати як у хмарному середовищі, так і локально, а також комбіновано, зберігаючи високий рівень керованості та відповідності політикам безпеки. У процесі проєктування враховано архітектурні особливості масштабованих систем: сервери баз даних, API-зв'язки, розподілену логіку перевірки запитів та централізовану систему моніторингу подій безпеки. Це дозволяє ефективно інтегрувати систему в існуючі корпоративні інфраструктури, мінімізуючи витрати на адаптацію та обслуговування.

На етапі створення системи значна увага приділялася не лише функціональності, але й питанню економічної доцільності. Враховано оптимальне використання ресурсів, вибір ліцензійного чи вільного програмного забезпечення, а також технічні параметри серверів і робочих станцій. Завдяки цьому забезпечується баланс між якістю захисту й витратами на реалізацію проєкту.

Окремо варто зазначити, що до розробки були залучені сучасні підходи до програмування та організації архітектури систем – використання REST API, асинхронної обробки запитів, контейнеризації за допомогою Docker, автоматизації збору логів через Elasticsearch/Logstash, а також використання бібліотек машинного навчання для виявлення аномалій у поведінці користувачів. Це дозволяє реалізувати систему, яка не лише відповідає сьогоднішнім вимогам, але й здатна адаптуватися до майбутніх викликів.

Розроблена підсистема також відповідає нормативно-правовим вимогам щодо захисту інформації, таким як загальний регламент захисту персональних даних (GDPR), стандарт ISO/IEC 27001, рекомендації OWASP тощо. Це розширює можливості її впровадження на міжнародному рівні та підвищує рівень довіри до організації, яка використовує відповідне програмне рішення.

Важливо підкреслити, що реалізація подібної системи не лише зменшує вірогідність витоку інформації чи зупинки критичних сервісів, але й позитивно впливає на бізнес-показники компанії. Впровадження безпечного середовища підвищує ефективність співробітників, спрощує аудит, знижує ризики порушення комерційної таємниці, підвищує конкурентоспроможність та покращує репутацію компанії перед партнерами та клієнтами.

4.2 Розрахунок витрат на проектування та впровадження системи

Для обґрунтування економічної доцільності створення інформаційної підсистеми захисту корпоративних даних необхідно здійснити розрахунок витрат, пов'язаних з усіма основними етапами її життєвого циклу: проектуванням, реалізацією, тестуванням, впровадженням і супроводом.

Загальні витрати на розробку системи можна розрахувати за формулою:

$$C_{\text{заг}} = C_{\text{пр}} + C_{\text{розр}} + C_{\text{тест}} + C_{\text{впров}} + C_{\text{супр}}$$

Де:

$C_{\text{пр}}$ – витрати на проектування,

$C_{\text{розр}}$ – витрати на розробку,

$C_{\text{тест}}$ – витрати на тестування,

$C_{\text{впров}}$ – витрати на впровадження,

$C_{\text{супр}}$ – витрати на супровід.

Витрати на проектування ($C_{\text{пр}}$) включають оплату праці фахівців з аналізу вимог, архітекторів системи, дизайнерів інтерфейсу. Орієнтовно такі роботи оцінюються у 80 годин при середній ставці 300 грн/год. Тоді:

$$C_{\text{пр}} = 80 * 300 = 24000 \text{грн.}$$

Витрати на розробку ($C_{\text{розр}}$) охоплюють написання коду, реалізацію архітектури, інтеграцію модулів. Загальна тривалість етапу – 180 годин, середня ставка розробника – 350 грн/год:

$$C_{\text{розр}} = 180 * 350 = 63000 \text{грн.}$$

Тестування системи ($C_{\text{тест}}$) включає функціональне, безпекове та навантажувальне тестування. Передбачено 60 годин роботи з оплатою 280 грн/год:

$$C_{\text{тест}} = 60 * 280 = 16800 \text{грн.}$$

Впровадження (**Свпров**) охоплює налаштування серверів, розгортання системи, підготовку користувачів. Витрати включають 40 годин технічної роботи (290 грн/год) і 20 годин навчання персоналу (250 грн/год):

$$C_{\text{впров}} = (40 * 290) + (20 * 250) = 11600 + 5000 = 16600 \text{грн.}$$

Супровід системи (**Ссупр**) розраховується на 3 місяці після впровадження з інтенсивністю 20 год/міс. при ставці 300 грн/год:

$$C_{\text{супр}} = 3 * 20 * 300 = 18000 \text{грн.}$$

Підставимо всі значення у загальну формулу:

$$C_{\text{заг}} = 24000 + 63000 + 16800 + 16600 + 18000 = 138400 \text{грн.}$$

Отже, загальні витрати на створення, впровадження і підтримку підсистеми захисту корпоративних даних становлять 138 400 грн. Ця сума є обґрунтованою з урахуванням масштабів системи, її функціонального наповнення, використання сучасних технологій, а також витрат на супровід протягом гарантійного періоду.

Всі витрати зведено у таблиці 4.1:

№	Стаття витрат	Години	Ставка, грн/год	Вартість, грн
1	Проектування	80	300	24 000
2	Розробка	180	350	63 000
3	Тестування	60	280	16 800
4	Впровадження (тех. роботи)	40	290	11 600
5	Впровадження (навчання персоналу)	20	250	5 000
6	Супровід (на 3 міс.)	60	300	18 000
	Разом			138 400

4.2.1 Техніко–економічний аналіз

Техніко–економічний аналіз дозволяє оцінити доцільність проектування та впровадження інформаційної підсистеми захисту даних у корпоративному середовищі. Основним критерієм ефективності в даному випадку є не лише

прямий економічний прибуток, а й зниження потенційних збитків від кіберзагроз, мінімізація ризиків витоку конфіденційної інформації та забезпечення відповідності міжнародним стандартам інформаційної безпеки.

Запровадження системи дозволяє уникнути або суттєво зменшити втрати, пов'язані з інцидентами безпеки, які можуть виникати через несанкціонований доступ, зловмисні дії з боку працівників або зовнішніх атак. За даними аналітичних центрів, середня сума збитків для українського бізнесу через інциденти кібербезпеки становить близько 250 000 грн на рік для середньої компанії. Якщо система захисту дозволить попередити хоча б половину таких інцидентів, то економічний ефект становитиме близько 125 000 грн щорічно.

Окрім цього, реалізація підсистеми дозволяє оптимізувати адміністративні процеси, пов'язані з моніторингом доступу, аудиторією дій користувачів, резервним копіюванням і реагуванням на інциденти. Це знижує навантаження на персонал служби безпеки та ІТ-відділу, даючи змогу скоротити витрати на ручне втручання, доопрацювання та ліквідацію наслідків порушень.

Період окупності проєкту можна визначити за формулою:

$$T = \frac{C_{\text{заг}}}{E_{\text{річн}}}$$

де

$C_{\text{заг}}$ — загальні витрати на впровадження системи (138 400 грн),
 $E_{\text{річн}}$ — річний економічний ефект (125 000 грн).

$$T = \frac{138400}{125000} = 1.11 \text{ року}$$

Отже, система повністю окупить себе менш ніж за півтора року експлуатації, після чого почне генерувати чисту економію для підприємства. Оскільки її обслуговування потребує мінімальних витрат у порівнянні з можливими втратами від порушень безпеки, її впровадження є доцільним як із технічної, так і з фінансової точки зору.

На додаток до економічного ефекту, варто відзначити і нематеріальні переваги: підвищення довіри клієнтів і партнерів, відповідність вимогам сертифікації та стандартам захисту інформації (зокрема, ISO/IEC 27001), а також зміцнення репутації компанії як надійного та безпечного суб'єкта господарювання.

4.2.2 Вартісний аналіз

Вартісний аналіз передбачає деталізовану оцінку фінансових витрат, пов'язаних із проектуванням, розробкою, впровадженням і підтримкою інформаційної підсистеми захисту корпоративних даних. Його метою є обґрунтування доцільності інвестицій у систему з позиції сукупної вартості володіння (ТСО – Total Cost of Ownership) та очікуваних вигод від впровадження.

Загальна вартість розробки системи вже була розрахована в попередньому підрозділі й становить 138 400 грн. Ця сума охоплює оплату праці фахівців (програміста, тестувальника, аналітика), амортизаційні витрати, витрати на енергоносії, а також непередбачені витрати, які потенційно можуть виникати на етапі інтеграції.

Для комплексного аналізу розглянемо структуру витрат у довгостроковій перспективі – на 3 роки експлуатації системи. До одноразових витрат належить етап створення та впровадження (138 400 грн), а до поточних – витрати на супровід, оновлення, резервне копіювання, навчання персоналу та технічну

підтримку. Орієнтовно ці витрати становлять близько 20 000 грн на рік, що включає як оплату праці спеціаліста з супроводу, так і витрати на резервне хмарне сховище.

Таким чином, сумарна вартість володіння системою за 3 роки експлуатації складе:

$$ТСО = C_{\text{розробка}} + 3 * C_{\text{експлуатація}} = 138400 + 3 * 20000 = 198400 \text{ грн.}$$

Для оцінки ефективності витрат використаємо показник **вартісної ефективності**, який розраховується як відношення економічного ефекту до повної вартості володіння:

$$K_{\text{еф}} = \frac{E_{\text{економічний}}}{ТСО} = \frac{375000}{198400} = 1,89$$

Отже, на кожную гривню витрат система забезпечує майже 1,9 гривні повернення у вигляді економічного ефекту. Це свідчить про високу рентабельність проєкту навіть за консервативних розрахунків.

Крім того, варто врахувати альтернативну вартість – у разі відсутності такої системи організація змушена буде або компенсувати втрати, спричинені витоками, або витрачати ресурси на постфактум-реагування. Також важливими чинниками є витрати на штрафи у випадку невідповідності регуляторним вимогам, зниження лояльності клієнтів та інші репутаційні ризики, що важко виражаються у конкретних сумах, але суттєво впливають на стабільність бізнесу.

Вартісний аналіз демонструє, що розробка інформаційної підсистеми не є затратною в довгостроковій перспективі, а навпаки – дозволяє створити ефективний механізм управління ризиками з помірними щорічними витратами. Це дає змогу не лише захистити інформаційні ресурси підприємства, а й

сформувати конкурентну перевагу завдяки підвищеній довірі клієнтів та партнерів.

4.3 Розрахунок економічної ефективності розробки і впровадження системи

Оцінювання економічної ефективності проєкту впровадження інформаційної підсистеми захисту корпоративних даних базується на порівнянні витрат на її розробку з очікуваними вигодами, які вона приносить у процесі експлуатації. До таких вигод належать зниження втрат від інцидентів інформаційної безпеки, підвищення продуктивності праці, зменшення витрат на ручні перевірки та аудит, а також забезпечення відповідності законодавчим вимогам.

Насамперед визначимо загальний економічний ефект, який утворюється завдяки зниженню імовірності витоків конфіденційної інформації, зменшенню часу простою внаслідок атак, оптимізації обробки доступу та централізації адміністрування. На основі експертної оцінки, щорічна економія коштів може становити орієнтовно 125 000 грн. За 3 роки експлуатації вона досягне:

$$E_{\text{загальний}} = 125000 * 3 = 375000 \text{грн.}$$

При цьому повна вартість володіння системою за три роки (враховуючи витрати на розробку та супровід) дорівнює:

$$TCO = 138400 + 3 * 20000 = 198400 \text{грн.}$$

Для визначення **чистого прибутку** від упровадження обчислимо різницю між економічним ефектом і сукупними витратами:

$$P_{\text{чистий}} = E_{\text{загальний}} - TCO = 375000 - 198400 = 176600 \text{ грн.}$$

Наступним показником є **період окупності**, що визначає час, за який проєкт повністю компенсує витрати:

$$T_{\text{окупн}} = \frac{TCO}{E_{\text{річний}}} = \frac{198400}{125000} = 1,59 \text{ року}$$

Таким чином, проєкт повністю окупається менш ніж за 2 роки, що є дуже позитивним показником для ІТ-рішення такого масштабу.

Ще одним важливим індикатором є коефіцієнт економічної ефективності, який розраховується як відношення чистого прибутку до повної вартості володіння:

$$K_{\text{еф}} = \frac{P_{\text{чистий}}}{TCO} = \frac{176600}{198400} = 0,89$$

Значення, близьке до одиниці, свідчить про доцільність інвестицій навіть у короткостроковій перспективі, не кажучи вже про довгострокову вигоду.

Варто також врахувати так звані **непрямі економічні вигоди**, що виникають унаслідок покращення внутрішніх бізнес-процесів, підвищення лояльності клієнтів, уникнення штрафів від регуляторів та спрощення сертифікації підприємства за міжнародними стандартами інформаційної безпеки (наприклад, ISO/IEC 27001). Хоча ці вигоди важко кількісно оцінити, вони суттєво посилюють стратегічну позицію компанії.

Висновок до розділу 4

У четвертому розділі було виконано техніко-економічне обґрунтування розробки інформаційної підсистеми захисту даних корпоративних систем. Проведений аналіз дозволив встановити доцільність створення та впровадження розробленої системи не лише з позицій безпеки, але й з огляду на фінансову ефективність проєкту. Визначено загальні параметри та характер майбутньої експлуатації, проаналізовано обсяги необхідних ресурсів, здійснено розрахунки витрат на проєктування, впровадження, обслуговування та супровід системи впродовж гарантійного та післягарантійного періоду.

Розрахунки показали, що загальні витрати на розробку, тестування, встановлення та супровід становлять 198,4 тис. грн. Водночас очікувані щорічні вигоди від зниження ризиків, уникнення інцидентів інформаційної безпеки, автоматизації процесів моніторингу та резервного копіювання становлять 125 тис. грн. Протягом трьох років експлуатації система забезпечує загальний економічний ефект у розмірі 375 тис. грн. Враховуючи ці дані, чистий прибуток становить 176,6 тис. грн, а період окупності проєкту – менше двох років. Це свідчить про високу рентабельність впровадження системи та швидке повернення інвестицій.

Також було враховано непрямі вигоди, які хоча й важко формалізувати у грошовому еквіваленті, мають вагоме значення для стратегічного розвитку підприємства. До них належать зростання довіри з боку партнерів, дотримання вимог стандартів інформаційної безпеки, спрощення сертифікації, зниження ризиків штрафних санкцій з боку регуляторних органів. Усі ці аспекти є важливою складовою довгострокової конкурентної переваги компанії.

РОЗДІЛ 5. ОХОРОНА ПРАЦІ

5.1 Вступ

Охорона праці є важливою складовою організації будь-якого виду діяльності, особливо у сфері інформаційних технологій, де робочий процес пов'язаний з постійним використанням комп'ютерної техніки, електронного обладнання та програмного забезпечення. Забезпечення безпечних і комфортних умов праці не лише гарантує збереження здоров'я працівників, але й сприяє підвищенню продуктивності, зниженню кількості травм та зменшенню ризиків виникнення професійних захворювань. Саме тому питання охорони праці під час розробки, тестування та впровадження інформаційних систем набуває особливої актуальності.

У межах реалізації програмного забезпечення для захисту корпоративних даних важливо враховувати умови, у яких здійснюється розробка, а також вплив факторів виробничого середовища на безпеку праці фахівців. Це передбачає дотримання вимог нормативно-правових актів у сфері охорони праці, організацію робочого простору відповідно до ергономічних стандартів, контроль рівня шуму, освітленості, мікроклімату, а також впровадження заходів щодо електробезпеки, пожежної безпеки та захисту працівників від дії шкідливих факторів.

Окрему увагу слід приділяти профілактиці перевтоми, психоемоційного вигорання та інших негативних наслідків, що можуть виникнути внаслідок надмірного інтелектуального навантаження або тривалої роботи з екранними пристроями. Рациональна організація праці, чергування роботи і відпочинку, використання якісних засобів індивідуального захисту та надання працівникам відповідних інструкцій є запорукою безпеки під час виконання виробничих завдань.

5.2 Аналіз небезпечних і шкідливих факторів

У процесі роботи над розробкою та впровадженням інформаційної підсистеми захисту корпоративних даних необхідно враховувати вплив виробничих умов на здоров'я та безпеку працівників, насамперед – фахівців, що працюють із персональними електронно-обчислювальними машинами (ПЕОМ), мережевим обладнанням, серверами, системами моніторингу та резервного копіювання. Робота з комп'ютерною технікою має свої особливості і пов'язана з низкою шкідливих і небезпечних виробничих факторів, які, хоча й не завжди є очевидними, можуть накопичуватись і викликати негативні наслідки при тривалому впливі.

З метою систематизації таких факторів проведено аналіз, результати якого узагальнено на рисунку 5.1. Центром впливу є робоче місце ІТ-спеціаліста (розробника, оператора ПЕОМ, тестувальника), на яке впливають чотири основні групи факторів: фізичні, хімічні, психофізіологічні та ергономічні. Кожна з них чинить своє специфічне навантаження, що вимагає впровадження відповідних заходів безпеки.

До **фізичних факторів** належить передусім нераціональне або надмірне освітлення, яке може викликати перевтому очей, зниження продуктивності та головний біль. Часто ігнорується рівень шуму в офісному середовищі, хоча тривалий фоновий шум від комп'ютерних систем, систем охолодження чи друкувального обладнання має накопичувальний вплив. Не менш важливими є вібрації, які можуть виникати в серверних приміщеннях або біля багатофункціональних пристроїв. Особливої уваги заслуговує електромагнітне випромінювання від моніторів – хоча сучасні дисплеї значно безпечніші за своїх попередників, тривале перебування на близькій відстані до екрана залишається джерелом потенційного ризику

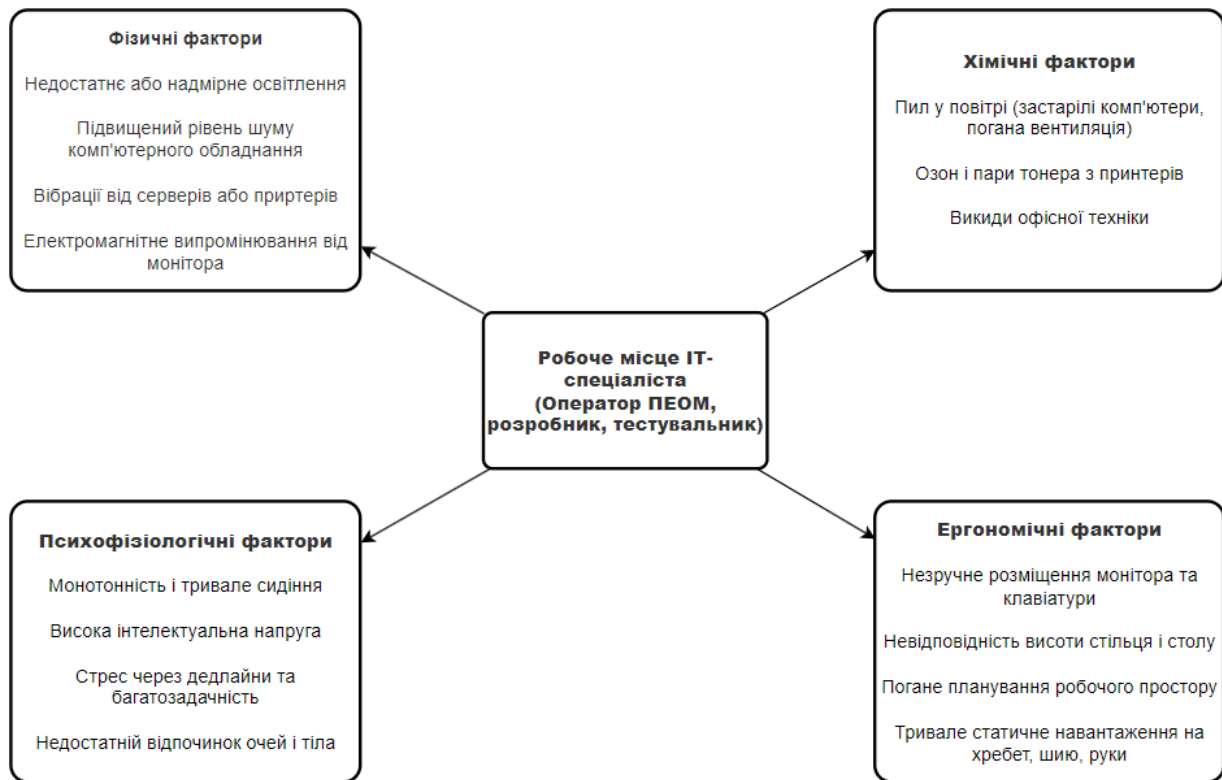


Рисунок 5.1 – Класифікація небезпечних і шкідливих виробничих факторів на робочому місці ІТ-спеціаліста

У середовищі офісної техніки присутні також хімічні фактори. Застарілі комп'ютери, пилові системні блоки, недостатня вентиляція в офісі – все це сприяє накопиченню пилу у повітрі, що може викликати алергічні реакції або захворювання органів дихання. Озон та інші продукти, що виділяються в процесі роботи лазерних принтерів, зокрема під час нагрівання тонера, також є токсичними у замкнених приміщеннях. Більше того, деякі пластики, з яких виготовлено комп'ютерні корпуси, при нагріванні виділяють формальдегід або інші леткі органічні сполуки, що погіршують якість повітря.

Окрему групу становлять психофізіологічні фактори, які пов'язані з характером роботи ІТ-спеціаліста. Насамперед це монотонність та тривале сидіння за комп'ютером, що спричиняє втому, зниження уваги та працездатності.

Складність завдань, потреба в постійній концентрації, багатозадачність, жорсткі дедлайни та високі очікування з боку керівництва формують стресові ситуації, що можуть мати хронічний характер. За відсутності регламентованих перерв, вправ для очей та фізичних розминок виникають ризики порушення функцій зору, нервової системи, а також професійного вигорання.

Завершує загальну структуру ергономічна група факторів, яка має безпосередній вплив на опорно-руховий апарат працівника. Зазвичай робоче місце ІТ-спеціаліста не адаптоване до індивідуальних анатомічних особливостей: висота монітора не відповідає рівню очей, клавіатура розміщена під неприродним кутом, стілець має обмежене регулювання. Унаслідок цього формується тривале статичне навантаження на шийний і поперековий відділи хребта, що сприяє розвитку остеохондрозу, викривлення постави або м'язових спазмів.

Таким чином, аналіз виявлених факторів свідчить про необхідність проведення комплексу профілактичних, ергономічних та організаційних заходів, спрямованих на мінімізацію ризиків. Це включає регулярну вентиляцію приміщення, правильне облаштування робочого простору, дотримання режиму праці та відпочинку, використання сучасного обладнання з низьким рівнем шуму та випромінювання. У подальших підрозділах будуть запропоновані конкретні заходи з охорони праці, відповідно до чинного законодавства України та нормативно-правових актів у сфері безпеки праці.

5.2.1 Освітленість робочого місця

Освітлення робочого місця ІТ-спеціаліста є важливим фактором, що безпосередньо впливає на продуктивність праці, рівень зорового навантаження, загальний комфорт і стан здоров'я працівника. В умовах постійної взаємодії з

екранами моніторів належне освітлення забезпечує зменшення втоми очей, запобігає погіршенню зору, підвищує концентрацію уваги та знижує кількість помилок у роботі.

Природне освітлення має перевагу завдяки спектральному складу та змінності інтенсивності протягом дня, що сприяє кращій адаптації зору та психофізіологічному самопочуттю. Робочі місця, розташовані поруч із вікнами, повинні бути організовані так, щоб уникати прямих сонячних променів на екрани моніторів, оскільки це викликає відблиски, які знижують контрастність зображення та провокують додаткове навантаження на очі. У випадках, коли природного освітлення недостатньо або воно відсутнє, слід забезпечити якісне штучне освітлення.

Штучне освітлення, у свою чергу, повинно відповідати нормам, встановленим чинними санітарно-гігієнічними нормативами України, зокрема ДСанПіН 3.3.2.007–98. Згідно з нормативами, освітленість робочої поверхні при роботі з ПЕОМ має становити не менше 300 лк при комбінованому освітленні та 400 лк – у випадку виключно штучного освітлення. Найкраще використовувати люмінесцентні або світлодіодні лампи з температурою кольору в діапазоні 4000–5000 К, що найбільше відповідає природному денному світлу.

Світильники мають бути встановлені таким чином, щоб рівномірно освітлювати робочий простір без створення тіней або зон з підвищеною яскравістю. Направлення світла повинне бути збалансованим, а джерела світла не мають потрапляти у пряму видимість користувача, щоб уникнути засліплення. Занадто яскраве або холодне освітлення може викликати головний біль, дратівливість та швидко втому, тоді як надто слабе освітлення призводить до перенапруження зорового апарату.

Особливу увагу варто приділяти організації локального освітлення, наприклад, за допомогою настільної лампи із регульованою інтенсивністю та напрямом світла. Це дозволяє адаптувати освітленість до індивідуальних потреб

працівника залежно від типу виконуваної роботи. При цьому колірна температура та яскравість додаткового джерела світла повинні бути узгоджені з загальним освітленням приміщення.

Регулярна перевірка рівня освітленості є важливою складовою системи охорони праці. За потреби необхідно проводити вимірювання люксометром та своєчасно замінювати джерела світла. Дотримання встановлених параметрів освітлення не лише сприяє збереженню здоров'я очей, але й покращує загальну ефективність праці працівника.

5.2.2 Вплив випромінювання

Випромінювання, що виникає під час роботи з електронно-обчислювальною технікою, зокрема персональними комп'ютерами, є важливим чинником, який необхідно враховувати при організації безпечного робочого середовища для ІТ-фахівців. Хоча рівень електромагнітного випромінювання сучасних пристроїв значно нижчий порівняно з устаткуванням попередніх поколінь, його вплив на організм людини за тривалої експлуатації залишається предметом уваги з боку гігієністів праці, технічних фахівців та фахівців з охорони праці.

Основним джерелом випромінювання на робочому місці є монітори, особливо ті, що використовують технології з електронно-променевою трубкою (ЕПТ). Такі пристрої генерують рентгенівське, ультрафіолетове, інфрачервоне та електромагнітне випромінювання у низькочастотному та радіочастотному діапазонах. Однак із переходом до моніторів на основі рідкокристалічних (LCD), світлодіодних (LED) або OLED-технологій ці загрози суттєво зменшилися. Проте залишаються чинними деякі форми електромагнітного випромінювання в межах радіо- та наднизькочастотного спектру, які виникають під час роботи самого пристрою та підключення до мережі.

Крім того, комп'ютери, мережеве обладнання, принтери та блоки живлення також створюють електромагнітні поля, інтенсивність яких залежить від потужності, якості екранізації компонентів і умов експлуатації. При тривалому перебуванні в зоні дії таких джерел можливі прояви функціональних змін у нервовій системі, порушення сну, втома, головний біль і зниження загального тону організму. Особливо чутливими до впливу випромінювання є люди з підвищеною індивідуальною реактивністю або хронічними захворюваннями.

Для зменшення негативного впливу випромінювання на користувача рекомендується дотримуватися нормативів безпеки, передбачених державними стандартами, такими як ДСанПіН 3.3.2.007–98, які встановлюють гранично допустимі рівні електромагнітних полів на робочому місці. Робоче місце має бути організоване з урахуванням безпечної відстані до екранів моніторів та інших джерел випромінювання (не менше 50–70 см), а також розміщене так, щоб уникнути перехресного впливу від кількох пристроїв одночасно.

Крім того, важливо правильно заземлити обладнання, уникати роботи зі зношеними чи несправними пристроями, які можуть створювати підвищений рівень фонових електромагнітних полів. Слід віддавати перевагу сертифікованим моделям техніки з енергетичними та безпековими маркуваннями (наприклад, TCO, CE, Energy Star).

Регулярне провітрювання приміщення, перерви в роботі з монітором, а також використання екранів-фільтрів для зменшення відблисків і статичного навантаження на очі, також є дієвими профілактичними заходами. У випадку роботи в середовищі з високою щільністю техніки (серверні кімнати, центри обробки даних) доцільно передбачити захисні екрани, екранізовані кабелі та системи моніторингу електромагнітного фону.

5.2.3 Вплив електричного струму

Електричний струм є одним із головних потенційно небезпечних фізичних факторів у середовищі ІТ-фахівця. Незважаючи на те, що робота за комп'ютером вважається низьковольтною діяльністю, сучасні інформаційні системи передбачають використання великої кількості електропристроїв, блоків живлення, розеткових ліній, периферійного обладнання, що створює умови для можливого ураження працівника електричним струмом.

Основними ризиками при роботі з комп'ютерною технікою є прямий дотик до струмопровідних частин, що опинилися під напругою через порушення ізоляції, несправність електричних з'єднань або відсутність заземлення. Крім того, вторинними факторами безпеки є можливість виникнення короткого замикання, перегріву електрокабелів, займання або вибуху акумуляторів.

Ураження електричним струмом може викликати низку небезпечних наслідків для організму людини – від незначного м'язового скорочення до зупинки дихання, фібриляції серця та летального результату. Ступінь ураження залежить від сили та тривалості струму, шляху його проходження через тіло, а також стану здоров'я потерпілого.

Для забезпечення безпеки в умовах офісного середовища необхідно суворо дотримуватись вимог нормативної документації, зокрема правил улаштування електроустановок (ПУЕ), правил охорони праці під час експлуатації електроустановок споживачів, а також ДСТУ EN 50110. Усі електропристрої повинні мати заводські сертифікати, бути справними, регулярно проходити технічне обслуговування та перевірку ізоляції.

Одним з ключових заходів є наявність ефективного захисного заземлення, яке забезпечує відведення струму в землю у разі пробоя ізоляції. В офісних приміщеннях має бути організована система автоматичного вимкнення живлення при витoku струму (застосування УЗО – пристроїв захисного відключення). Крім

того, робочі місця повинні бути оснащені якісною кабельною інфраструктурою, без оголених або скручених проводів, що знаходяться у відкритому доступі.

Особливої уваги вимагає використання тимчасових розгалужувачів, подовжувачів і нестандартних джерел живлення. Таке обладнання часто є джерелом підвищеної небезпеки через відсутність сертифікації, перевантаження або порушення конструктивної цілісності.

Профілактикою ураження електричним струмом є регулярні інструктажі з електробезпеки, дотримання персоналом правил безпечного поводження з електропристроями, недопущення використання несправного обладнання та постійний візуальний контроль за станом мережі. У випадках появи сторонніх запахів (гару), перегріву пристроїв або іскріння – експлуатацію слід негайно припинити.

Отже, навіть у сфері інформаційних технологій, де основна діяльність не пов'язана з електромонтажними роботами або високою напругою, ризик ураження електричним струмом залишається актуальним. Саме тому забезпечення електробезпеки є невід'ємною складовою загальної системи охорони праці на підприємстві.

5.2.4 Виробничий шум

В умовах роботи ІТ-фахівців, зокрема операторів ПЕОМ, розробників і тестувальників, виробничий шум є поширеним шкідливим фактором, який може мати негативний вплив на стан здоров'я, продуктивність праці та загальний психоемоційний стан працівника. Незважаючи на те, що офісне середовище зазвичай не асоціюється з високим рівнем шумового забруднення, сукупна дія багатьох джерел може спричиняти перевищення допустимих норм і створювати хронічне навантаження на слуховий апарат і нервову систему.

Основними джерелами шуму в офісному середовищі є системні блоки комп'ютерів, сервери, системи охолодження, принтери, джерела безперебійного живлення (ДБЖ), кондиціонери, а також фонові розмови колег, робота телефонів та інша офісна техніка. Постійна дія низько- або середньочастотного шуму, навіть при порівняно невисокому рівні інтенсивності, викликає подразнення, втому, зниження концентрації уваги, порушення когнітивних функцій, а в деяких випадках – головний біль та дратівливість.

Згідно з нормами ДСН 3.3.6.037–99 «Гігієнічна класифікація праці за показниками шкідливості та небезпечності факторів виробничого середовища», допустимий рівень шуму на робочому місці, що не потребує високої акустичної чутливості, не повинен перевищувати 50 дБ. У разі тривалого перевищення цього рівня зростає ризик розвитку нейросенсорної туговухості, порушень серцево-судинної системи та емоційного вигорання.

Для мінімізації негативного впливу шуму необхідно впроваджувати комплекс заходів. Серед технічних рішень варто зазначити використання сучасного комп'ютерного обладнання з низьким рівнем шуму, розміщення серверів у спеціалізованих ізольованих приміщеннях, установлення шумопоглинальних матеріалів у стінах і стелях, а також забезпечення акустичної ізоляції при плануванні офісного простору. Крім того, ефективним заходом є організація «тихих зон» для зосередженої роботи.

Організаційні заходи включають контроль за дотриманням допустимих рівнів шуму, проведення вимірювань та аудиту акустичних характеристик приміщень, чергування інтенсивної роботи з перервами, а також ротацію персоналу для зниження рівня шумового навантаження. У разі перевищення граничнодопустимих рівнів рекомендовано використання індивідуальних засобів захисту слуху (беруші, навушники з шумозаглушенням).

5.2.5 Умови мікроклімату

Мікроклімат приміщень є одним із ключових факторів, що визначає безпечність та комфортність умов праці, особливо у сфері інформаційних технологій, де працівники проводять тривалий час у закритому офісному просторі перед моніторами. Параметри мікроклімату – це температура повітря, вологість, швидкість руху повітря та інтенсивність теплового випромінювання – мають бути оптимальними, щоб не викликати фізіологічного дискомфорту, втоми або порушень здоров'я.

Відповідно до вимог ДСанПіН 3.3.6.042–99 «Державні санітарні правила і норми», оптимальні параметри мікроклімату для користувачів ПЕОМ у холодний період року складають: температура повітря – 21–23 °С, відносна вологість – 40–60 %, швидкість руху повітря – не більше 0,1 м/с. У теплий період року допустимими є: температура – 23–25 °С, вологість – до 60 %, швидкість повітря – не вище 0,2 м/с. Відхилення від цих меж, особливо при тривалому впливі, можуть викликати гіпотермію або перегрів організму, зневоднення, сонливість, втрату концентрації, а також загострення хронічних захворювань.

У сучасних офісах основну роль у підтриманні мікроклімату відіграють системи вентиляції, кондиціонування та опалення. Вентиляція забезпечує приплив свіжого повітря, видалення вуглекислого газу та інших забруднень. Кондиціонери регулюють температуру й вологість повітря, але при неправильному використанні можуть спричиняти пересушення повітря, застій повітряних мас або навіть локальні переохолодження.

Недостатня вологість у приміщенні може викликати пересушення слизових оболонок, подразнення очей, головний біль і підвищену стомлюваність, що особливо небезпечно для працівників, які довго працюють за комп'ютером. Надмірна ж вологість може сприяти розвитку плісняви, грибків і створювати сприятливе середовище для мікроорганізмів. Оптимальним рішенням є

встановлення автоматизованих систем клімат-контролю, які постійно відслідковують параметри повітря та підтримують їх у межах нормативів.

Особливу увагу слід приділяти локальним джерелам тепла – моніторам, комп'ютерам, мережевому обладнанню, які можуть істотно впливати на мікроклімат окремих зон приміщення. Їх необхідно розміщувати з урахуванням циркуляції повітря і забезпечення охолодження.

Організаційні заходи, спрямовані на поліпшення умов мікроклімату, включають регулярний контроль температури й вологості, провітрювання приміщень, обмеження тривалості безперервної роботи за комп'ютером і створення умов для відпочинку у добре провітрюваних зонах.

5.2.6 Організація робочого місця

Раціональна організація робочого місця є ключовим чинником забезпечення безпеки, комфорту та ефективності праці працівників, які взаємодіють із комп'ютерною технікою. Належна організація дозволяє мінімізувати професійні ризики, пов'язані з тривалою статичною позою, втомою очей, порушенням постави, перенапруженням м'язів спини, шиї та кистей рук.

Робоче місце має бути обладнане відповідно до вимог ДСанПіН 3.3.2.007–98 та інших нормативних документів, що регламентують умови праці користувачів персональних електронно-обчислювальних машин. Комп'ютерний стіл повинен мати достатню площу для розміщення монітора, клавіатури, миші, документів та інших необхідних елементів. Висота столу повинна забезпечувати зручне положення рук користувача на клавіатурі з кутом у ліктьовому суглобі приблизно 90 градусів. Поверхня столу має бути матовою, щоб уникати відблисків і зайвого навантаження на зір.

Крісло для користувача повинно бути регульованим за висотою, мати спинку, що підтримує природний вигин хребта, підлокітники та можливість

фіксації положення. Особливу увагу слід приділити наявності підставки для ніг, якщо робоче місце не дозволяє користувачу тримати ступні повністю на підлозі.

Монітор комп'ютера необхідно встановлювати на відстані 60–70 см від очей користувача, причому верхній край екрана повинен бути на рівні очей або трохи нижче. Це дозволяє зменшити напруження очних м'язів і знизити ризик розвитку зорового стомлення. Екран не повинен бути джерелом відблисків, тому його розміщують під прямим кутом до вікон або джерел штучного світла. Також рекомендовано використовувати антивідблискові фільтри.

Периферійні пристрої, зокрема клавіатура та миша, мають бути розташовані на одному рівні, без необхідності додаткового навантаження на кисті. Варто уникати занадто великої або надмірно маленької амплітуди рухів. Оптимальна площа для роботи за столом передбачає вільне переміщення рук і тіла працівника без надмірного нахилу чи розтягування.

До додаткових заходів безпеки належить обмеження тривалості безперервної роботи з ПЕОМ. Згідно з вимогами, рекомендовано робити короткотривалі перерви кожні 50–60 хвилин, під час яких працівник виконує вправи для зняття м'язового і зорового навантаження.

5.3 Розрахунок освітленості робочого місця

Освітленість робочого місця має важливе значення для забезпечення безпеки та ефективності праці. Недостатній рівень освітлення призводить до швидкої втоми очей, зниження продуктивності, погіршення концентрації та підвищення ризику професійних захворювань зору. Тому освітлення має відповідати вимогам ДБН В.2.5-28:2018 та ДСанПіН 3.3.2.007–98.

Для розрахунку необхідної кількості світильників у приміщенні використовується метод світлового потоку. Його основна формула має вигляд:

$$N = \frac{E * S * K}{F * n * \eta}$$

де:

N – кількість світильників;

E – нормована освітленість, лк;

S – площа приміщення, м²;

K – коефіцієнт запасу (1.5 – для ламп зі стабільними характеристиками);

F – світловий потік однієї лампи, лм;

n – кількість ламп у світильнику;

η – коефіцієнт використання світлового потоку (приймаємо 0.6).

Вважаємо, що розрахункове приміщення має розміри 6 м × 4 м, отже:

$$S = 6 * 4 = 24 \text{ м}^2$$

Нормована освітленість для роботи з комп'ютером згідно ДБН становить:

$$E = 300 \text{ лк}$$

Світловий потік однієї світлодіодної лампи:

$$F = 1800 \text{ лм}$$

Кількість ламп у кожному світильнику:

$$n = 2$$

Підставимо значення в основну формулу:

$$N = \frac{300 * 24 * 1.5}{1800 * 2 * 0.6} = \frac{10800}{2160} = 5$$

Таким чином, для забезпечення нормативного рівня освітленості необхідно встановити 5 світильників з двома світлодіодними лампами по 1800 лм кожна.

З урахуванням рівномірного розміщення освітлювальних приладів, їх слід розташовувати у шаховому порядку на стелі, забезпечуючи однакову відстань між ними та рівномірне розсіювання світлового потоку. Це дозволить уникнути утворення тіней, відблисків і зон з недостатньою яскравістю. Висота підвісу або монтажу світильників також має бути оптимальною – не нижче 2,5 м, щоб забезпечити комфортне освітлення без засліплення.

Таблиця 5.1 – Вихідні дані для розрахунку освітленості

Параметр	Значення
Розміри приміщення	6 × 4 м
Площа приміщення S	24 м²
Нормована освітленість E	300 лк
Коефіцієнт запасу K	1.5
Світловий потік лампи F	1800 лм
Кількість ламп у світильнику n	2
Коефіцієнт використання η	0.6
Необхідна кількість світильників N	5

5.4 Розробка заходів щодо зменшення впливу небезпечних і шкідливих факторів

Робоче середовище користувача комп'ютерної системи захисту корпоративних даних супроводжується низкою небезпечних і шкідливих

факторів, серед яких ключовими є неадекватне освітлення, електромагнітне випромінювання, вплив електричного струму, виробничий шум, порушення мікроклімату та ергономічні недоліки робочого місця. Для забезпечення безпеки праці необхідно розробити і впровадити комплекс профілактичних заходів, які б дозволили мінімізувати їхній негативний вплив на людину.

Насамперед, для зменшення навантаження на зір і запобігання зоровій втомі забезпечується відповідний рівень освітленості на робочому місці. Освітлення має бути рівномірним, не створювати тіней або відблисків, а також відповідати вимогам нормативів, встановлених для роботи з комп'ютерною технікою. Для цього використовуються сучасні світлодіодні світильники з нейтральним білим спектром, розташовані на достатній висоті з урахуванням розсіювання світлового потоку.

Ще одним важливим аспектом є зменшення впливу електромагнітного випромінювання, яке створюється моніторами, блоками живлення та іншими пристроями. З огляду на це, робочі місця обладнуються екранами з мінімальним рівнем електромагнітного фону, відповідними сертифікатами безпеки. Додатково проводиться регулярна перевірка рівнів випромінювання з використанням спеціалізованих приладів. У разі виявлення перевищення допустимих норм здійснюється заміна обладнання або вдосконалення заземлення.

Враховуючи потенційну небезпеку ураження електричним струмом, в офісі впроваджується багаторівневий захист, який включає наявність автоматичних вимикачів, пристроїв захисного відключення, перевірку електропроводки на відповідність стандартам, а також використання якісних сертифікованих джерел живлення. Персонал проходить інструктаж з електробезпеки, де ознайомлюється з правилами користування електроприборами, зокрема – заборонаю доторкання до відкритих контактів та самостійного втручання у електричні схеми.

Шумове навантаження, хоча і не є домінуючим у сфері офісної праці, все ж може чинити негативний вплив на увагу та нервову систему. Для зменшення

рівня шуму використовуються малOSHумні комп'ютери, енергозберігаючі блоки живлення, безшумні системи охолодження. У разі наявності джерел постійного шуму (наприклад, серверних) рекомендується їх звукоізоляція або винесення у спеціальні приміщення. Також слід забезпечити належну акустику самого робочого простору: встановлення звукопоглинаючих матеріалів на стінах, підвісна стеля, килимові покриття підлоги.

Оптимальний мікроклімат у приміщенні має ключове значення для продуктивності роботи та загального самопочуття працівників. Температура повітря має підтримуватися на рівні 20–24 °C у холодний період та 22–26 °C у теплий. Вологість повітря не повинна знижуватися нижче 40 %. Забезпечення таких умов досягається за рахунок автоматизованих систем вентиляції, кондиціонування повітря та встановлення зволожувачів у зимовий період. Контроль параметрів здійснюється за допомогою кімнатних термогігрометрів або систем розумного моніторингу клімату.

Окремо слід звернути увагу на ергономічні характеристики робочого місця. Робоче місце має бути обладнане регульованим кріслом з підтримкою поперекового відділу спини, а висота столу й положення монітора повинні відповідати анатомічним особливостям користувача. Екран монітора розташовується на відстані 50–70 см від очей, причому його верхній край має бути приблизно на рівні очей. Клавіатура розміщується на відстані, що забезпечує вільне положення передпліччя, не викликаючи напруги у зап'ястях.

Впровадження наведених заходів дозволяє істотно підвищити рівень безпеки праці, мінімізувати вплив шкідливих факторів, а також створити комфортні умови для роботи персоналу. Ретельна організація умов праці має не лише санітарно-гігієнічне значення, але й впливає на ефективність використання інформаційної системи, зменшуючи ймовірність помилок та підвищуючи загальний рівень дисципліни та відповідальності співробітників.

5.4.1. Заходи щодо зниження величини виникаючих зарядів статичної електрики

У процесі експлуатації комп'ютерної техніки та інших елементів електронної апаратури, особливо в умовах офісних приміщень з низькою вологістю повітря та високою інтенсивністю переміщення повітря, часто виникає проблема накопичення зарядів статичної електрики. Це явище може мати негативні наслідки як для самого електронного обладнання, так і для користувачів, оскільки супроводжується потенційним ризиком електростатичного пробоя, пошкодженням чутливих компонентів або навіть короточасними порушеннями в роботі систем.

З метою мінімізації рівня накопичення зарядів статичної електрики у приміщеннях, де встановлюється інформаційна система захисту корпоративних даних, передбачається впровадження низки організаційних і технічних заходів. Одним з ключових напрямів є регулювання вологості повітря, оскільки низький рівень вологості сприяє більш активному накопиченню зарядів на поверхнях. Для цього застосовуються системи автоматичного зволоження, які підтримують показники вологості в межах оптимального діапазону – від 45 до 60 %. Таке середовище значно знижує ймовірність утворення зарядів.

Особливу увагу слід приділити вибору матеріалів для оздоблення приміщення та робочих поверхонь. Синтетичні покриття, особливо з пластмаси, мають високий рівень електростатичного накопичення. Тому для підлог рекомендовано використовувати антистатичні лінолеуми або килимові покриття з вуглецевим прошарком. Робочі столи також мають бути виготовлені з антистатичних матеріалів або покриватися спеціальними антистатичними підкладками. Крім того, запроваджується регулярна обробка поверхонь антистатичними засобами, що створюють захисну плівку й знижують електростатичну напругу.

Ефективним технічним заходом є заземлення всього електронного обладнання. Заземлювальні контури повинні відповідати нормативним вимогам і мати стабільне електричне з'єднання із заземлювальними шинами будівлі. Всі металеві частини корпусів комп'ютерів, серверів, шаф повинні бути з'єднані з контуром заземлення, що унеможливорює накопичення електричного заряду. Окремо слід відзначити доцільність встановлення антистатичних браслетів або підлогових контактних стрічок у зонах ремонту чи тестування обладнання.

Також велике значення має організація робочої поведінки персоналу. Працівники повинні уникати носіння одягу з матеріалів, що сприяють накопиченню зарядів (наприклад, з поліестеру). Перевагу слід надавати одягу з натуральних тканин або з антистатичним просоченням. Крім того, важливо навчати співробітників правилам безпечної роботи з електронною технікою, включаючи заборону доторкання до внутрішніх частин апаратури без попереднього заземлення.

Застосування комплексного підходу до вирішення проблеми електростатичних зарядів дозволяє забезпечити не лише довготривалу працездатність інформаційної системи, але й створити безпечні умови праці для персоналу, знизити ризики пошкодження обладнання та запобігти збоїв у роботі програмно-апаратного комплексу.

5.4.2 Заходи щодо зниження шуму на робочому місці

Шум на робочому місці є одним із основних чинників, що впливають на працездатність і самопочуття працівників, особливо у сфері інформаційних технологій, де передбачається тривале перебування в офісних приміщеннях із високою щільністю електронного обладнання. Надмірний рівень шуму призводить до підвищеної втомлюваності, зниження концентрації, погіршення когнітивних функцій, а в тривалій перспективі – до серйозних фізіологічних

наслідків, зокрема порушення слуху, головного болю та підвищення артеріального тиску.

Для забезпечення сприятливих умов праці під час розробки та впровадження інформаційної системи захисту корпоративних даних передбачено комплекс заходів, спрямованих на зниження рівня шуму в приміщенні. Першочергово реалізується правильне планування розміщення шумогенерувального обладнання, зокрема серверів, мережевих комутаторів, систем охолодження. Ці пристрої виносяться у спеціалізовані технічні приміщення або серверні кімнати з відповідною звукоізоляцією. Таке рішення дозволяє фізично відокремити джерела шуму від основного простору для роботи персоналу.

У самому робочому приміщенні використовуються конструктивні елементи для поглинання шуму. До таких належать звукопоглинальні панелі на стінах та стелі, килимові покриття на підлозі, м'які меблі й жалюзі, які зменшують відбиття звукових хвиль. Особливу увагу приділяється матеріалам оздоблення, зокрема вибору пористих акустичних панелей і звукопоглинального гіпсокартону, які знижують рівень реверберації й створюють комфортне акустичне середовище.

Технічна модернізація обладнання також є важливим напрямом. Використання комп'ютерів і периферійних пристроїв із низьким рівнем шуму, наприклад, безвентиляторних корпусів, твердотільних накопичувачів замість традиційних жорстких дисків, а також енергоефективних блоків живлення зі зниженим рівнем вібрації дозволяє значно зменшити загальну акустичну напругу. Також передбачено періодичне технічне обслуговування систем охолодження для уникнення зайвих вібрацій і шумів через накопичення пилу або механічні пошкодження.

Організаційні заходи включають регламентування часу експлуатації деяких пристроїв у години найменшої активності персоналу, а також надання

співробітникам засобів індивідуального захисту слуху (наприклад, шумозаглушувальних навушників) у разі виконання завдань у зоні з підвищеним рівнем шуму. Водночас у проєкті враховано ергономічне розміщення робочих місць, з таким розрахунком, щоб найменш шумні ділянки були відведені для зон тривалого перебування працівників.

Застосування вказаних заходів дає змогу забезпечити відповідність акустичних умов на робочому місці гігієнічним нормативам, підвищити рівень комфорту та ефективності праці, а також зменшити вплив негативних факторів на здоров'я співробітників.

Висновок до розділу 5

У межах п'ятого розділу було здійснено всебічний аналіз умов праці, що супроводжують процес розробки та впровадження інформаційної системи захисту корпоративних даних. Особлива увага приділялася вивченню чинників, які можуть потенційно впливати на безпеку й ефективність працівників, залучених до експлуатації технічних засобів у межах сучасного офісного середовища. Розгляд таких аспектів, як освітленість робочих місць, вплив електромагнітного випромінювання, виробничого шуму, електричного струму, мікрокліматичних умов та загальна організація простору, дав змогу сформулювати цілісне уявлення про наявні ризики та способи їхньої нейтралізації.

Встановлено, що в умовах інтенсивного використання комп'ютерної техніки та іншого електронного обладнання особливого значення набувають параметри освітлення та мікроклімату, які безпосередньо впливають на стан зору, рівень стомлюваності та працездатність персоналу. Аналіз показав, що перевищення граничнодопустимих рівнів шуму та електромагнітного фону, а також нераціональне розміщення обладнання можуть призводити до погіршення самопочуття й виникнення професійних захворювань. З цієї причини було

здійснено розрахунок освітленості робочого місця з урахуванням нормативних вимог та визначено необхідні характеристики освітлювальних приладів для досягнення оптимального рівня світлового середовища.

Також проаналізовано потенційні джерела небезпеки, пов'язані з накопиченням статичної електрики, підвищенням рівнем шуму та можливим контактом з електричним струмом. Для зменшення негативного впливу зазначених факторів було запропоновано комплекс профілактичних і захисних заходів, які включають як інженерно-технічні, так і організаційні рішення. Серед них особливу роль відіграють використання звукопоглинальних матеріалів, екранування джерел електромагнітного випромінювання, запровадження систем вентиляції й кондиціонування, а також чітке дотримання правил електробезпеки.

Результати проведеного аналізу свідчать про необхідність системного підходу до охорони праці на всіх етапах реалізації інформаційної системи. Забезпечення безпечних та комфортних умов праці не лише відповідає нормативним вимогам, а й сприяє зростанню продуктивності, підвищенню мотивації працівників та зниженню рівня професійних ризиків. Таким чином, дотримання стандартів з охорони праці є обов'язковим елементом будь-якого сучасного проєкту в галузі інформаційних технологій.

РОЗДІЛ 6. ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

6.1 Вступ

У сучасних умовах стрімкого розвитку інформаційних технологій питання охорони навколишнього середовища набуває особливого значення. Незважаючи на те, що сфера ІТ зазвичай асоціюється з невеликим фізичним впливом на довкілля, у процесі розробки, впровадження та експлуатації програмних систем виникає низка екологічних аспектів, які не можна ігнорувати. До таких чинників належать енергоспоживання серверного обладнання, утилізація електронних пристроїв, використання витратних матеріалів, а також викиди, пов'язані з логістикою та експлуатацією комп'ютерної інфраструктури.

Охорона навколишнього середовища у контексті інформаційних систем охоплює комплекс заходів, спрямованих на зменшення екологічного сліду від усіх етапів життєвого циклу програмного забезпечення – від проектування до його супроводу. Це включає раціональне використання ресурсів, впровадження енергоощадних технологій, продовження терміну експлуатації обладнання та правильну утилізацію електронних відходів. Особливої уваги вимагає організація серверної інфраструктури, яка має значне споживання електроенергії та потребує ефективної системи охолодження.

Таким чином, розділ присвячено аналізу впливу ІТ-систем на довкілля, визначенню основних екологічних ризиків, пов'язаних із функціонуванням інформаційної підсистеми захисту корпоративних даних, та обґрунтуванню заходів щодо їхньої мінімізації. Раціональний підхід до екологічної безпеки ІТ-рішень є не лише відповідальним кроком з боку розробника, а й важливим елементом сталого розвитку організації в умовах глобальних викликів.

6.2 Загальні відомості про забруднення

Проблема забруднення навколишнього середовища залишається однією з найгостріших у світовій екологічній політиці. В умовах стрімкого розвитку промисловості, транспорту та інформаційних технологій антропогенний вплив на природу набуває все більших масштабів, спричиняючи деструктивні зміни у біосфері. Забруднення – це процес надходження до довкілля фізичних, хімічних, біологічних або енергетичних агентів, які порушують природний стан середовища, знижують його якість та потенційно загрожують здоров'ю людей і живим організмам. Це явище носить як локальний, так і глобальний характер і впливає на всі компоненти екосистеми: повітря, воду, ґрунт, кліматичну рівновагу.

У широкому розумінні забруднення класифікують за видом впливу: хімічне, фізичне, біологічне, теплове, світлове та радіаційне. Хімічне забруднення виникає внаслідок потрапляння до довкілля токсичних речовин – газів, рідин чи твердих часток, які порушують хімічний баланс природного середовища. Найчастіше це оксиди сірки та азоту, чадний газ, метали, мийні засоби, нафтопродукти. Фізичне забруднення охоплює шум, вібрацію, теплові викиди, електромагнітне випромінювання, а також техногенне засмічення побутовими і промисловими відходами. Біологічне забруднення проявляється у вигляді проникнення у природу збудників захворювань, паразитів чи чужорідних біологічних агентів, що порушують стійкість місцевих екосистем. Теплове забруднення обумовлене скиданням нагрітих стоків у водойми або локальним підвищенням температури повітря. Окремо виокремлюють світлове та радіаційне забруднення, пов'язані з роботою нічного освітлення або техногенними джерелами іонізуючого випромінювання.

Забруднення довкілля, викликане інформаційними технологіями, на перший погляд не є таким очевидним, як промислові викиди чи транспортні

вихлопи. Однак непрямий внесок ІТ-сфери у процес забруднення зростає з кожним роком. Основними джерелами такого впливу є виробництво комп'ютерної техніки, утилізація електронних компонентів, експлуатація дата-центрів, витрати енергії на підтримку інфраструктури. Наприклад, утилізація електронних плат без дотримання екологічних норм призводить до виділення свинцю, ртуті, кадмію, бромованих вогнезахисних добавок, які є вкрай небезпечними для здоров'я людини. Неправильне зберігання акумуляторів або мікросхем спричиняє забруднення ґрунтів важкими металами, що потрапляють у підземні води.

Значну частку у структурі екологічного навантаження інформаційної галузі займає споживання електроенергії. У глобальному масштабі дата-центри, хмарні сервіси та телекомунікаційне обладнання є великими споживачами електричної енергії. Якщо енергетична система регіону базується на викопному паливі, то кожен спожитий кіловат електроенергії супроводжується викидом парникових газів у атмосферу, передусім вуглекислого газу. Таким чином, цифрові сервіси опосередковано впливають на зміну клімату, збільшення кислотності дощів та порушення природних екосистем.

Крім того, функціонування комп'ютерного обладнання супроводжується нагріванням, що вимагає додаткового кондиціонування приміщень, вентиляції та охолодження – усе це спричиняє додаткове споживання електроенергії та, відповідно, посилює вплив на навколишнє середовище. У масштабі великих організацій цей ефект стає відчутним навіть на рівні регіонального енергетичного балансу.

У таблиці 6.1 представлено основні типи забруднень та їхні джерела, пов'язані з функціонуванням ІТ-інфраструктури.

Таблиця 6.1 – Основні види забруднення, що пов’язані з інформаційними технологіями

Вид забруднення	Джерела у сфері ІТ	Можливі наслідки
Хімічне	Утилізація електронних плат, батарей, кабелів	Отруєння ґрунтів, вод, негативний вплив на флору і фауну
Фізичне	Робота комп’ютерів, серверів, блоків живлення	Електромагнітне випромінювання, шум, перегрівання
Біологічне	Обмежене, можливе через кондиționери та вентиляцію	Поширення мікроорганізмів у закритих просторах
Теплове	Робота дата-центрів і обчислювальної техніки	Перегрівання приміщень, локальне підвищення температури
Радіаційне	Монітори, джерела живлення низької потужності	Незначне, але накопичувальне опромінення

Таким чином, сучасні інформаційні системи, хоч і не мають безпосереднього агресивного впливу на природу, формують складну екологічну взаємодію, яка вимагає постійного моніторингу та запровадження стійких технологій. Розробка та експлуатація ІТ-систем мають відбуватись із урахуванням екологічних ризиків, впровадженням енергоефективних рішень, програм утилізації техніки та мінімізації цифрового сліду.

6.3 Заходи щодо запобігання забруднення навколишнього середовища

Функціонування будь-якої інформаційної системи, зокрема системи захисту корпоративних даних, пов’язане не лише з технічними й енергетичними ресурсами, а й із потенційним впливом на навколишнє середовище. Тому важливим напрямом стало впровадження комплексу екологічно орієнтованих

заходів, спрямованих на зниження рівня забруднення та раціональне використання ресурсів.

Запобігання забрудненню навколишнього середовища передбачає комплекс дій на всіх етапах життєвого циклу ІТ-системи: від проєктування, вибору обладнання, розміщення та експлуатації до утилізації застарілих компонентів. Одним із першочергових завдань є оптимізація енергоспоживання, оскільки саме електроенергія, що виробляється переважно з невідновлюваних джерел, супроводжується найбільшими викидами в атмосферу. Для зменшення споживання ресурсів використовуються енергоефективні сервери, монітори з автоматичним регулюванням яскравості, блоки живлення класу 80 PLUS тощо.

Наступним напрямом є раціональна організація інфраструктури. Забезпечення ефективного охолодження дата-центрів дозволяє уникати перевитрати енергії на кондиціонування. Досягнення цього можливе завдяки впровадженню систем рекуперації тепла, пасивного охолодження, використанню вікон часу, коли споживання є мінімальним, і застосуванню хмарних рішень замість фізичних серверів, коли це можливо.

Ще одним важливим аспектом є зменшення кількості електронних відходів. Це досягається шляхом подовження терміну експлуатації обладнання, використання модульних комп'ютерних систем із можливістю модернізації, а також правильного поводження з відпрацьованими батареями, платами, кабелями. Забороняється самотійна утилізація або зберігання пошкоджених електронних компонентів, адже це може призвести до викидів токсичних речовин у ґрунт або повітря. Замість цього впроваджуються системи централізованого збору та передачі електронних відходів на сертифіковані переробні підприємства.

У сфері розробки програмного забезпечення також можуть бути реалізовані екологічні підходи, наприклад, шляхом створення оптимізованого коду, що не перевантажує серверні потужності та потребує менше обчислювальних ресурсів. При проєктуванні архітектури системи рекомендовано

дотримуватись принципів «зеленої розробки», які передбачають мінімізацію використання складних обчислень і підтримку лише необхідної кількості фонових процесів.

Важливою частиною заходів також є екологічна освіта персоналу, адже саме працівники щоденно взаємодіють з обладнанням і впливають на обсяг споживаних ресурсів. Проведення інструктажів щодо енергоефективного використання комп'ютерної техніки, правильного поводження з відходами, вимкнення обладнання після завершення роботи сприяє загальному зменшенню екологічного навантаження організації.

Крім того, інформатизація підприємства дозволяє вивести частину процесів у цифрове середовище, що знижує потребу у використанні паперових документів, транспорту та зберігання матеріальних носіїв. Електронний документообіг та віртуалізація зберігання зменшують площі, необхідні для архівів, та знижують обсяг сміття, що генерується.

Таблиця 6.2 – Основні заходи запобігання забрудненню під час функціонування ІТ-системи

Захід	Напрямок дії	Очікуваний результат
Впровадження енергоефективного обладнання	Енергозбереження	Зменшення споживання електроенергії
Модернізація систем охолодження	Технічна інфраструктура	Зниження витрат на кондиціонування
Централізований збір електронних відходів	Утилізація	Унеможливлення потрапляння токсинів у природу
Перехід до електронного документообігу	Адміністративні процеси	Зниження використання паперу та витрат на логістику
Проведення еко-інструктажів для персоналу	Організаційний рівень	Формування культури екологічної відповідальності
Оптимізація програмного забезпечення	Зниження обчислювального навантаження	Менше навантаження на сервери та мережі

Таким чином, впровадження екологічно орієнтованих заходів не лише знижує негативний вплив на довкілля, а й підвищує репутацію організації, оптимізує витрати на енергоресурси та забезпечує відповідність чинним екологічним нормам і стандартам.

Висновок до розділу 6

У цьому розділі було досліджено екологічні аспекти впровадження та функціонування інформаційної підсистеми захисту корпоративних даних. Розглянуто основні джерела забруднення навколишнього середовища, що супроводжують роботу комп'ютерної техніки, серверного обладнання, систем зберігання даних, а також непрямі чинники, пов'язані з виробництвом, експлуатацією та утилізацією електронних компонентів.

Аналіз показав, що найбільший негативний вплив має енергоспоживання обладнання та неправильне поводження з електронними відходами. Використання морально застарілих пристроїв, неефективних систем охолодження, надмірного документообігу на паперових носіях, а також недотримання правил утилізації є серйозною загрозою для екологічного балансу.

Запропоновані в роботі заходи щодо зменшення негативного впливу передбачають впровадження енергоощадних технологій, організацію централізованого збору електронних відходів, перехід до цифрового середовища, автоматизацію процесів та підвищення екологічної обізнаності персоналу. Було сформовано таблицю практичних рішень щодо оптимізації функціонування системи без шкоди для довкілля.

ВИСНОВКИ

У результаті виконання дипломної роботи було повністю реалізовано проєкт створення інформаційної підсистеми для захисту корпоративних даних, яка відповідає сучасним вимогам безпеки, надійності та ефективності. Зростання обсягів і значення цифрових даних у діяльності організацій, поєднане з ризиками кібератак, витоку конфіденційної інформації та втрати контролю над внутрішніми інформаційними потоками, зумовлює актуальність таких систем. У зв'язку з цим дослідження питань розробки безпечного програмного забезпечення, здатного забезпечити захист корпоративних інформаційних ресурсів, є своєчасним та обґрунтованим.

На першому етапі роботи було проведено всебічний аналіз предметної області. Розглянуто ключові поняття, пов'язані з інформаційною безпекою, вивчено методи криптографічного захисту даних, а також визначено роль логування, моніторингу, доступу до ресурсів і контролю інцидентів у структурі сучасних безпекових систем. Було обґрунтовано вибір архітектурного підходу до побудови підсистеми, у тому числі концепцію "захисту за глибиною", модель "нульової довіри", використання SIEM, систем резервного копіювання, багаторівневої автентифікації, шифрування та централізованого управління політиками доступу. Окрема увага приділялася вимогам до надійності, масштабованості, підтримки хмарної інфраструктури та інтеграції з іншими інформаційними системами організації.

У другому розділі було розроблено концепцію застосунку та інформаційної системи. Визначено функціональні блоки, інтерфейси взаємодії, розглянуто моделі обміну інформацією між клієнтом, сервером і сховищем. Побудовано діаграми, які наочно демонструють архітектуру та принципи роботи розробленого застосунку. Зокрема, у діаграмі розгортання (рис. 3.1) було відображено взаємозв'язки між клієнтськими комп'ютерами, сервером додатка,

сервером бази даних, хмарним сховищем і SIEM-сервером. Така схема забезпечує логічну та фізичну відокремленість функцій, що підвищує захищеність системи та дозволяє гнучко масштабувати її залежно від змін у навантаженні або архітектурі підприємства.

Проведений аналіз технічних і програмних вимог до системи дозволив сформулювати чітке бачення щодо використання мов програмування, фреймворків, СУБД, інструментів моніторингу, засобів шифрування та аутентифікації. Було запропоновано використання сучасних інструментів і підходів, таких як JWT для токен-аутентифікації, TLS/SSL для передачі зашифрованих даних, AES-256 для шифрування сховищ і повідомлень, бібліотеки машинного навчання для виявлення аномалій. Технічні рішення були адаптовані до особливостей корпоративного середовища: підтримка хмарної інфраструктури, резервування даних, централізоване адміністрування та відповідність регуляторним вимогам (наприклад, ISO/IEC 27001).

На основі концепції було реалізовано прототип захисного застосунку, який включає компоненти для автентифікації користувачів, контролю доступу, шифрування даних, моніторингу активності та реагування на потенційні інциденти. Було розроблено й реалізовано архітектуру клієнт-серверного типу, яка забезпечує ізолюваність функцій, безпечний обмін даними, а також можливість розгортання у локальному, хмарному або гібридному середовищі. Програмні модулі реалізовано на базі мови Python з використанням фреймворку Flask для серверної частини, а також JavaScript і бібліотеки Axios для клієнтської взаємодії.

У четвертому розділі проведено техніко-економічне обґрунтування розробки. Було здійснено розрахунки витрат на проєктування, програмну реалізацію та впровадження системи. Розглянуто альтернативні варіанти впровадження, включаючи використання готових програмних рішень і open-source платформ. Розраховано коефіцієнт економічної ефективності, який

свідчить про переваги запропонованої системи у порівнянні з традиційними підходами щодо зниження фінансових ризиків, витрат на ліквідацію інцидентів та втрат через витоки даних. Підтверджено доцільність інвестування в подібні рішення з огляду на потенційне зростання рівня кібербезпеки підприємства.

У п'ятому розділі було проаналізовано фактори впливу на безпеку праці при експлуатації програмного забезпечення. Розглянуто питання освітлення, впливу електромагнітного випромінювання, електричного струму, виробничого шуму, мікроклімату та ергономіки робочого місця. Було запропоновано комплекс заходів, спрямованих на зниження впливу шкідливих чинників, зокрема встановлення джерел штучного освітлення, екранів для моніторів, шумопоглинаючих матеріалів та інших інженерно-організаційних рішень.

Останній розділ був присвячений охороні навколишнього середовища. Враховуючи зростаючі вимоги екологічного законодавства та політику екологічної відповідальності підприємств, було проаналізовано основні джерела забруднення та запропоновано ефективні заходи для його мінімізації. Серед них – цифровізація документообігу, оптимізація енергоспоживання, вторинна переробка обладнання та впровадження політик зеленої IT-інфраструктури.

Узагальнюючи результати виконаної дипломної роботи, можна стверджувати, що поставлені завдання були реалізовані повністю. Розроблена інформаційна підсистема захисту корпоративних даних відповідає сучасним вимогам безпеки, має чітко спроектовану архітектуру, високий рівень автоматизації процесів та економічну доцільність. Отримані результати можуть бути використані в реальних умовах для підвищення рівня захищеності інформаційних ресурсів організацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бондаренко В. С. Інформаційна безпека: підручник. – К.: КНЕУ, 2020. – 356 с.
2. Шевченко О. Ю. Системи захисту інформації в комп'ютерних мережах. – Львів: Видавництво ЛНУ, 2021. – 224 с.
3. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги.
4. Білецький С. О., Тихомиров А. В. Основи криптографії та захисту інформації. – Харків: ХНУРЕ, 2019. – 312 с.
5. Андрєєв Д. І. Основи технічного захисту інформації: навч. посіб. – Одеса: ОНПУ, 2018. – 174 с.
6. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls.
7. Stallings W. Cryptography and Network Security: Principles and Practice. – 8th ed. – Pearson, 2023. – 752 p.
8. Tanenbaum A. S., Wetherall D. J. Computer Networks. – 5th ed. – Pearson Education, 2021. – 960 p.
9. Чорній А. В. Програмна інженерія. – К.: НАУ, 2020. – 284 с.
10. ДСТУ 2861-94. Охорона праці. Терміни та визначення.
11. Микитенко В. І., Петренко Н. М. Охорона праці в галузі. – Київ: Кондор, 2021. – 296 с.
12. Сидоренко О. М. Економіка підприємства. – К.: Центр учбової літератури, 2019. – 368 с.
13. Чумаченко В. Г. Економічне обґрунтування проектів. – Харків: ХНЕУ, 2020. – 210 с.
14. Gai P., Kim S. Cloud Computing Security: Foundations and Challenges. – Springer, 2020. – 275 p.

15. Bishop M. Computer Security: Art and Science. – 2nd ed. – Addison-Wesley, 2020. – 1408 p.
16. Комарова Л. І. Основи інформаційної безпеки в ІТ-системах. – Київ: КНУ, 2018. – 192 с.
17. NIST SP 800-53 Rev.5: Security and Privacy Controls for Information Systems. – National Institute of Standards and Technology, 2020.
18. Задорожний Ю. П. Захист інформації в комп'ютерних системах. – Київ: Вид-во НАУ, 2021. – 176 с.
19. Європейський регламент GDPR (General Data Protection Regulation). Офіційний текст: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679>
20. Open Web Application Security Project (OWASP): <https://owasp.org>
21. Ковальчук І. В., Дмитренко І. О. Програмне забезпечення та бази даних. – Київ: КНЕУ, 2022. – 210 с.
22. Мережеві протоколи та архітектура. Cisco Academy. Навчальні матеріали: <https://www.netacad.com/>
23. Firebase documentation: <https://firebase.google.com/docs>
24. Django Security documentation: <https://docs.djangoproject.com/en/dev/topics/security/>
25. Flask Security Guide: <https://flask.palletsprojects.com/en/latest/security/>
26. SIEM Solutions Overview – IBM QRadar: <https://www.ibm.com/qradar>
27. Microsoft Azure Security Documentation: <https://learn.microsoft.com/en-us/security/azure/>
28. Apache Kafka Security Documentation: <https://kafka.apache.org/documentation/#security>
29. Програмна документація до бібліотеки Cryptography для Python: <https://cryptography.io/>
30. Python JWT Authentication – PyJWT: <https://pyjwt.readthedocs.io>

31. Elasticsearch та Kibana Documentation:
<https://www.elastic.co/guide/index.html>
32. Рекомендації щодо оцінки професійних ризиків – МОП:
<https://www.ilo.org>
33. Стандарти безпеки праці в ІТ: <https://dsp.gov.ua>
34. Розробка засобів захисту інформації. Методичні матеріали НАСА:
<https://ntrs.nasa.gov>
35. База знань з кіберзахисту від CERT-UA: <https://cert.gov.ua>

ДОДАТКИ

Додаток А Інструкція користувача

У цьому додатку наведено детальний опис взаємодії користувача з інформаційною підсистемою захисту корпоративних даних, а також роз'яснення щодо основних функцій, доступних у графічному інтерфейсі застосунку.

КРОК 1. Вступ до роботи з програмою

Після запуску застосунку користувач бачить головне вікно, яке містить поле авторизації. Для доступу до функціональності необхідно ввести облікові дані: **логін та пароль**. Якщо автентифікація проходить успішно, відкривається основний інтерфейс, який адаптується до ролі користувача (адміністратор або звичайний співробітник).

КРОК 2. Опис інтерфейсу після входу

Головне вікно містить панель навігації, яка дозволяє переходити між основними розділами системи: **«Користувачі»**, **«Пристрої»**, **«Моніторинг»**, **«Шифрування»**, **«Журнали подій»** та **«Аналітика»**. У правій частині вікна відображається інформація про поточного користувача та кнопка виходу з системи.

КРОК 3. Робота з користувачами та доступами

Для додавання нового користувача адміністратор натискає на пункт меню **«Користувачі»**, після чого відкривається форма з полями: ім'я, логін, пароль, роль. Після заповнення даних та натискання кнопки **«Зберегти»** новий користувач додається до системи. Зміна ролей та блокування також доступні через цей інтерфейс.

КРОК 4. Реєстрація та моніторинг пристроїв

У вкладці **«Пристрої»** адміністратор може зареєструвати новий пристрій, вказавши його тип, ідентифікатор та рівень безпеки. Після збереження пристрій з'являється в загальному списку. Система автоматично перевіряє відповідність політикам безпеки та відображає попередження у разі порушень. Користувач може переглянути список дозволених пристроїв, відключити небезпечні або ініціювати процедуру видалення даних.

КРОК 5. Шифрування даних

У розділі «Шифрування» користувач має можливість обрати файли, які потрібно зашифрувати. Після натискання кнопки «Додати файл» відкривається діалог вибору. Після вибору файлу активується кнопка «Шифрувати». Система застосовує алгоритм AES-256, і шифрований файл зберігається у вибраній директорії. Дешифрування виконується аналогічно, з попереднім введенням ключа доступу.

КРОК 6. Моніторинг та сповіщення

У розділі «Моніторинг» відображається активність користувачів у реальному часі. Вікно поділено на дві частини: зліва — фільтри та налаштування журналів, справа — таблиця подій. Підозрілі дії автоматично позначаються червоним кольором. У разі виявлення несанкціонованого входу або спроби доступу до захищених даних, система надсилає повідомлення адміністратору через вбудований центр сповіщень.

КРОК 7. Журнали подій та аналітика

У вкладці «Журнали» користувач може переглядати історію подій: вхід у систему, операції шифрування, зміни налаштувань, доступ до файлів. Доступна фільтрація за датою, IP-адресою, типом дії. У розділі «Аналітика» надаються графіки активності користувачів, топ-подій, підозрілі IP, завантаження системи тощо.

КРОК 8. Вихід із системи

Для завершення сеансу користувач натискає кнопку «Вийти», після чого система повертає його на вікно авторизації. Усі незбережені дії буде скасовано, а доступ до функцій буде обмежено.

КРОК 9. Завершення

У підсумку, запропонована інформаційна підсистема забезпечує інтуїтивну взаємодію користувача з усіма модулями захисту даних. Інструкція дозволяє швидко ознайомитися з функціоналом програми та гарантує правильне її використання в межах корпоративної політики безпеки.

Додаток Б Технічне завдання

№	Розділ ТЗ	Зміст
1	Найменування системи	Інформаційна підсистема захисту корпоративних даних
2	Підстава для розробки	Наказ про розробку, результати аналізу потреб підприємства
3	Мета і призначення	Забезпечення конфіденційності, цілісності та доступності даних у корпоративній мережі

№	Розділ ТЗ	Зміст
4	Функціональні вимоги	Аутентифікація, шифрування, моніторинг, управління доступом, резервне копіювання
5	Технічні вимоги	Сумісність з Windows/Linux, використання СУБД PostgreSQL, підтримка TLS, двофакторна автентифікація
6	Вимоги до інтерфейсу	Наявність веб-інтерфейсу для адміністратора, мобільної версії для співробітників
7	Умови експлуатації	Цілодобова робота, доступність 99,9%, резервування даних щогодини
8	Порядок контролю та приймання	Проведення модульного і функціонального тестування, звіти про тестування, акт прийому
9	Вимоги до персоналу	Необхідні знання з інформаційної безпеки, досвід з Linux-системами та Python/JS
10	Орієнтовні строки розробки	Початок – жовтень 2024, завершення – квітень 2025
11	Джерела фінансування	Внутрішні кошти підприємства або грантова підтримка

Додаток В Фрагмент програмного коду.

```

from werkzeug.security import generate_password_hash
from flask_sqlalchemy import SQLAlchemy
from flask_login import UserMixin
from datetime import datetime

db = SQLAlchemy()

class User(db.Model, UserMixin):
    __tablename__ = 'users'

    id = db.Column(db.Integer, primary_key=True)
    username = db.Column(db.String(50), unique=True, nullable=False)
    password_hash = db.Column(db.String(255), nullable=False)

    def __repr__(self):
        return f"<User {self.username}>"

class CorporateData(db.Model):
    __tablename__ = 'corporate_data'

    id = db.Column(db.Integer, primary_key=True)
    data = db.Column(db.Text, nullable=False)
    owner_id = db.Column(db.Integer, db.ForeignKey('users.id',
ondelete="CASCADE"), nullable=False)
    owner = db.relationship('User', backref=db.backref('corporate_data',
lazy=True))

    def __repr__(self):
        return f"<CorporateData owner_id={self.owner_id}>"

class UserLog(db.Model):
    """ Таблиця логування дій користувача """
    __tablename__ = 'user_logs'

```

```

        id = db.Column(db.Integer, primary_key=True)
        user_id = db.Column(db.Integer, db.ForeignKey('users.id',
ondelete="CASCADE"), nullable=False)
        action = db.Column(db.String(255), nullable=False) # Опис дії
        timestamp = db.Column(db.DateTime, default=datetime.utcnow) # Час виконання
дії

        user = db.relationship('User', backref=db.backref('logs', lazy=True))

        def __repr__(self):
            return f"<UserLog user_id={self.user_id}, action={self.action},
timestamp={self.timestamp}>"

# -----
# ФУНКЦІЯ ІНІЦІАЛІЗАЦІЇ ТА ДОДАВАННЯ ТЕСТОВИХ ДАНИХ
# -----

def init_db(app):
    with app.app_context():
        db.create_all()

        existing_user = User.query.first()
        if existing_user:
            print("База даних вже містить дані, пропускаємо ініціалізацію.")
            return

        print("База даних порожня. Додаємо тестові дані...")

        # Додавання тестового користувача
        test_user = User(username="test_user",
password_hash=generate_password_hash("password"))
        db.session.add(test_user)
        db.session.commit()

        # Додавання тестових корпоративних даних
        test_data = CorporateData(data="Зашифровані тестові дані",
owner_id=test_user.id)
        db.session.add(test_data)
        db.session.commit()
        test_data = CorporateData(data="Зашифровані тестові дані2",
owner_id=test_user.id)
        db.session.add(test_data)
        db.session.commit()
        test_data = CorporateData(data="Зашифровані тестові дані3",
owner_id=test_user.id)
        db.session.add(test_data)
        db.session.commit()
        test_data = CorporateData(data="Зашифровані тестові дані4",
owner_id=test_user.id)
        db.session.add(test_data)
        db.session.commit()
        test_data = CorporateData(data="Зашифровані тестові дані5",
owner_id=test_user.id)
        db.session.add(test_data)
        db.session.commit()

        print("Тестові дані створено успішно!")

from flask import Blueprint, render_template, request, redirect, url_for, flash
from werkzeug.security import generate_password_hash, check_password_hash
from flask_login import login_user, logout_user, login_required, current_user
from db import db, User

auth_bp = Blueprint('auth_bp', __name__)

```

```

@auth_bp.route('/login', methods=['POST', 'GET'])
def login():
    if request.method == 'POST':
        username = request.form['username']
        password = request.form['password']
        user = User.query.filter_by(username=username).first()
        if user and check_password_hash(user.password_hash, password):
            login_user(user)
            flash("Вхід успішний!")
            return redirect(url_for('main_bp.index'))
        else:
            flash("Невірні дані для входу.")
    return render_template('login.html')

@auth_bp.route('/logout')
@login_required # Потрібно бути авторизованим, щоб виконати вихід
def logout():
    logout_user()
    flash("Ви вийшли із системи.")
    return redirect(url_for('auth_bp.login'))

@auth_bp.route('/register', methods=['GET', 'POST'])
def register():
    if request.method == 'POST':
        username = request.form['username']
        password = request.form['password']

        # Перевірка, чи існує користувач із таким іменем
        existing_user = User.query.filter_by(username=username).first()
        if existing_user:
            flash("Користувач із таким ім'ям уже існує!")
            return redirect(url_for('auth_bp.register'))

        # Створюємо нового користувача
        new_user = User(
            username=username,
            password_hash=generate_password_hash(password)
        )
        db.session.add(new_user)
        db.session.commit()

        flash("Реєстрація успішна! Тепер ви можете увійти.")
        return redirect(url_for('auth_bp.login'))

    return render_template('register.html')

from flask import Blueprint, render_template, request, flash, redirect, url_for
from flask_login import login_required, current_user
from werkzeug.security import check_password_hash, generate_password_hash
from cryptography.fernet import Fernet

from db import db, CorporateData, UserLog

main_bp = Blueprint('main_bp', __name__)
cipher = Fernet(b'GhT39LXa7sOQbNp16ZfXtT9wGd2qJJK_3xGVoYkVX7c=')

def log_action(user_id, action):
    """ Функція запису дій користувача в лог """
    log_entry = UserLog(user_id=user_id, action=action)
    db.session.add(log_entry)
    db.session.commit()

@main_bp.route('/')
@login_required
def index():
    encrypted_data =
    CorporateData.query.filter_by(owner_id=current_user.id).all()

```

```

        for data in encrypted_data:
            try:
                data.decrypted_data = cipher.decrypt(data.data.encode()).decode()
            except Exception:
                data.decrypted_data = "[Помилка розшифрування]"

        return render_template('index.html', encrypted_data=encrypted_data)

@main_bp.route("/change_password", methods=["GET", "POST"])
@login_required
def change_password():
    """Зміна пароля користувача."""
    if request.method == "POST":
        current_password = request.form.get("current_password")
        new_password = request.form.get("new_password")
        confirm_password = request.form.get("confirm_password")

        if not check_password_hash(current_user.password_hash,
current_password):
            flash("Неправильний поточний пароль!", "danger")
        elif new_password != confirm_password:
            flash("Новий пароль та підтвердження не співпадають!", "danger")
        else:
            current_user.password_hash = generate_password_hash(new_password)
            db.session.commit()
            flash("Пароль успішно змінено!", "success")
            log_action(current_user.id, "Змінив пароль")
            return redirect(url_for("main_bp.index"))

    return render_template("change_password.html")

@main_bp.route('/delete/<int:data_id>', methods=['POST'])
@login_required
def delete_data(data_id):
    data = CorporateData.query.filter_by(id=data_id,
owner_id=current_user.id).first()
    if data:
        db.session.delete(data)
        db.session.commit()
        log_action(current_user.id, "Видалив зашифровані дані")
        flash("Запис успішно видалено!")
    else:
        flash("Помилка: запис не знайдено або у вас немає прав на його
видалення.")

    return redirect(url_for('main_bp.index'))

@main_bp.route('/encrypt', methods=['GET', 'POST'])
@login_required
def encrypt_data():
    if request.method == 'POST':
        raw_data = request.form['data']

        # Шифруємо дані
        encrypted_data = cipher.encrypt(raw_data.encode()).decode()

        # Зберігаємо у базу
        new_data = CorporateData(data=encrypted_data, owner_id=current_user.id)
        db.session.add(new_data)
        db.session.commit()

        log_action(current_user.id, "Зашифрував нові дані")

        flash("Дані успішно зашифровані та збережені!")
        return redirect(url_for('main_bp.index'))

```

```

        return render_template('encrypt.html')

# main.py
import os
from flask import Flask
from db import db, init_db
from flask_login import LoginManager
from db import User

from routes.auth import auth_bp
from routes.index import main_bp

def create_app():
    app = Flask(__name__)
    db_name = "shifr.db"
    app.secret_key = "some_very_secret_string"

    app.config["SQLALCHEMY_DATABASE_URI"] = f"sqlite:/// {db_name}"
    app.config["SQLALCHEMY_TRACK_MODIFICATIONS"] = False

    db.init_app(app)

    if not os.path.exists(db_name):
        print("База даних не знайдена. Створюємо нову...")
        init_db(app)
    else:
        with app.app_context():
            db.create_all()
            init_db(app)

    login_manager = LoginManager()
    login_manager.init_app(app)

    @login_manager.user_loader
    def load_user(user_id):
        return User.query.get(int(user_id))

    login_manager.login_view = "auth_bp.login"

    app.register_blueprint(auth_bp)
    app.register_blueprint(main_bp)

    return app

# Ось тут головне! Імпортуємо `app`, щоб PythonAnywhere його знайшов
app = create_app()

if __name__ == '__main__':
    app.run(debug=True)

```