НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет інформатики та обчислювальної техніки

Кафедра інформаційних систем та технологій

«На правах рукопису»
УДК _004.9_

До захисту допущено:
Завідувач кафедри
_____ Олександр РОЛІК
«___»_____2024 р.

Магістерська дисертація

на здобуття ступеня магістра

за освітньо-професійною програмою
«Інформаційні управляючі системи та технології»

зі спеціальності 126 «Інформаційні системи та технології»

на тему: «Система захищеного обміну інформацією в офісі»

Виконав:
студент 2 курсу, групи ІС-32мп
Миргородський Назар Володимирович _____

Керівник:
к.т.н., доцент
Голубєв Леонтій Петрович _____

Рецензент:
доцент каф.ІПІ , к.т.н., доцент
Баклан Ігор Всеволодович _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2024 року

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет інформатики та обчислювальної техніки

Кафедра інформаційних систем та технологій

Рівень вищої освіти – другий (магістерський)

Спеціальність – 126 «Інформаційні системи та технології»

Освітньо-професійна програма «Інформаційні управляючі системи та технології»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Олександр РОЛІК

«___»_____2024 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Миргородському Назару Володимировичу

1. Тема дисертації «Система захищеного обміну інформацією в офісі», науковий керівник дисертації Голубєв Леонтій Петрович, к.т.н. доц., затверджені наказом по університету від «08» 11 2024 р. № 5016-с

2. Термін подання студентом дисертації «09» 12 2024 р.

3. Об’єкт дослідження: Система захищеного обміну інформацією

4. Вихідні дані: система забезпечує швидкість відповіді до 1 секунди, підтримку до 100 запитів у секунду, безпеку персональних даних, інтеграцію з AI API

5. Перелік завдань, які потрібно розробити: провести аналіз існуючих рішень, спроєктувати архітектуру системи, реалізувати бек-енд та фронт-енд, провести тестування, підготувати текстову та графічну частину пояснювальної записки

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: діаграма процесу діяльності, діаграма варіантів використання, ER-діаграма бази даних, структурна схема, діаграма послідовності, діаграма об’єктів, діаграма пакетів серверної частини, діаграма класів

7. Орієнтовний перелік публікацій: не плануються

8. Дата видачі завдання 02.09.2024 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1.	Огляд літератури	09.09	
2.	Аналіз існуючих рішень	16.09	
3.	Дослідження методів шифрування та безпеки даних	23.09	
4.	Розробка концепції системи	30.09	
5.	Проектування та розробка архітектури системи	07.10	
6.	Розробка програмного інтерфейсу застосунку	21.10	
7.	Розробка системи шифрування	28.10	
8.	Розробка базового інтерфейсу користувача	04.11	
9.	Розробка інтеграції з AI	11.11	
10.	Оформлення документації	18.11	
11.	Подання роботи на попередній захист	25.11	
12.	Подання роботи на основний захист		

Студент Назар МИРГОРОДСЬКИЙ

Науковий керівник Леонтій ГОЛУБЄВ

РЕФЕРАТ

Система захищеного обміну інформацією в офісі: 112 с., 20 табл., 8 рис., 8 дод., 19 джерел.

ЗАХИЩЕНИЙ ОБМІН ДАНИМИ, КОРПОРАТИВНІ КОМУНІКАЦІЇ, ШТУЧНИЙ ІНТЕЛЕКТ, АВТОМАТИЗОВАНА ЗВІТНІСТЬ, ДВОШАРОВЕ ШИФРУВАННЯ.

В сучасних умовах цифрової трансформації бізнесу зростає потреба в захищених системах корпоративних комунікацій з розширеними можливостями аналізу та обробки інформації. Забезпечення конфіденційності даних при одночасному підвищенні ефективності комунікаційних процесів стає критично важливим завданням для організацій. Використання технологій штучного інтелекту відкриває нові можливості для автоматизації аналізу комунікацій та формування аналітичної звітності.

Метою роботи є розробка системи захищеного обміну інформацією в офісі з інтегрованими функціями автоматизованого аналізу комунікацій на основі технологій штучного інтелекту. Для досягнення мети були поставлені наступні задачі: провести аналіз існуючих рішень в області корпоративних комунікацій; розробити архітектуру системи з урахуванням вимог безпеки та масштабованості; реалізувати механізми двошарового шифрування даних; впровадити технології штучного інтелекту для аналізу комунікацій; розробити функціонал автоматизованого формування звітності.

Об'єктом дослідження є процеси захищеного обміну інформацією в корпоративному середовищі. Предметом дослідження виступають методи та технології забезпечення безпеки корпоративних комунікацій з використанням штучного інтелекту для аналізу даних.

Практична значимість роботи полягає у створенні готового до впровадження рішення, яке дозволяє організаціям підвищити ефективність внутрішніх комунікацій та процесів управління проєктами при забезпеченні високого рівня безпеки даних.

ABSTRACT

Secure office information exchange system: 112 p., 20 tab., 8 draw., 8 app., 19 sources.

SECURE DATA EXCHANGE, CORPORATE COMMUNICATIONS, ARTIFICIAL INTELLIGENCE, AUTOMATED REPORTING, TWO-LAYER ENCRYPTION.

In the current context of digital business transformation, there is a growing need for secure corporate communication systems with enhanced capabilities for information analysis and processing. Ensuring data confidentiality while increasing the efficiency of communication processes is becoming a critical task for organizations. The use of artificial intelligence technologies opens new opportunities for automating communication analysis and generating analytical reports.

The aim of the work is to develop a secure office information exchange system with integrated functions for automated communication analysis based on artificial intelligence technologies. To achieve this goal, the following tasks were set: to analyze existing solutions in the field of corporate communications; to develop system architecture taking into account security and scalability requirements; to implement two-layer data encryption mechanisms; to implement artificial intelligence technologies for communications analysis; to develop functionality for automated report generation.

The object of research is the processes of secure information exchange in the corporate environment. The subject of research is methods and technologies for ensuring the security of corporate communications using artificial intelligence for data analysis.

The practical significance of the work lies in creating a ready-to-implement solution that allows organizations to increase the efficiency of internal communications and project management processes while ensuring a high level of data security.

ЗМІСТ

ВСТУП

В сучасному бізнес-середовищі ефективна комунікація та управління інформацією стають ключовими факторами успіху організацій. Особливо актуальним це питання стає в умовах зростаючої цифровізації та переходу до віддаленої роботи, коли традиційні методи обміну інформацією та координації діяльності потребують суттєвого переосмислення та модернізації.

Сучасні організації генерують величезні обсяги даних через різноманітні канали комунікації - корпоративні чати, електронну пошту, системи обміну файлами. Ця інформація часто залишається розрізненою, що ускладнює її ефективне використання для прийняття управлінських рішень та моніторингу прогресу проєктів. Крім того, забезпечення безпеки корпоративних комунікацій та захист конфіденційної інформації стають все більш критичними завданнями в умовах зростання кіберзагроз.

Особливо гостро стоїть проблема систематизації та аналізу накопиченої інформації для формування регулярних звітів про стан проєктів та напрямків роботи. Керівники витрачають значний час на збір та узагальнення даних з різних джерел, що знижує ефективність управлінських процесів. При цьому традиційні методи роботи з інформацією часто не дозволяють виявити важливі тенденції та взаємозв'язки, які могли б допомогти в прийнятті більш обґрунтованих рішень.

З появою технологій штучного інтелекту відкриваються нові можливості для автоматизації процесів обробки та аналізу корпоративної інформації. Системи штучного інтелекту здатні обробляти великі обсяги неструктурованих даних, виділяти ключові тези та формувати змістовні узагальнення. Це дозволяє значно підвищити ефективність роботи з корпоративною інформацією та якість управлінської звітності.

Актуальність даної роботи обумовлена необхідністю створення комплексного рішення для організації захищених корпоративних комунікацій та автоматизованої обробки інформації з використанням технологій штучного інтелекту. Таке рішення дозволить організаціям оптимізувати внутрішні

комунікації, підвищити безпеку обміну даними та забезпечити більш ефективний контроль за реалізацією проєктів.

У контексті сучасних технологічних тенденцій, впровадження систем захищених комунікацій з елементами штучного інтелекту стає важливим фактором конкурентоспроможності організацій. Це дозволяє не лише оптимізувати внутрішні процеси, але й створити основу для подальшого розвитку та масштабування бізнесу в умовах цифрової економіки.

Важливим аспектом є також забезпечення гнучкості та масштабованості системи, можливості її адаптації до специфічних потреб різних організацій та інтеграції з існуючими корпоративними системами. При цьому особлива увага має приділятися питанням безпеки та захисту даних, включаючи шифрування комунікацій та управління правами доступу користувачів.

Система повинна забезпечувати не лише базовий функціонал захищених комунікацій, але й можливості для ефективної організації проєктної роботи, включаючи створення тематичних груп, управління доступом учасників та автоматизоване формування звітності. Використання технологій штучного інтелекту для аналізу накопиченої інформації дозволить суттєво підвищити якість та оперативність управлінської звітності.

Впровадження такої системи дозволить організаціям:

– забезпечити захищений обмін інформацією між співробітниками;

– оптимізувати процеси управління проєктами та контролю їх виконання;

– автоматизувати формування регулярної звітності;

– підвищити ефективність прийняття управлінських рішень;

– створити єдине захищене середовище для корпоративних комунікацій.

Метою даної роботи є створення інформаційної системи захищених корпоративних комунікацій з функціями автоматизованого аналізу інформації на основі технологій штучного інтелекту.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

– провести аналіз існуючих рішень в області корпоративних комунікацій та виявити їх основні недоліки;

– розробити архітектуру системи захищених комунікацій з урахуванням вимог до безпеки та функціональності;

– реалізувати механізми шифрування даних та управління правами доступу користувачів;

– інтегрувати технології штучного інтелекту для аналізу корпоративної інформації;

– розробити функціонал автоматизованого формування звітності;

– провести тестування системи та оцінити її ефективність.

Практична значимість роботи полягає у створенні готового до впровадження рішення, яке дозволить організаціям підвищити ефективність внутрішніх комунікацій та процесів управління проєктами. Використання сучасних технологій забезпечить високий рівень безпеки та зручності користування системою.

1 АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ

1.1 Microsoft Teams та Power BI

Microsoft Teams є однією з найпопулярніших платформ для корпоративних комунікацій, яка активно використовується організаціями по всьому світу. Ця система представляє собою комплексне рішення для організації робочого процесу, що включає в себе різноманітні інструменти для спілкування та співпраці. Основою платформи є функціонал миттєвих повідомлень, який дозволяє співробітникам обмінюватися текстовими повідомленнями, файлами та медіаконтентом у реальному часі.

Однією з ключових особливостей Microsoft Teams є можливість створення окремих каналів для різних проєктів або напрямків роботи. Це дозволяє структурувати комунікації та забезпечити зручний доступ до релевантної інформації для всіх учасників проєкту. В кожному каналі можна організовувати обговорення, зберігати важливі документи та налаштовувати інтеграції з іншими сервісами Microsoft 365.

Система надає розширені можливості для проведення відеоконференцій, що особливо актуально в умовах віддаленої роботи. Користувачі можуть організовувати як заплановані зустрічі, так і спонтанні відеодзвінки, використовувати функції демонстрації екрану та спільної роботи над документами. Вбудовані інструменти запису та транскрибації дозволяють зберігати важливу інформацію з онлайн-зустрічей для подальшого використання.

В контексті безпеки Microsoft Teams пропонує комплексний підхід до захисту даних. Усі комунікації захищені за допомогою сучасних протоколів шифрування, а система управління правами доступу дозволяє гнучко налаштовувати рівні доступу для різних користувачів та груп. Адміністратори можуть встановлювати політики безпеки, контролювати доступ до конфіденційної інформації та відстежувати активність користувачів.

Інтеграція з Power BI розширює можливості аналітики в Microsoft Teams. Power BI є потужним інструментом для візуалізації даних та створення

інтерактивних звітів. Користувачі можуть створювати детальні дашборди, які відображають ключові метрики та показники ефективності проєктів. Система підтримує роботу з різними джерелами даних та дозволяє налаштовувати автоматичне оновлення звітів [1].

Однак, незважаючи на широкі можливості, комбінація Microsoft Teams та Power BI має певні обмеження. Основним недоліком є відсутність вбудованих інструментів для автоматичного аналізу текстової інформації з чатів та обговорень. Хоча Power BI дозволяє створювати складні аналітичні звіти, він орієнтований переважно на структуровані дані і не має функціоналу для автоматичного узагальнення неструктурованої інформації з різних каналів комунікації.

Також варто відзначити, що процес налаштування аналітики в Power BI вимагає специфічних технічних знань та навичок. Для створення якісних звітів необхідно розуміти принципи роботи з даними, володіти навичками використання мови DAX та розуміти особливості візуалізації інформації. Це може створювати додаткові складнощі для організацій, які не мають відповідних спеціалістів.

Ще одним обмеженням є те, що хоча Microsoft Teams підтримує інтеграцію з різними сервісами, основний функціонал найкраще працює саме з продуктами екосистеми Microsoft. Це може створювати певні обмеження для організацій, які використовують інструменти від різних постачальників або мають специфічні вимоги до організації робочих процесів.

Система не передбачає автоматичного формування змістовних резюме по проєктах на основі аналізу всіх каналів комунікації. Хоча користувачі можуть створювати власні звіти та дашборди, відсутність автоматизованого AI-аналізу комунікацій значно обмежує можливості для оперативного моніторингу стану проєктів та прийняття управлінських рішень.

Таким чином, хоча Microsoft Teams у поєднанні з Power BI є потужним інструментом для організації корпоративних комунікацій та аналітики, це рішення не забезпечує повноцінної автоматизації процесів аналізу інформації та формування звітності, що є важливою вимогою для сучасних організацій.

1.2 Slack та Slack AI

Slack є однією з провідних платформ для командної співпраці, яка здобула широку популярність завдяки своєму інтуїтивному інтерфейсу та гнучким можливостям для організації комунікацій. Система побудована навколо концепції каналів, які можуть бути організовані за різними принципами – від проєктних команд до функціональних напрямків роботи. Такий підхід дозволяє ефективно структурувати комунікації та забезпечує легкий доступ до необхідної інформації.

Одним із ключових переваг Slack є розвинута система пошуку та архівування повідомлень. Вся історія комунікацій зберігається у доступному форматі, що дозволяє швидко знаходити потрібну інформацію навіть у старих обговореннях. Система підтримує розширений пошук з використанням фільтрів та операторів, що значно полегшує роботу з великими обсягами історичних даних.

Платформа пропонує широкі можливості для інтеграції з іншими сервісами та інструментами, що використовуються в організації. Завдяки великій кількості готових конекторів та відкритому API, Slack може стати центральним хабом для агрегації інформації з різних джерел – від систем управління проєктами до моніторингових інструментів. Це дозволяє користувачам отримувати важливі сповіщення та оновлення безпосередньо в робочому просторі Slack.

З точки зору безпеки, Slack забезпечує необхідний рівень захисту корпоративних комунікацій. Система підтримує шифрування даних, двофакторну автентифікацію та розширені можливості для управління правами доступу. Адміністратори можуть встановлювати політики безпеки та контролювати доступ до конфіденційної інформації на рівні окремих каналів та робочих просторів [2].

Нещодавно компанія представила Slack AI – набір інструментів штучного інтелекту, інтегрованих безпосередньо в платформу. Ця функціональність спрямована на підвищення продуктивності користувачів та автоматизацію рутинних завдань. Slack AI може автоматично узагальнювати довгі обговорення, виділяти ключові моменти та генерувати короткі резюме каналів.

Однак, незважаючи на інноваційність підходу, поточна реалізація AI-функціоналу в Slack має певні обмеження. По-перше, система здатна аналізувати лише інформацію, що міститься безпосередньо в каналах Slack, і не може автоматично агрегувати дані з інших джерел, таких як електронна пошта або документи, що зберігаються в інших системах. Це значно обмежує можливості для комплексного аналізу проєктної інформації.

Крім того, генерація резюме в Slack AI зосереджена переважно на узагальненні окремих обговорень або каналів, і не передбачає створення структурованих звітів про стан проєктів на основі аналізу всієї доступної інформації. Відсутня можливість налаштування специфічних шаблонів звітності або критеріїв аналізу відповідно до потреб конкретної організації.

Важливим обмеженням є також те, що Slack AI не надає інструментів для глибокого аналізу тенденцій та взаємозв'язків у комунікаціях. Система не може автоматично виявляти потенційні ризики, відслідковувати прогрес за ключовими показниками або генерувати прогнози на основі історичних даних. Це знижує її цінність як інструменту для підтримки прийняття управлінських рішень.

Варто відзначити і обмеження, пов'язані з масштабуванням системи. При збільшенні кількості каналів та користувачів може виникати складність у підтримці ефективної структури комунікацій. Відсутність автоматичних інструментів для категоризації та організації інформації може призводити до інформаційного перевантаження та зниження ефективності роботи.

З точки зору інтеграції з корпоративними процесами, Slack та Slack AI не забезпечують повноцінної підтримки складних робочих процесів, характерних для проєктного управління. Хоча система дозволяє організувати базові процеси узгодження та координації, вона не має вбудованих інструментів для управління завданнями, відслідковування дедлайнів та автоматизації рутинних операцій.

Таким чином, хоча Slack з інтегрованим AI-функціоналом є потужним інструментом для організації командної роботи, це рішення не забезпечує всіх необхідних можливостей для комплексного управління проєктною інформацією та автоматизованого формування аналітичної звітності. Організаціям, які потребують

більш глибокої інтеграції AI-технологій та автоматизації процесів аналізу інформації, може знадобитися додаткове програмне забезпечення або розробка власних рішень.

1.3 Zoom Team Chat та Zoom IQ

Zoom Team Chat, разом із інтегрованим AI-асистентом Zoom IQ, представляє собою комплексне рішення для організації корпоративних комунікацій, яке виросло з популярної платформи для відеоконференцій. Основною перевагою цього рішення є глибока інтеграція функціоналу обміну повідомленнями з можливостями відеозв'язку, що особливо актуально в умовах гібридного формату роботи. Система дозволяє безперешкодно переключатися між різними форматами комунікації – від текстових повідомлень до відеодзвінків – в рамках єдиного інтерфейсу.

Zoom Team Chat пропонує стандартний набір функцій для організації групової роботи, включаючи створення каналів, обмін файлами та можливість згадувати користувачів у повідомленнях. Особливістю платформи є тісна інтеграція з календарем та можливість планування зустрічей безпосередньо з чату, що спрощує координацію команди. Система також підтримує створення тематичних каналів для різних проєктів та напрямків роботи.

Впровадження Zoom IQ значно розширило можливості платформи в області автоматизації та аналітики. Цей AI-асистент спеціалізується на обробці та аналізі аудіо- та відеоконтенту, що генерується під час онлайн-зустрічей. Zoom IQ може автоматично створювати транскрипції розмов, виділяти ключові моменти обговорень та генерувати короткі підсумки зустрічей. Це особливо корисно для команд, які проводять багато часу у відеоконференціях та потребують ефективних інструментів для документування прийнятих рішень.

Важливою функцією Zoom IQ є можливість автоматичного аналізу настроїв та емоційного забарвлення комунікацій під час відеозустрічей. Система може відстежувати рівень залученості учасників, виявляти моменти напруги або незгоди,

що допомагає покращувати якість командної взаємодії. Крім того, AI-асистент може надавати рекомендації щодо покращення комунікативних навичок на основі аналізу стилю спілкування [5].

Однак, незважаючи на потужні можливості в області відеокомунікацій, система має ряд суттєвих обмежень. Перш за все, функціонал текстового чату в Zoom Team Chat є менш розвиненим порівняно з спеціалізованими месенджерами. Відсутні деякі важливі функції для організації асинхронної комунікації, такі як розширений пошук по історії повідомлень або можливість створення тематичних тредів у каналах.

Ще одним значним обмеженням є те, що Zoom IQ переважно фокусується на аналізі синхронних комунікацій (відеозустрічей) і має обмежені можливості для роботи з текстовою інформацією та документами. Система не може ефективно агрегувати та аналізувати дані з різних джерел, таких як електронна пошта, документи або сторонні системи управління проєктами. Це ускладнює формування цілісного уявлення про стан проєктів та обмежує можливості для комплексного аналізу інформації.

Суттєвим недоліком є також відсутність розвинутих інструментів для автоматизації робочих процесів та інтеграції з корпоративними системами. Хоча Zoom пропонує API для інтеграції, кількість готових конекторів та можливості для налаштування автоматизацій є досить обмеженими. Це може створювати складнощі для організацій, які потребують тісної інтеграції комунікаційної платформи з існуючими бізнес-процесами.

З точки зору формування аналітичної звітності, Zoom IQ також має певні обмеження. Хоча система може генерувати автоматичні резюме відеозустрічей, вона не надає інструментів для створення комплексних звітів про стан проєктів або аналізу тенденцій у командній роботі. Відсутня можливість налаштування специфічних метрик та показників ефективності відповідно до потреб конкретної організації.

Варто відзначити і питання, пов'язані з безпекою та конфіденційністю даних. Хоча Zoom пропонує стандартні механізми захисту інформації, деякі організації

можуть мати concerns щодо використання хмарного AI-сервісу для аналізу конфіденційних комунікацій. Система не передбачає можливості розгортання на власній інфраструктурі, що може бути критичним для організацій з високими вимогами до безпеки.

Крім того, функціонал Zoom IQ для аналізу комунікацій поки що знаходиться на ранній стадії розвитку і може мати обмеження в точності та релевантності генерованих підсумків. Система може пропускати важливі деталі або неправильно інтерпретувати контекст обговорень, що вимагає додаткової перевірки та редагування автоматично згенерованих матеріалів.

Таким чином, хоча комбінація Zoom Team Chat та Zoom IQ пропонує цікаві можливості для організації відеокомунікацій та їх автоматичного аналізу, це рішення не забезпечує повноцінної підтримки всіх аспектів корпоративних комунікацій та проєктної роботи. Організаціям, які потребують комплексного рішення для управління інформацією та автоматизованого формування аналітичної звітності, може знадобитися додаткове програмне забезпечення або розробка власних інструментів.

1.4 Mattermost

Mattermost представляє собою відкриту платформу для організації корпоративних комунікацій, яка відрізняється від інших рішень можливістю повного контролю над розгортанням та налаштуванням системи. Ця особливість робить Mattermost особливо привабливим для організацій, які мають високі вимоги до безпеки даних та потребують гнучкості в налаштуванні комунікаційної інфраструктури. Система може бути розгорнута як на власних серверах організації, так і в хмарному середовищі, що забезпечує максимальну гнучкість у виборі моделі розгортання.

Архітектура Mattermost побудована з урахуванням потреб великих організацій та забезпечує високу масштабованість системи. Платформа підтримує створення необмеженої кількості каналів та робочих просторів, що дозволяє

ефективно організувати комунікації навіть у великих розподілених командах. Система також забезпечує стабільну роботу при високих навантаженнях та має вбудовані механізми балансування навантаження.

Важливою перевагою Mattermost є розвинута система управління правами доступу та безпекою. Адміністратори мають можливість встановлювати детальні політики безпеки, включаючи вимоги до паролів, налаштування двофакторної автентифікації та обмеження доступу на рівні окремих каналів або груп користувачів. Система також підтримує інтеграцію з корпоративними системами автентифікації, такими як LDAP або Active Directory.

З точки зору користувацького досвіду, Mattermost пропонує інтуїтивно зрозумілий інтерфейс, який нагадує популярні месенджери. Платформа підтримує різні формати комунікації – від простого обміну повідомленнями до створення тематичних обговорень та спільної роботи над документами. Вбудована система пошуку дозволяє швидко знаходити потрібну інформацію в історії повідомлень.

Однією з сильних сторін Mattermost є можливість розширення функціоналу через систему плагінів та інтеграцій. Розробники можуть створювати власні розширення для додавання специфічного функціоналу або інтеграції з іншими корпоративними системами. Платформа має відкритий API, що дозволяє реалізовувати складні сценарії автоматизації та інтеграції [3].

Проте, незважаючи на гнучкість та розширюваність, Mattermost має суттєві обмеження в контексті автоматизованого аналізу інформації. Основним недоліком є відсутність вбудованих інструментів штучного інтелекту для обробки та аналізу комунікацій. Система не може автоматично генерувати резюме обговорень, виявляти ключові теми або формувати аналітичні звіти на основі накопиченої інформації.

Ще одним обмеженням є відсутність готових інструментів для проєктного управління та відслідковування прогресу робіт. Хоча базова функціональність може бути розширена за допомогою плагінів, створення комплексної системи управління проєктами вимагає значних зусиль з розробки та інтеграції додаткових компонентів.

Система також має обмежені можливості для роботи з різними типами контенту. Хоча Mattermost підтримує обмін файлами та базове форматування тексту, відсутні вбудовані інструменти для спільної роботи над документами або візуалізації даних. Це може створювати незручності для команд, які потребують тісної співпраці над складними документами або презентаціями.

З точки зору аналітики, Mattermost пропонує лише базові інструменти для збору статистики використання системи. Відсутні можливості для глибокого аналізу патернів комунікації, відслідковування ефективності командної роботи або автоматичного виявлення потенційних проблем у проєктах. Це обмежує можливості для прийняття обґрунтованих управлінських рішень на основі аналізу комунікаційних даних.

Варто також відзначити, що хоча відкритий характер платформи надає значні можливості для кастомізації, це також означає необхідність виділення ресурсів на підтримку та розвиток системи. Організації повинні мати власну команду технічних спеціалістів для забезпечення стабільної роботи платформи та розробки необхідних розширень.

Хоча Mattermost може бути хорошим вибором для організацій, які потребують повного контролю над своєю комунікаційною інфраструктурою, відсутність вбудованих інструментів для автоматизованого аналізу інформації та формування звітності робить це рішення менш привабливим для організацій, які прагнуть впровадити сучасні підходи до управління знаннями та проєктною інформацією. В таких випадках може знадобитися значна додаткова розробка або інтеграція з іншими системами для забезпечення необхідного функціоналу.

1.5 Symphony

Symphony є спеціалізованою платформою для захищених корпоративних комунікацій, яка була розроблена з урахуванням суворих вимог фінансового сектору до безпеки та відповідності регуляторним нормам. Ця система відрізняється від інших рішень своїм фокусом на забезпеченні максимального

рівня захисту конфіденційної інформації при збереженні зручності використання для кінцевих користувачів.

Архітектура Symphony побудована на принципах end-to-end шифрування, що забезпечує повну конфіденційність комунікацій між користувачами. Кожне повідомлення та файл, що передається через систему, автоматично шифрується з використанням унікальних ключів, доступ до яких мають лише авторизовані учасники комунікації. Така архітектура гарантує, що навіть у випадку компрометації серверної інфраструктури, зловмисники не зможуть отримати доступ до змісту повідомлень.

Особливу увагу в Symphony приділено відповідності регуляторним вимогам фінансової галузі. Система забезпечує повне протоколювання всіх дій користувачів, зберігання історії комунікацій відповідно до встановлених термінів та можливість проведення аудиту комунікацій. Платформа також підтримує складні політики управління доступом, що дозволяють точно контролювати, хто і яку інформацію може бачити та передавати [4].

З точки зору функціональності для кінцевих користувачів, Symphony пропонує широкий набір інструментів для організації комунікацій. Система підтримує створення групових чатів, тематичних каналів та приватних бесід. Користувачі можуть обмінюватися файлами, створювати опитування та використовувати розширене форматування повідомлень. Платформа також включає вбудовані інструменти для проведення захищених відеоконференцій.

Важливою особливістю Symphony є можливість інтеграції з іншими корпоративними системами через API та готові конектори. Це дозволяє автоматизувати робочі процеси та забезпечити безперебійний обмін інформацією між різними платформами, що використовуються в організації. Система також підтримує створення ботів та автоматизованих помічників для виконання рутинних завдань.

Проте, незважаючи на потужні можливості в області безпеки, Symphony має ряд суттєвих обмежень. Основним недоліком є відсутність розвинутих інструментів для автоматичного аналізу комунікацій та генерації аналітичних

звітів. Хоча система зберігає всю історію повідомлень, можливості для автоматизованого виявлення важливих тенденцій або формування змістовних резюме обговорень досить обмежені.

Платформа також не має вбудованих інструментів штучного інтелекту для обробки природної мови та аналізу контенту повідомлень. Це означає, що організації не можуть автоматично відстежувати ключові теми обговорень, виявляти потенційні ризики або генерувати структуровані звіти про стан проєктів на основі аналізу комунікацій.

З точки зору проєктного управління, Symphony пропонує досить базовий функціонал. Відсутні спеціалізовані інструменти для планування завдань, відстеження прогресу робіт або візуалізації проєктних даних. Хоча ці обмеження можуть бути частково компенсовані через інтеграцію з іншими системами, відсутність вбудованої підтримки проєктного управління може створювати незручності для команд.

Варто також відзначити високу вартість впровадження та підтримки Symphony, що обумовлено фокусом системи на фінансовий сектор та необхідністю забезпечення максимального рівня безпеки. Це може бути суттєвим бар'єром для організацій з обмеженим бюджетом, які шукають рішення для захищених корпоративних комунікацій.

Ще одним обмеженням є складність налаштування та адміністрування системи. Для ефективного використання всіх можливостей Symphony потрібна команда кваліфікованих технічних спеціалістів, які розуміють специфіку роботи з криптографічними системами та можуть забезпечити правильне налаштування політик безпеки.

Symphony також має обмежені можливості для кастомізації інтерфейсу та адаптації функціоналу під специфічні потреби організації. Хоча система підтримує створення власних розширень через API, процес розробки та впровадження нових функцій може бути досить складним через суворі вимоги до безпеки.

Таким чином, хоча Symphony є потужним рішенням для організацій, які потребують максимального рівня захисту комунікацій та відповідності

регуляторним вимогам, платформа має суттєві обмеження в контексті автоматизації аналізу інформації та підтримки проєктної роботи. Організаціям, які шукають комплексне рішення для управління корпоративними комунікаціями з можливостями AI-аналітики, може знадобитися додаткове програмне забезпечення або розробка власних інструментів.

1.5 Telegram Enterprise

Telegram Enterprise є корпоративною версією популярного месенджера Telegram, розробленою спеціально для бізнес-користувачів з урахуванням їхніх специфічних потреб у безпеці та управлінні комунікаціями. Ця платформа успадкувала всі переваги звичайного Telegram, такі як швидкість роботи, зручний інтерфейс та широкі можливості для обміну різними типами контенту, додавши до них розширені функції для корпоративного використання.

Однією з ключових особливостей Telegram Enterprise є розширена система управління користувачами та правами доступу. Адміністратори можуть створювати ієрархічні структури груп та каналів, що відповідають організаційній структурі компанії, та встановлювати детальні політики доступу для різних категорій користувачів. Це дозволяє забезпечити контрольований доступ до корпоративної інформації та ефективно управляти комунікаційними потоками.

Безпека в Telegram Enterprise реалізована на найвищому рівні завдяки використанню протоколу MTProto, який забезпечує надійне шифрування всіх комунікацій. Система підтримує end-to-end шифрування для секретних чатів, що гарантує повну конфіденційність особливо важливих обговорень. Крім того, платформа надає можливість встановлення додаткових налаштувань безпеки, таких як двофакторна автентифікація та обмеження на пересилання повідомлень [6].

Важливою перевагою Telegram Enterprise є можливість інтеграції з корпоративними системами через API. Платформа підтримує створення ботів та автоматизованих сервісів, які можуть виконувати різноманітні задачі – від простого

інформування про події до складної автоматизації бізнес-процесів. Розробники можуть використовувати Bot API для створення кастомізованих рішень, що відповідають специфічним потребам організації.

Система також пропонує потужні можливості для роботи з медіаконтентом. Користувачі можуть обмінюватися файлами різних форматів без обмежень на розмір, створювати голосові та відеоповідомлення, проводити групові відеоконференції. Вбудований редактор дозволяє форматувати текст, створювати опитування та використовувати інші інтерактивні елементи для підвищення ефективності комунікацій.

Однак, незважаючи на широкі можливості базового функціоналу, Telegram Enterprise має ряд суттєвих обмежень для використання як повноцінної системи корпоративних комунікацій. Головним недоліком є відсутність вбудованих інструментів для аналітики та обробки інформації. Система не має можливостей для автоматичного аналізу змісту повідомлень, виявлення важливих тем або генерації звітів на основі комунікаційних даних.

Ще одним значним обмеженням є відсутність спеціалізованих інструментів для проєктного управління. Хоча базова функціональність дозволяє організувати обговорення проєктів у групах та каналах, відсутні можливості для структурованого управління завданнями, відстеження прогресу робіт або автоматизованого збору статистики по проєктах.

Telegram Enterprise також не пропонує вбудованих інструментів для інтеграції з популярними корпоративними системами, такими як CRM або системи управління документами. Хоча такі інтеграції можливі через розробку власних ботів, це вимагає значних ресурсів на розробку та підтримку додаткового функціоналу.

З точки зору корпоративного управління, система має обмежені можливості для аудиту та контролю комунікацій. Відсутні інструменти для автоматичного моніторингу дотримання корпоративних політик або виявлення потенційних порушень безпеки. Це може створювати складнощі для організацій, які працюють

у регульованих галузях або мають високі вимоги до контролю інформаційних потоків.

Платформа також не підтримує створення складних робочих процесів або автоматизованих ланцюжків дій. Хоча боти можуть виконувати окремі автоматизовані операції, відсутня можливість налаштування комплексних сценаріїв обробки інформації або автоматичного розподілу завдань між учасниками проєктів.

Важливим обмеженням є також відсутність вбудованих інструментів для спільної роботи над документами. Користувачі можуть обмінюватися файлами, але відсутня можливість одночасного редагування документів або відстеження версій, що може створювати незручності при роботі над спільними проєктами.

Таким чином, хоча Telegram Enterprise пропонує надійну та зручну платформу для базових корпоративних комунікацій, вона має суттєві обмеження для використання як комплексного рішення для управління проєктною інформацією та автоматизації бізнес-процесів. Організаціям, які потребують розвинутих можливостей для аналізу комунікацій та автоматизованого формування звітності, може знадобитися впровадження додаткових систем або розробка власних рішень на базі Telegram API.

Висновки до розділу 1

Проведений аналіз існуючих рішень в області корпоративних комунікацій та управління інформацією виявив значний розрив між потребами сучасних організацій та можливостями доступних платформ. Хоча кожне з розглянутих рішень має свої сильні сторони, жодне з них не забезпечує повноцінної підтримки всіх аспектів корпоративних комунікацій з інтегрованими можливостями AI-аналітики та автоматизованого формування звітності.

Microsoft Teams у поєднанні з Power BI представляє собою потужне рішення для організації командної роботи та візуалізації даних, проте має обмежені можливості для автоматичного аналізу неструктурованої інформації з різних

каналів комунікації. Відсутність вбудованих інструментів для автоматичного узагальнення текстової інформації та формування змістовних звітів про стан проєктів значно обмежує можливості платформи для ефективного управління знаннями.

Slack, незважаючи на впровадження AI-функціоналу, також не забезпечує необхідного рівня автоматизації в обробці та аналізі проєктної інформації. Хоча Slack AI може генерувати короткі резюме окремих обговорень, система не здатна забезпечити комплексний аналіз інформації з різних джерел та формування структурованих звітів про стан проєктів. Це створює суттєві обмеження для організацій, які потребують глибокого розуміння процесів та автоматизованої підтримки прийняття рішень.

Zoom Team Chat з інтегрованим Zoom IQ демонструє інноваційний підхід до аналізу відеокомунікацій, проте має обмежені можливості для роботи з текстовою інформацією та документами. Фокус на синхронних комунікаціях та відсутність інструментів для комплексного аналізу проєктної інформації робить це рішення недостатнім для організацій, які потребують повноцінної підтримки всіх аспектів корпоративної взаємодії.

Mattermost, як відкрита платформа для корпоративних комунікацій, надає високу гнучкість у налаштуванні та розгортанні, проте відсутність вбудованих інструментів для AI-аналітики вимагає значних додаткових інвестицій у розробку необхідного функціоналу. Це може бути суттєвим бар'єром для організацій, які прагнуть швидко впровадити сучасні підходи до управління інформацією.

Symphony, орієнтована на фінансовий сектор, забезпечує найвищий рівень безпеки комунікацій, але має обмежені можливості для автоматизованого аналізу інформації та формування аналітичної звітності. Висока вартість впровадження та складність адміністрування також можуть бути суттєвими обмеженнями для багатьох організацій.

Telegram Enterprise, попри зручність використання та надійність базового функціоналу, не забезпечує необхідних можливостей для комплексного управління проєктною інформацією та автоматизації бізнес-процесів. Відсутність вбудованих

інструментів аналітики та обмежені можливості для інтеграції з корпоративними системами роблять це рішення недостатнім для організацій, які потребують глибокої автоматизації процесів обробки інформації.

Проведений аналіз також виявив загальні тенденції в розвитку систем корпоративних комунікацій, включаючи зростаючу роль штучного інтелекту в обробці інформації, підвищення вимог до безпеки даних та необхідність тісної інтеграції з існуючими бізнес-процесами. Однак існуючі рішення поки що не забезпечують оптимального балансу між цими вимогами.

Виявлені обмеження існуючих платформ підкреслюють актуальність розробки нового рішення, яке б забезпечувало комплексний підхід до організації корпоративних комунікацій з інтегрованими можливостями AI-аналітики. Таке рішення повинно поєднувати зручність використання, високий рівень безпеки та потужні інструменти для автоматизованого аналізу інформації та формування звітності.

Особливу увагу при розробці нового рішення необхідно приділити створенню гнучкої архітектури, яка дозволить легко адаптувати систему під специфічні потреби різних організацій, забезпечуючи при цьому високий рівень безпеки та ефективності обробки інформації. Важливим аспектом також є забезпечення простоти впровадження та використання системи, що дозволить організаціям швидко отримати практичну користь від впровадження нових технологій.

Таким чином, розробка нової системи корпоративних комунікацій з інтегрованими можливостями AI-аналітики є актуальним та перспективним напрямком, який дозволить задовольнити зростаючі потреби організацій у ефективному управлінні інформацією та автоматизації процесів прийняття рішень.

2 **ФОРМУВАННЯ ВИМОГ ДО СИСТЕМИ**

2.1 Функціональні вимоги

2.1.1 Вимоги до системи автентифікації та авторизації

Система автентифікації та авторизації є фундаментальним компонентом корпоративної комунікаційної платформи, що забезпечує контроль доступу та захист інформації. В контексті розроблюваної системи цей компонент повинен забезпечувати багаторівневий захист з урахуванням різних сценаріїв використання та потреб безпеки.

Основною вимогою до системи автентифікації є реалізація механізму JWT (JSON Web Tokens) через Spring Security. Система повинна генерувати захищені токени при успішній автентифікації користувача, які містять зашифровану інформацію про його ідентифікатор та права доступу. JWT-токени повинні мати обмежений термін дії та підписуватися секретним ключем для запобігання підробки.

Система повинна забезпечувати надійне зберігання облікових даних користувачів у базі даних PostgreSQL. Паролі користувачів повинні зберігатися виключно у вигляді захищених хешів з використанням сучасних алгоритмів хешування (наприклад, bcrypt). Важливо передбачити механізми захисту від атак перебором та обмеження кількості невдалих спроб входу.

В частині авторизації система повинна реалізовувати модель контролю доступу на основі ролей (RBAC) з можливістю тонкого налаштування прав для різних категорій користувачів. Права доступу повинні перевірятися на рівні API-ендпоінтів з використанням анотацій Spring Security. Система також повинна забезпечувати можливість динамічного управління правами доступу без необхідності перезавантаження сервера.

Система повинна забезпечувати безпечне з'єднання між клієнтом і сервером через протокол HTTPS. Додатково, для захисту обміну повідомленнями в реальному часі через Socket.IO, необхідно реалізувати двошарове шифрування:

– серверний рівень шифрування для повідомлень, що зберігаються в базі даних та потребують AI-аналізу;

– транспортний рівень шифрування для захисту даних під час передачі між клієнтом і сервером [14].

Кожен рівень шифрування повинен використовувати окремі ключі, при цьому транспортні ключі мають генеруватися динамічно для кожної сесії зв'язку.

Система також повинна забезпечувати механізми протоколювання всіх критичних операцій, пов'язаних з автентифікацією та авторизацією. Журнали безпеки повинні містити інформацію про всі спроби входу, зміни прав доступу та інші важливі події, зберігаючись у захищеному вигляді з можливістю подальшого аудиту.

Важливою вимогою є реалізація механізму управління сесіями користувачів. Система повинна підтримувати можливість примусового завершення сесій, автоматичного виходу при бездіяльності та обмеження кількості одночасних сесій для одного користувача. Необхідно також забезпечити коректну обробку завершення сесій WebSocket для підтримки актуального статусу підключення користувачів.

2.1.2 Вимоги до організації комунікацій

Організація ефективних комунікацій є центральним аспектом розроблюваної системи, що вимагає реалізації комплексного набору функціональних можливостей для забезпечення безперешкодного обміну інформацією між співробітниками організації. Система повинна підтримувати різноманітні формати комунікації та забезпечувати гнучкість у налаштуванні комунікаційних потоків.

В основі системи має лежати концепція тематичних робочих просторів, які відповідають різним проєктам або напрямкам діяльності організації. Кожен робочий простір повинен функціонувати як окреме середовище з власною структурою каналів комунікації та набором учасників. Система повинна

забезпечувати можливість створення необмеженої кількості робочих просторів та їх гнучкого налаштування відповідно до потреб конкретних проєктів.

У контексті текстових комунікацій система повинна підтримувати різні формати повідомлень, включаючи миттєві повідомлення, структуровані обговорення та тематичні треди. Важливо забезпечити можливість включення медіаконтенту.

Особливу увагу необхідно приділити організації групових обговорень. Система повинна підтримувати створення тематичних каналів з різними рівнями доступу, де учасники можуть обмінюватися інформацією та спільно працювати над завданнями. Важливо забезпечити можливість модерації обговорень, включаючи призначення модераторів та встановлення правил комунікації.

Додатково система повинна підтримувати механізми збору та аналізу зворотного зв'язку від користувачів щодо якості комунікацій та зручності використання платформи. Це дозволить постійно вдосконалювати систему та адаптувати її до потреб користувачів.

2.1.3 Вимоги до управління файлами та документами

Система управління файлами та документами є важливим компонентом корпоративної комунікаційної платформи, що забезпечує ефективну організацію та доступ до робочих матеріалів. В рамках розроблюваної системи цей компонент зосереджується на безпечному зберіганні та управлінні файлами без реалізації вбудованих механізмів перегляду документів.

Основною вимогою до системи управління файлами є забезпечення надійного та структурованого зберігання документів. Кожен робочий простір повинен мати власне файлове сховище, де документи організовуються відповідно до тематики проєкту або напрямку роботи. Система повинна підтримувати створення ієрархічної структури папок для логічної організації файлів та забезпечувати можливість гнучкого управління цією структурою.

Система повинна підтримувати завантаження файлів різних форматів та розмірів, забезпечуючи при цьому оптимальне використання серверних ресурсів. Необхідно реалізувати механізми контролю розміру файлів та перевірки їх на наявність шкідливого програмного забезпечення при завантаженні.

У контексті організації спільної роботи система повинна забезпечувати можливість швидкого обміну файлами між користувачами та групами. Користувачі повинні мати можливість легко ділитися документами в рамках робочих просторів та окремих обговорень, зберігаючи при цьому контроль над правами доступу до файлів.

В рамках управління життєвим циклом документів система повинна забезпечувати можливість встановлення термінів зберігання файлів та автоматичного архівування або видалення застарілих документів відповідно до корпоративних політик.

2.1.4 Вимоги до AI-аналітики та обробки даних

Інтеграція технологій штучного інтелекту для аналізу та обробки корпоративних комунікацій є ключовим компонентом розроблюваної системи. AI-аналітика повинна забезпечувати автоматизований аналіз інформації з різних каналів комунікації та формування структурованих звітів для підтримки прийняття управлінських рішень.

Система повинна забезпечувати автоматизований збір даних з усіх каналів комунікації, включаючи текстові повідомлення та файлові вкладення. Зібрана інформація повинна агрегуватися за тематичними напрямками та проєктами, забезпечуючи цілісне представлення всіх комунікацій в рамках кожної теми.

В контексті аналізу текстової інформації система повинна забезпечувати автоматичне виявлення ключових тем та трендів в обговореннях. AI-компонент повинен вміти визначати основні питання, що обговорюються, виділяти важливі рішення та відстежувати статус виконання завдань на основі аналізу комунікацій.

Особливу увагу необхідно приділити здатності системи розуміти контекст обговорень та визначати їх релевантність для різних проєктів.

Важливою вимогою є реалізація функціоналу автоматичного формування тижневих резюме по кожній темі або проєкту. AI-система повинна аналізувати всі комунікації за визначений період та генерувати структуровані звіти, що містять основні досягнення, проблеми, прийняті рішення та плани на майбутнє. Ці звіти повинні бути інформативними та придатними для використання керівниками проєктів без необхідності додаткової обробки.

Система повинна підтримувати можливість налаштування параметрів AI-аналізу відповідно до специфіки різних проєктів та організаційних потреб. Це включає визначення ключових метрик та показників, які повинні відстежуватися, налаштування форматів звітності та встановлення пріоритетів для різних типів інформації.

В рамках аналізу ефективності комунікацій AI-компонент повинен відстежувати патерни взаємодії між учасниками, виявляти потенційні проблеми в комунікації та надавати рекомендації щодо покращення процесів обміну інформацією. Система повинна автоматично виявляти ситуації, що потребують уваги керівництва, такі як затримки у відповідях на важливі повідомлення або відсутність прогресу в критичних обговореннях.

Особливу увагу необхідно приділити забезпеченню точності та релевантності AI-аналізу. Система повинна мати механізми валідації результатів аналізу та можливість коригування алгоритмів на основі зворотного зв'язку від користувачів. Важливо забезпечити прозорість процесу аналізу, щоб користувачі розуміли, на чому базуються висновки та рекомендації системи.

В контексті безпеки та конфіденційності AI-аналітика повинна враховувати встановлені права доступу та обмеження на використання інформації. Система повинна забезпечувати, що конфіденційна інформація не потрапляє у звіти, доступні користувачам без відповідних прав доступу.

Система повинна також підтримувати можливість експорту результатів AI-аналізу у різних форматах для подальшого використання в інших корпоративних

системах або для презентації керівництву. Це включає генерацію структурованих звітів у форматах PDF або отримання листа на пошту, а також можливість отримання даних через API для інтеграції з іншими аналітичними інструментами.

В рамках постійного вдосконалення AI-компонент повинен мати можливість навчатися на основі накопичених даних та адаптувати свої алгоритми для підвищення точності аналізу. Система повинна зберігати історію аналізу та використовувати цю інформацію для покращення майбутніх результатів.

Важливою вимогою є забезпечення швидкодії AI-аналізу та оптимального використання обчислювальних ресурсів. Система повинна забезпечувати своєчасну обробку великих обсягів даних без значного впливу на продуктивність інших компонентів платформи.

2.1.5 Вимоги до архівування інформації

Система архівування є критично важливим компонентом корпоративної комунікаційної платформи, що забезпечує довгострокове зберігання та доступність історичної інформації. В контексті розроблюваної системи архівування повинно забезпечувати надійне збереження всіх типів комунікаційних даних з можливістю їх подальшого відновлення та аналізу.

Система повинна автоматично архівувати всі комунікації, включаючи текстові повідомлення, електронні листи та файли, зберігаючи при цьому їх оригінальну структуру та метадані. Архівування має відбуватися в режимі реального часу, забезпечуючи збереження інформації одразу після її створення або модифікації. Особливу увагу необхідно приділити збереженню контексту комунікацій, включаючи зв'язки між повідомленнями та їх приналежність до конкретних проєктів або тем.

У контексті організації архівних даних система повинна забезпечувати структуроване зберігання інформації з можливістю її категоризації за різними параметрами. Архівні дані повинні автоматично індексуватися для забезпечення швидкого пошуку.

Система архівування повинна підтримувати політики зберігання даних відповідно до корпоративних вимог та регуляторних норм. Це включає можливість встановлення різних термінів зберігання для різних типів інформації та автоматичне видалення застарілих даних після закінчення встановленого терміну. При цьому важливо забезпечити можливість створення резервних копій критично важливої інформації перед її видаленням.

В контексті безпеки архівних даних система повинна забезпечувати надійне шифрування всієї архівної інформації та контроль доступу до неї. Доступ до архівних даних повинен надаватися тільки авторизованим користувачам відповідно до їх рівня доступу та службових обов'язків.

Особливу увагу необхідно приділити забезпеченню цілісності архівних даних. Система повинна гарантувати, що архівована інформація не може бути модифікована або видалена без відповідних повноважень.

Система повинна забезпечувати можливість експорту архівних даних у стандартних форматах для використання в інших системах або для довгострокового зберігання. Це включає підтримку різних форматів експорту та можливість вибіркового експорту даних за визначеними критеріями. При експорті повинна зберігатися вся необхідна метаінформація для забезпечення повноцінного відновлення даних у майбутньому.

В рамках оптимізації використання ресурсів система повинна підтримувати механізми стиснення архівних даних та управління дисковим простором. Важливо забезпечити баланс між ефективністю зберігання та швидкістю доступу до архівної інформації. Система повинна автоматично моніторити використання дискового простору та сповіщати адміністраторів про необхідність розширення сховища.

2.2 Нефункціональні вимоги

2.2.1 Вимоги до продуктивності та масштабованості

Для забезпечення ефективної роботи корпоративної комунікаційної системи критично важливо визначити чіткі метрики продуктивності та забезпечити можливості для масштабування відповідно до зростаючих потреб організації. Система повинна підтримувати стабільну роботу при збільшенні навантаження та забезпечувати оптимальне використання ресурсів.

В контексті швидкодії система повинна забезпечувати мінімальний час відгуку при виконанні основних операцій. Час відправки та отримання текстових повідомлень не повинен перевищувати 100 мілісекунд при нормальному навантаженні. Операції з файлами, такі як завантаження документів розміром до 10 МБ, повинні виконуватися не довше 3 секунд при стабільному мережевому з'єднанні.

Система повинна ефективно працювати при одночасному підключенні значної кількості користувачів. На початковому етапі необхідно забезпечити стабільну роботу для організацій з кількістю до 1000 активних користувачів, з можливістю подальшого масштабування. При цьому важливо підтримувати можливість одночасної роботи не менше 50% від загальної кількості користувачів без погіршення продуктивності системи.

В області обробки даних система повинна забезпечувати ефективну роботу з великими обсягами інформації. Швидкість індексації нових повідомлень та файлів повинна бути достатньою для забезпечення миттєвого пошуку по всьому масиву даних. Операції пошуку повинні виконуватися не довше 2 секунд, навіть при роботі з архівними даними за тривалий період.

Особливу увагу необхідно приділити оптимізації використання серверних ресурсів. Система повинна ефективно управляти пам'яттю та процесорним часом, не допускаючи надмірного споживання ресурсів окремими компонентами. Середнє використання CPU не повинно перевищувати 60% при нормальному навантаженні, з можливістю короткочасного збільшення до 80% при пікових навантаженнях.

В контексті масштабованості архітектура системи повинна підтримувати горизонтальне масштабування компонентів. Необхідно забезпечити можливість додавання нових серверів для розподілу навантаження без необхідності припинення роботи системи. Важливо реалізувати автоматичне балансування навантаження між серверами для забезпечення оптимальної продуктивності.

Система повинна підтримувати ефективне кешування даних для зменшення навантаження на базу даних та прискорення доступу до часто запитуваної інформації. Механізми кешування повинні автоматично адаптуватися до патернів використання системи, забезпечуючи оптимальне співвідношення між швидкістю доступу до даних та використанням ресурсів.

2.2.2 Вимоги до надійності та відмовостійкості

Основною вимогою до надійності системи є забезпечення показника доступності (uptime) на рівні не менше 99.9%, що відповідає максимальному часу простою близько 8.76 годин на рік. Для досягнення цього показника система повинна мати архітектуру, що виключає єдині точки відмови, та підтримувати автоматичне перемикання на резервні компоненти у разі виникнення збоїв.

Система повинна зберігати працездатність при відмові окремих компонентів інфраструктури. У разі виходу з ладу одного з серверів навантаження повинно автоматично перерозподілятися між іншими серверами без втрати даних та припинення обслуговування користувачів. Час перемикання на резервні компоненти не повинен перевищувати 30 секунд.

Система повинна коректно обробляти пікові навантаження, що перевищують звичайний рівень активності. При досягненні граничних значень навантаження система повинна автоматично обмежувати неприорітетні операції для забезпечення стабільної роботи критично важливих функцій. Важливо забезпечити прозоре інформування користувачів про можливі затримки в роботі системи.

В рамках забезпечення відмовостійкості важливо передбачити механізми автоматичного відновлення сесій користувачів після короткочасних збоїв у роботі

мережі. Система повинна зберігати стан користувацьких сесій та забезпечувати безшовне відновлення роботи після відновлення з'єднання без втрати даних та необхідності повторної автентифікації.

2.2.3 Вимоги до інтерфейсу користувача

Інтерфейс повинен забезпечувати інтуїтивно зрозумілий доступ до всіх функцій системи, одночасно підтримуючи високу продуктивність при виконанні щоденних завдань.

У контексті організації робочого простору інтерфейс повинен забезпечувати чітку візуальну ієрархію елементів та логічне групування функціональних компонентів. Основні елементи керування повинні бути легко доступними, а другорядні функції повинні бути згруповані в підменю для уникнення перевантаження інтерфейсу. Навігація між різними розділами системи повинна бути прозорою та потребувати мінімальної кількості дій від користувача.

Система повинна підтримувати адаптивний дизайн, що забезпечує коректне відображення інтерфейсу на різних пристроях та при різних роздільних здатностях екрану. Усі елементи інтерфейсу повинні масштабуватися відповідно до розміру екрану, зберігаючи при цьому функціональність та зручність використання. Особливу увагу слід приділити забезпеченню зручної роботи на мобільних пристроях.

В області візуального оформлення система повинна використовувати консистентну кольорову палітру та типографіку, що відповідає корпоративному стилю. Кольорові акценти повинні використовуватися помірно та цілеспрямовано для привертання уваги до важливих елементів інтерфейсу. Текстові елементи повинні мати достатній контраст із фоном для забезпечення легкості читання.

Система повинна надавати чіткий візуальний зворотний зв'язок на дії користувача. Усі інтерактивні елементи повинні мати явні стани наведення та активації, а виконання тривалих операцій повинно супроводжуватися

індикаторами прогресу. Важливо забезпечити інформативні повідомлення про помилки та підказки щодо їх виправлення.

В контексті доступності інтерфейс повинен відповідати стандартам WCAG 2.1 рівня AA. Система повинна підтримувати використання клавіатурної навігації та програм зчитування з екрану. Усі інтерактивні елементи повинні мати достатній розмір для зручного використання на сенсорних екранах, а інтервали між елементами повинні запобігати випадковим натисканням.

Особливу увагу необхідно приділити швидкодії інтерфейсу. Час відгуку на базові дії користувача не повинен перевищувати 100 мілісекунд для забезпечення відчуття миттєвої реакції. При виконанні складних операцій система повинна зберігати чуйність інтерфейсу та надавати користувачу можливість продовжувати роботу з іншими функціями.

2.2.4 Технічні вимоги до розгортання

Система повинна підтримувати гнучкі сценарії розгортання, забезпечуючи при цьому надійність та безпеку робочого середовища.

Серверна частина системи повинна підтримувати розгортання як у хмарному середовищі, так і на власній інфраструктурі організації. Для забезпечення стабільної роботи сервери повинні відповідати мінімальним технічним характеристикам: процесор з тактовою частотою не менше 2.5 GHz, оперативна пам'ять не менше 16 GB, та швидкий доступ до сховища даних з використанням SSD накопичувачів.

Система повинна підтримувати контейнеризацію з використанням Docker, що забезпечує ізоляцію компонентів та спрощує процес масштабування. Всі компоненти системи повинні бути оформлені у вигляді Docker-контейнерів з чітко визначеними залежностями та конфігураціями. Система повинна включати готові конфігурації для оркестрації контейнерів з використанням Docker Compose.

В контексті системи управління базами даних необхідно забезпечити підтримку PostgreSQL версії 12 або вище. База даних повинна бути налаштована

для роботи в режимі високої доступності з можливістю автоматичного відновлення після збоїв. Система повинна підтримувати автоматичне створення та застосування міграцій бази даних при оновленні версій.

Мережева інфраструктура повинна забезпечувати безпечне з'єднання між компонентами системи. Всі з'єднання повинні використовувати протокол HTTPS з дійсними SSL-сертифікатами.

Процес розгортання повинен бути максимально автоматизованим та підтримувати методологію безперервної інтеграції та доставки (CI/CD). Система повинна включати скрипти для автоматизації процесу встановлення та оновлення, а також інструменти для моніторингу стану розгортання. Важливо забезпечити можливість швидкого відкату до попередньої версії у разі виникнення проблем.

Система повинна підтримувати гнучке управління конфігурацією через змінні середовища та конфігураційні файли. Усі чутливі параметри, такі як ключі доступу та паролі, повинні зберігатися в захищеному сховищі секретів та підтримувати можливість ротації без переривання роботи системи.

В контексті резервного копіювання система повинна надавати інструменти для автоматизованого створення та відновлення резервних копій всіх компонентів, включаючи бази даних та файлові сховища. Процес резервного копіювання не повинен впливати на продуктивність системи та має підтримувати шифрування резервних копій.

Система повинна мати чітко визначені вимоги до середовища розробки, включаючи версії всіх залежностей та інструментів. Документація з розгортання повинна містити детальні інструкції щодо налаштування середовища розробки та процедур тестування перед розгортанням у продуктивне середовище.

2.2.5 Технічні вимоги аналізу текстових комунікацій

В контексті аналізу текстових комунікацій система повинна забезпечувати високу точність розпізнавання ключових тем та концепцій. Рівень точності визначення основних тем обговорення повинен становити не менше 95% для

загальних тематик та не менше 90% для спеціалізованих технічних обговорень. Система повинна коректно ідентифікувати контекст обговорень та зв'язки між різними темами навіть при використанні професійної термінології.

При формуванні тижневих резюме по проєктах система повинна забезпечувати високий рівень релевантності та інформативності. Згенеровані звіти повинні включати всі ключові події та рішення, прийняті протягом звітного періоду, з точністю відбору значущої інформації не менше 90%. Особливо важливо забезпечити точне визначення статусу завдань та проблем, що вимагають уваги керівництва.

Система повинна демонструвати високу якість обробки природної мови при роботі з текстами різних стилів та форматів. При аналізі неформальних комунікацій у чатах система повинна коректно інтерпретувати контекст повідомлень, враховуючи емоційне забарвлення та непрямі посилання. Точність розуміння контексту повідомлень повинна становити не менше 85%.

В області агрегації даних з різних джерел система повинна забезпечувати коректне об'єднання інформації та усунення дублювання. Важливо забезпечити точну ідентифікацію пов'язаних обговорень та документів, навіть якщо вони відбуваються в різних каналах комунікації. Рівень точності встановлення зв'язків між різними елементами інформації повинен становити не менше 90%.

Час обробки інформації AI-системою повинен відповідати вимогам оперативності. Генерація тижневого звіту по окремому проєкту не повинна перевищувати 5 хвилин, навіть при аналізі великого обсягу даних. При цьому система повинна забезпечувати стабільну якість аналізу незалежно від обсягу оброблюваної інформації.

У сфері виявлення критичних ситуацій та ризиків система повинна забезпечувати мінімальний рівень помилкових спрацьовувань. Частка помилкових позитивних результатів при виявленні потенційних проблем не повинна перевищувати 5%. При цьому система повинна виявляти не менше 95% реальних критичних ситуацій, що вимагають уваги.

Важливим аспектом є здатність системи до самонавчання та адаптації до специфіки конкретної організації. Система повинна демонструвати покращення точності аналізу мінімум на 5% протягом перших трьох місяців використання за рахунок накопичення та аналізу даних про паттерни комунікацій в організації.

В контексті обробки конфіденційної інформації система повинна забезпечувати повне дотримання встановлених політик безпеки. AI-аналіз повинен коректно обробляти обмеження доступу та не допускати витоку конфіденційної інформації через згенеровані звіти або рекомендації. Система повинна підтримувати можливість аудиту всіх операцій AI-аналізу для перевірки дотримання вимог безпеки.

Висновки до розділу 2

Проведений аналіз вимог до системи корпоративних комунікацій дозволив сформувати комплексне бачення функціональних та нефункціональних характеристик, необхідних для створення ефективного рішення. Визначені вимоги охоплюють всі ключові аспекти системи, від базової функціональності до технічних параметрів розгортання та експлуатації.

У розділі функціональних вимог було детально описано необхідні можливості системи, включаючи механізми автентифікації та авторизації, організацію комунікацій, управління файлами та документами, а також функціонал AI-аналітики. Особливу увагу було приділено вимогам до безпеки та захисту даних, що є критично важливим для корпоративної системи комунікацій.

Важливим аспектом функціональних вимог є забезпечення ефективної організації комунікацій через створення тематичних робочих просторів та підтримку різних форматів обміну інформацією. Система повинна надавати користувачам гнучкі інструменти для структурування та категоризації інформації, що дозволить підвищити ефективність командної роботи та проєктного управління.

В області нефункціональних вимог було визначено чіткі метрики продуктивності, масштабованості та надійності системи. Встановлені вимоги до

швидкодії та часу відгуку забезпечать комфортну роботу користувачів, а вимоги до масштабованості дозволять системі ефективно адаптуватися до зростаючих потреб організації.

Особливу увагу було приділено вимогам до якості AI-аналізу, що є ключовим компонентом системи. Встановлені критерії точності та релевантності результатів аналізу забезпечать високу цінність автоматично генерованих звітів та рекомендацій для користувачів системи. Важливим аспектом є також вимоги до прозорості процесу аналізу та можливості валідації результатів.

В контексті технічного розгортання було сформульовано чіткі вимоги до інфраструктури та процесів встановлення системи. Підтримка контейнеризації та автоматизації розгортання забезпечить гнучкість у виборі середовища функціонування та спростить процеси оновлення та масштабування системи.

Визначені вимоги до користувацького інтерфейсу забезпечать створення інтуїтивно зрозумілого та ефективного інструменту для щоденної роботи. Особлива увага до аспектів доступності та адаптивності дизайну дозволить забезпечити комфортне використання системи на різних пристроях та платформах.

Загалом, сформульовані вимоги створюють міцну основу для розробки високоякісної системи корпоративних комунікацій, що відповідає сучасним стандартам та потребам користувачів. Чітке визначення функціональних та нефункціональних характеристик дозволить забезпечити ефективну реалізацію системи та її успішне впровадження в організаціях різного масштабу.

3 МАТЕМАТИЧНЕ ЗАБЕЗПЕЧЕННЯ

3.1 Криптографічні основи двошарового шифрування

У системі захищеного обміну інформацією в офісі реалізовано двошарове шифрування для забезпечення максимального захисту даних. Перший рівень - серверне шифрування, використовує симетричний алгоритм AES (Advanced Encryption Standard) в режимі GCM (Galois/Counter Mode). Другий рівень - транспортне шифрування, забезпечує додатковий захист даних при їх передачі між клієнтом та сервером.

На серверному рівні використовується AES-256-GCM, де процес шифрування повідомлення M можна представити як послідовність математичних операцій. Спочатку повідомлення розбивається на блоки фіксованого розміру по 128 біт: $M = \{M_1, M_2, ..., M_n\}$

Для кожного блоку виконується шифрування з використанням ключа та лічильника CTR за формулою (3.1):

$$C_i = M_i \oplus AES(K, CTR + i), \quad (3.1)$$

де C_i - зашифрований блок, $\oplus$ - операція побітового додавання за модулем 2.

Особливістю режиму GCM є додаткове обчислення автентифікаційного тегу T за формулою (3.2), який забезпечує цілісність даних:

$$T = GHASH(H, C, A) \oplus E(K, J_0), \quad (3.2)$$

де $H = E(K, 0^{128})$, GHASH - спеціальна хеш-функція в полі Галуа $GF(2^{128})$, A - додаткові автентифікаційні дані, J_0 - початкове значення лічильника.

Для кожного сеансу зв'язку генерується за формулою (3.3) унікальний вектор ініціалізації IV довжиною 96 біт за допомогою криптографічно стійкого генератора випадкових чисел:

$$IV = CSPRNG(96). \quad (3.3)$$

Транспортний рівень шифрування використовує окремий набір ключів, які генеруються для кожної сесії. Процес генерації сесійного ключа K_s базується на алгоритмі Діффі-Хеллмана (3.4) з використанням еліптичних кривих (ECDH):

$$K_{\mathrm{s}} = ECDH(d_{\mathrm{a}}, Q_{\beta}) = ECDH(d_{\beta}, Q_{\mathrm{a}}) = d_{\mathrm{a}} d_{\beta} G, \quad (3.4)$$

де d_a, d_β - приватні ключі сторін, Q_a, Q_β - відповідні публічні ключі, G - генератор групи точок еліптичної кривої.

Фінальне шифрування повідомлення відбувається послідовним застосуванням обох рівнів шифрування за формулою (3.5):

$$C = E\_transport(E\_server(M, K_{\mathrm{server}}), K_{\mathrm{session}}), \quad (3.5)$$

де *E_server* та *E_transport* - функції шифрування відповідних рівнів.

Процес дешифрування на стороні отримувача виконується у зворотному порядку за формулою (3.6):

$$M = D\_server(D\_transport(C, K_{\mathrm{session}}), K_{\mathrm{server}}), \quad (3.6)$$

де *D_server* та *D_transport* - відповідні функції дешифрування.

Важливим аспектом є регулярна зміна ключів шифрування. Серверні ключі оновлюються за розкладом за формулою (3.7):

$$K_{\mathrm{nev}} = KDF(K_{\mathrm{urrent}} \,||\, salt \,||\, timestamp), \quad (3.7)$$

де *KDF* - функція виведення ключа, *salt* - випадкове значення, *timestamp* - часова мітка.

Така система двошарового шифрування забезпечує високий рівень захисту даних як при зберіганні, так і при передачі. Використання різних ключів та механізмів шифрування на кожному рівні створює додатковий захист від потенційних атак, оскільки компрометація одного рівня не призводить до компрометації всієї системи.

3.2 Автентифікація та управління доступом

У системі захищеного обміну інформацією в офісі механізм автентифікації та управління доступом базується на використанні JSON Web Token (JWT). JWT представляє собою компактний, самодостатній метод безпечної передачі інформації між сторонами у вигляді JSON об'єкта. Структура JWT складається з трьох частин: заголовка (header), корисного навантаження (payload) та підпису (signature).

Заголовок JWT містить інформацію про тип токена та алгоритм підпису. В системі використовується алгоритм HMAC-SHA256 для формування підпису. Математично заголовок можна представити як $H = Base64Url(\{\text{alg: HS256, typ: JWT}\})$, де *Base64Url* - функція кодування у Base64URL формат.

Корисне навантаження містить claims - твердження про користувача та додаткові дані. Основні claims включають ідентифікатор користувача, роль та час дії токена. Математично це представляється як:

P = Base64Url({
"sub": user_id,
"role": user_role,
"iat": issued_at,
"exp": expiration_time
})

Підпис токена обчислюється з використанням секретного ключа сервера за формулою (3.8):

$$S = HMACSHA256(H + "." + P, secret\_key), \quad (3.8)$$

де *HMACSHA256* - криптографічна хеш-функція з ключем.

Фінальний JWT токен формується конкатенацією всіх трьох компонентів: *JWT = H + "." + P + "." + Base64Url(S)*

При кожному запиті до системи відбувається валідація токена. Процес валідації включає перевірку підпису та часу дії токена. Для перевірки підпису сервер обчислює *S' = HMACSHA256(H + "." + P, secret_key)*

Токен вважається валідним, якщо виконується умова *S' = S*

Додатково перевіряється час дії токена: *current_time < expiration_time*

Для підвищення безпеки в системі використовується механізм ротації ключів підпису. Новий ключ генерується за формулою (3.9):

$$new\_key = HKDF(current\_key, salt, info), \quad (3.9)$$

де *HKDF* - функція виведення ключа на основі HMAC, *salt* - випадкове значення, *info* - контекстна інформація.

Для захисту від атак повторного використання токенів система підтримує blacklist недійсних токенів. При виході користувача з системи або зміні його прав доступу, відповідний токен додається до blacklist. Математично це можна представити як множину (3.10):

$$B = \{JWT_1, JWT_2, \ldots, JWT_n\}, \quad (3.1)$$

де JWT_i - недійсні токени.

Перед валідацією токена система перевіряє його відсутність у blacklist: $JWT \notin B$

Тільки після успішного проходження всіх перевірок система надає доступ до захищених ресурсів. Такий комплексний підхід до автентифікації забезпечує надійний захист від несанкціонованого доступу та різних видів атак на систему автентифікації [11].

Висновки до розділу 3

В даному розділі було детально розглянуто математичне забезпечення системи захищеного обміну інформацією в офісі. Зокрема, описано криптографічні основи двошарового шифрування та механізми автентифікації і управління доступом.

Розроблена система двошарового шифрування базується на використанні симетричного алгоритму AES-256-GCM на серверному рівні та механізму ECDH для транспортного рівня. Такий підхід забезпечує надійний захист даних як при зберіганні, так і при передачі. Важливим аспектом є регулярна ротація ключів шифрування, що реалізується через спеціальну функцію виведення ключів KDF.

Механізм автентифікації та управління доступом побудовано на основі JWT токенів з використанням алгоритму HMAC-SHA256 для формування підпису. Реалізовано валідацію терміну дії токенів та підтримку blacklist для недійсних токенів, що забезпечує надійний захист від несанкціонованого доступу.

Обрані математичні методи та алгоритми відповідають сучасним вимогам до безпеки корпоративних систем та створюють надійну основу для захищеного обміну інформацією. Використання перевірених криптографічних алгоритмів у поєднанні з власними механізмами управління ключами та токенами забезпечує високий рівень захисту даних у системі.

4 ПРОГРАМНЕ ТА ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ

4.1 Архітектура та інфраструктурні технології

Для реалізації системи захищеного обміну інформацією в офісі обрано розподілену архітектуру, що складається з незалежних компонентів, кожен з яких відповідає за окремий функціональний аспект системи. Такий підхід забезпечує гнучкість у розробці та масштабуванні окремих компонентів, а також дозволяє оптимізувати роботу кожного з них під конкретні задачі [15].

Основу системи формують два незалежних серверних додатки. Перший, реалізований на базі Spring Framework, забезпечує основну бізнес-логіку системи, включаючи автентифікацію користувачів, управління даними та взаємодію з базою даних. Spring Framework надає потужний набір інструментів для розробки корпоративних додатків, забезпечуючи високу надійність та безпеку системи. Цей компонент реалізує REST API для взаємодії з клієнтською частиною та відповідає за збереження даних у PostgreSQL [7].

Другий серверний додаток, побудований з використанням WebSocket.io, спеціалізується на забезпеченні комунікації в реальному часі між користувачами системи. Відокремлення WebSocket функціоналу в окремий сервіс дозволяє оптимізувати обробку великої кількості одночасних підключень та забезпечити ефективну маршрутизацію повідомлень між користувачами. Така архітектурна організація гарантує стабільну роботу системи навіть при значному збільшенні навантаження.

В якості системи управління базами даних використовується PostgreSQL, що забезпечує надійне та ефективне зберігання даних. PostgreSQL надає всі необхідні механізми для роботи з великими обсягами інформації, підтримує складні запити та транзакції, що критично важливо для корпоративної системи комунікацій. Особлива увага приділена організації структури бази даних для забезпечення швидкого доступу до історії повідомлень та ефективного пошуку в архівних даних.

Клієнтська частина системи реалізована з використанням React та являє собою окремий застосунок, що взаємодіє з обома серверними компонентами. React

забезпечує створення сучасного та інтуїтивно зрозумілого інтерфейсу користувача, ефективно обробляє динамічні дані та забезпечує responsive дизайн. Клієнтський додаток використовує REST API для отримання та оновлення даних, а також підтримує WebSocket з'єднання для обміну повідомленнями в реальному часі.

Безпека даних забезпечується через впровадження двошарової системи шифрування. Серверний рівень шифрування захищає дані при зберіганні та забезпечує можливість їх аналізу, в той час як транспортний рівень гарантує безпеку при передачі даних між компонентами системи. На серверному рівні використовуються криптографічні алгоритми для шифрування повідомлень перед їх збереженням у базі даних, що захищає інформацію навіть у випадку несанкціонованого доступу до сховища даних.

Транспортний рівень шифрування реалізує додатковий захист через використання унікальних ключів для кожної сесії зв'язку. Такий підхід забезпечує безпеку при передачі даних між клієнтом та сервером, гарантуючи, що навіть при перехопленні мережевого трафіку зловмисники не зможуть отримати доступ до змісту повідомлень.

Для забезпечення надійності та уніфікації середовища виконання використовується контейнеризація на основі Docker. Кожен компонент системи працює у власному контейнері, що забезпечує ізоляцію та спрощує процеси розгортання та масштабування. Docker контейнери гарантують однакове середовище виконання незалежно від інфраструктури, що значно спрощує процеси розробки, тестування та розгортання системи.

Обрана розподілена архітектура забезпечує необхідний рівень продуктивності, безпеки та надійності системи, створюючи міцну основу для подальшого розвитку та масштабування відповідно до зростаючих потреб користувачів. Використання сучасних технологій та перевірених архітектурних рішень гарантує стабільну роботу системи та можливість її адаптації до нових вимог бізнесу.

4.2 Серверні технології

Для реалізації серверної частини системи захищеного обміну інформацією в офісі використано комбінацію сучасних технологій, що забезпечують надійність, безпеку та високу продуктивність системи. Серверна частина розділена на два незалежних компоненти, кожен з яких оптимізований під свої специфічні задачі.

Основний серверний компонент реалізований з використанням Java 17 та Spring Framework 3, що забезпечує надійну та перевірену основу для розробки корпоративних додатків. Spring Boot значно спрощує процес розробки та конфігурації додатку, надаючи готові рішення для типових задач та автоматичне налаштування компонентів системи. Spring Security використовується для реалізації механізмів автентифікації та авторизації, зокрема для роботи з JWT токенами, що забезпечує безпечний доступ до системи [7].

Взаємодія з базою даних PostgreSQL реалізована через Spring Data JPA, що надає зручний об'єктно-орієнтований інтерфейс для роботи з даними. Використання Hibernate як ORM забезпечує ефективне відображення об'єктів Java на структури бази даних та автоматичне управління зв'язками між сутностями. Spring Data JPA також надає потужні можливості для створення запитів та управління транзакціями, що спрощує розробку складної бізнес-логіки [8].

REST API реалізовано за допомогою Spring Web MVC, що забезпечує створення RESTful веб-сервісів з підтримкою різних форматів даних та HTTP методів. Використання анотацій Spring суттєво спрощує процес розробки контролерів та обробку HTTP запитів. Для серіалізації та десеріалізації JSON використовується Jackson, що забезпечує гнучку роботу з даними та підтримку різних форматів.

Для забезпечення комунікації в реальному часі розроблено окремий серверний компонент на основі WebSocket.io. Цей компонент реалізує власний протокол обміну повідомленнями, що забезпечує ефективну двонаправлену комунікацію між клієнтами. WebSocket.io надає надійний механізм для роботи з

веб-сокетами, включаючи автоматичне відновлення з'єднання при розривах та оптимізацію використання мережевих ресурсів.

Важливим аспектом серверної реалізації є система шифрування даних. На серверному рівні використовується алгоритм AES для шифрування повідомлень перед їх збереженням у базі даних. Ключі шифрування зберігаються окремо від даних та управляються через спеціальний сервіс, що забезпечує їх безпечне використання та ротацію. Для транспортного рівня шифрування використовуються динамічно згенеровані ключі, унікальні для кожної сесії зв'язку.

Взаємодія між різними компонентами системи організована через чітко визначені інтерфейси, що забезпечує низьку зв'язність та високу модульність системи. Це дозволяє незалежно масштабувати та оновлювати різні частини системи без впливу на інші компоненти. Для забезпечення узгодженості даних між компонентами використовуються транзакції та механізми синхронізації.

В системі реалізовано комплексне логування та моніторинг з використанням SLF4J та Logback. Це дозволяє відстежувати роботу системи, виявляти потенційні проблеми та збирати метрики продуктивності. Всі критичні операції, особливо пов'язані з безпекою та обробкою даних, детально протоколюються для можливості подальшого аудиту.

Для оптимізації продуктивності використовується кешування на різних рівнях системи. Spring Cache з провайдером Caffeine застосовується для кешування часто запитуваних даних, що значно знижує навантаження на базу даних. Налаштовані пули з'єднань з базою даних та механізми connection pooling забезпечують ефективне використання ресурсів системи.

Важливою частиною серверної реалізації є система обробки помилок та виключних ситуацій. Реалізовано глобальну обробку винятків, що забезпечує коректне формування відповідей на помилки та їх належне протоколювання. Це дозволяє системі грамотно реагувати на різні проблемні ситуації та надавати користувачам зрозумілі повідомлення про помилки.

Вся серверна інфраструктура розгортається в Docker контейнерах, що забезпечує ізоляцію компонентів та спрощує процес розгортання. Використання

Docker дозволяє створити ідентичні середовища для розробки, тестування та продакшену, мінімізуючи можливі проблеми при розгортанні системи [12].

Така організація серверної частини забезпечує надійну та безпечну роботу системи, створюючи основу для подальшого розвитку та масштабування функціоналу відповідно до потреб користувачів. Використання сучасних технологій та перевірених архітектурних рішень гарантує високу продуктивність та стабільність роботи системи.

4.3 Технології безпеки

В системі захищеного обміну інформацією в офісі особлива увага приділяється безпеці даних та захисту від несанкціонованого доступу. Система безпеки побудована на сучасних технологіях та включає кілька рівнів захисту, що забезпечують комплексний підхід до забезпечення конфіденційності корпоративних комунікацій.

Автентифікація та авторизація користувачів реалізована з використанням Spring Security та механізму JWT (JSON Web Tokens). При успішній автентифікації користувача система генерує JWT токен, який містить інформацію про користувача та його права доступу. Всі подальші запити до системи повинні містити цей токен у заголовку для підтвердження прав доступу. Термін дії токенів обмежений, що зменшує ризики у випадку їх компрометації [11].

Особливістю системи є реалізація двошарового шифрування даних. Серверний рівень шифрування забезпечує захист повідомлень при їх зберіганні в базі даних. Для цього використовується симетричний алгоритм AES (Advanced Encryption Standard) у режимі GCM (Galois/Counter Mode). Ключі шифрування генеруються з використанням криптографічно стійкого генератора випадкових чисел та зберігаються окремо від зашифрованих даних. Важливо, що навіть при отриманні несанкціонованого доступу до бази даних, зловмисник не зможе прочитати зміст повідомлень без доступу до ключів шифрування.

Транспортний рівень шифрування реалізує захист даних під час їх передачі між клієнтом та сервером. Для кожної сесії зв'язку генерується унікальний ключ шифрування, який використовується для додаткового шифрування повідомлень. Це забезпечує захист від перехоплення даних при їх передачі через мережу, навіть якщо зловмисник отримає доступ до мережевого трафіку.

Процес відправки повідомлення включає послідовне застосування обох рівнів шифрування. Спочатку повідомлення шифрується серверним ключем, а потім додатково захищається транспортним шифруванням перед передачею по мережі. На серверній стороні відбувається розшифрування транспортного рівня, після чого повідомлення, все ще захищене серверним шифруванням, зберігається в базі даних.

Система управління доступом реалізована на основі ролей (RBAC - Role-Based Access Control), що дозволяє гнучко налаштовувати права користувачів. Кожен користувач може мати одну або декілька ролей, які визначають його можливості в системі. Перевірка прав доступу здійснюється на рівні контролерів за допомогою анотацій Spring Security, що забезпечує надійний контроль доступу до функціоналу системи.

Для захисту від поширених веб-вразливостей реалізовано комплекс заходів безпеки. Всі користувацькі паролі зберігаються у вигляді хешів, обчислених за допомогою алгоритму BCrypt з додаванням унікальної солі для кожного паролю. Система включає захист від SQL-ін'єкцій через використання параметризованих запитів та ORM, захист від XSS-атак через екранування спеціальних символів, та захист від CSRF-атак через генерацію та перевірку CSRF-токенів.

Всі компоненти системи регулярно оновлюються для усунення відомих вразливостей. Впроваджено процедури регулярного резервного копіювання даних та плани відновлення роботи системи у випадку збоїв або атак. Це забезпечує безперервність роботи системи та захист користувацьких даних.

Така комплексна система безпеки забезпечує надійний захист корпоративних комунікацій від різноманітних загроз, зберігаючи при цьому зручність використання системи для кінцевих користувачів. Постійний моніторинг та

вдосконалення механізмів безпеки дозволяють підтримувати високий рівень захисту даних відповідно до сучасних вимог інформаційної безпеки.

4.4 Комунікаційні технології

Комунікаційна складова системи захищеного обміну інформацією в офісі реалізована з використанням комбінації сучасних технологій, що забезпечують надійний та захищений обмін даними між користувачами. Основою комунікаційного стеку є поєднання REST API для стандартних операцій та WebSocket.io для обміну повідомленнями в реальному часі.

Для забезпечення стандартної взаємодії між клієнтом та сервером використовується REST API, реалізований за допомогою Spring Web MVC. Цей інтерфейс забезпечує базові операції системи, такі як автентифікація користувачів, управління профілями, отримання історії повідомлень та інші операції, що не вимагають миттєвої передачі даних. REST API працює через захищене HTTPS з'єднання, що забезпечує базовий рівень захисту даних при передачі.

Ключовим компонентом системи є окремий сервер WebSocket.io, що забезпечує обмін повідомленнями в реальному часі. Цей сервер підтримує постійне з'єднання з клієнтами та забезпечує миттєву доставку повідомлень. WebSocket.io був обраний через його надійність, ефективність та вбудовану підтримку автоматичного відновлення з'єднання при втраті зв'язку.

Процес обміну повідомленнями організований наступним чином: коли користувач надсилає повідомлення, воно спочатку проходить через механізми шифрування на клієнтській стороні. Зашифроване повідомлення передається через WebSocket з'єднання на сервер, де воно зберігається в базі даних PostgreSQL. Одночасно система надсилає повідомлення всім активним учасникам чату через WebSocket канали.

При підключенні користувача до чату система автоматично завантажує історію повідомлень з бази даних через REST API. Це дозволяє користувачам бачити попередні повідомлення та контекст обговорень.

Важливим аспектом комунікаційної системи є обробка статусів користувачів. WebSocket сервер відстежує підключення та відключення користувачів, оновлює їх статуси та сповіщає інших учасників чату про зміни. Це дозволяє користувачам бачити, хто зараз онлайн та доступний для спілкування.

Система також підтримує передачу файлів між користувачами. Для цього використовується окремий механізм, що забезпечує безпечне завантаження та зберігання файлів. Файли шифруються перед збереженням та передаються через захищене з'єднання, забезпечуючи конфіденційність переданих даних.

Така організація комунікаційних технологій забезпечує надійну та ефективну роботу системи, створюючи комфортне середовище для корпоративного спілкування з гарантією безпеки та конфіденційності даних. Комбінація REST API та WebSocket.io дозволяє оптимально вирішувати різні комунікаційні задачі, забезпечуючи при цьому високу продуктивність та стабільність роботи системи.

4.5 Технології користувацького інтерфейсу

Користувацький інтерфейс системи захищеного обміну інформацією в офісі реалізовано з використанням сучасного стеку веб-технологій, де основою виступає бібліотека React. Такий вибір обумовлений необхідністю створення динамічного та інтерактивного інтерфейсу, здатного ефективно працювати з даними в реальному часі та забезпечувати комфортну роботу користувачів.

React забезпечує компонентний підхід до розробки інтерфейсу, що дозволяє створювати перевикористовувані елементи та підтримувати чітку структуру коду. Кожен елемент інтерфейсу, від простих кнопок до складних діалогових вікон, реалізований як окремий компонент з власною логікою та станом. Це спрощує розробку, тестування та подальшу підтримку системи.

Для управління станом додатку використовується глобальне сховище Redux. Воно забезпечує централізоване зберігання даних про поточний стан чатів, користувачів, повідомлень та інших елементів системи. Redux особливо ефективний для синхронізації даних між різними компонентами та обробки

асинхронних операцій, таких як відправка повідомлень або завантаження історії чату [13].

Взаємодія з серверною частиною через REST API реалізована за допомогою Axios. Ця бібліотека забезпечує зручний інтерфейс для виконання HTTP-запитів та обробки відповідей. Для роботи з WebSocket з'єднаннями використовується Socket.IO-client, що забезпечує надійний двосторонній зв'язок з сервером та автоматичне відновлення з'єднання при втраті зв'язку.

Для створення адаптивного дизайну використовується CSS-in-JS підхід з використанням Styled Components. Це дозволяє створювати стилізовані компоненти, які легко модифікуються та перевикористовуються. Інтерфейс адаптується під різні розміри екранів та забезпечує комфортну роботу як на десктопних, так і на мобільних пристроях [16].

Особлива увага приділена реалізації чату як основного елементу інтерфейсу. Чат підтримує відображення різних типів повідомлень, включаючи текстові повідомлення, файли та системні сповіщення. Реалізовано механізми автоматичного прокручування до нових повідомлень, підвантаження історії при прокручуванні вгору та індикації статусу доставки повідомлень.

Для оптимізації продуктивності використовується віртуалізація списків, що дозволяє ефективно відображати великі обсяги даних без втрати продуктивності.

Безпека на рівні інтерфейсу забезпечується через реалізацію механізмів валідації введених даних, захист від XSS-атак та безпечне зберігання чутливих даних. Всі операції з криптографічними ключами виконуються в захищеному контексті, а чутливі дані ніколи не зберігаються в відкритому вигляді.

Для покращення продуктивності застосовано ряд оптимізацій, включаючи ліниве завантаження компонентів, кешування даних на клієнтській стороні та оптимізацію рендерингу React-компонентів. Це забезпечує швидку роботу інтерфейсу навіть при великій кількості активних чатів та повідомлень.

Розроблений користувацький інтерфейс забезпечує інтуїтивно зрозумілу та ефективну роботу з системою, поєднуючи сучасний дизайн з високою функціональністю та безпекою. Використання актуальних веб-технологій дозволяє

підтримувати високу продуктивність та забезпечувати позитивний користувацький досвід при роботі з системою.

4.6 Технології штучного інтелекту та обробки даних

Для забезпечення інтелектуальної обробки комунікаційних даних в системі використовується Google Gemini API - потужний інструмент штучного інтелекту нового покоління. Вибір цієї технології обумовлений її широкими можливостями для аналізу тексту, генерації контенту та здатністю розуміти контекст комунікацій [9].

Інтеграція з Gemini API реалізована через REST API з використанням Spring Framework. При обробці повідомлень система виконує автоматичний аналіз контенту для формування змістовних звітів та узагальнень. Важливим аспектом є те, що аналіз повідомлень відбувається лише після їх розшифрування на серверному рівні, що забезпечує конфіденційність даних при збереженні можливості їх аналізу.

Система використовує Gemini API для декількох ключових функцій. Основною є автоматична генерація тижневих звітів по кожному проєкту або напрямку роботи. AI-модель аналізує всі повідомлення за визначений період, виділяє ключові теми обговорень, важливі рішення та проблемні питання. На основі цього аналізу формується структурований звіт, який надає керівникам чітке розуміння прогресу та стану справ.

Для забезпечення якості аналізу розроблено спеціалізовані промпти, які направляють роботу AI-моделі та забезпечують генерацію релевантної інформації. Система враховує контекст обговорень, зв'язки між повідомленнями та їх важливість для формування повної картини комунікацій. При цьому особлива увага приділяється фільтрації неважливої інформації та виділенню дійсно значущих моментів.

Для забезпечення конфіденційності при використанні AI реалізовано механізми анонімізації даних перед їх передачею до Gemini API. Система

автоматично видаляє або маскує персональні дані, конфіденційну інформацію та інші чутливі дані, забезпечуючи відповідність вимогам безпеки при збереженні якості аналізу.

Важливим компонентом є система зворотного зв'язку, яка дозволяє користувачам оцінювати якість згенерованих звітів та вносити корективи. Ці оцінки використовуються для вдосконалення промптів та налаштування параметрів аналізу, що дозволяє постійно підвищувати якість роботи AI-компонента.

Обробка та аналіз даних в системі не обмежується лише текстовим аналізом. Реалізовано також збір та аналіз метрик активності користувачів, статистики використання системи та інших кількісних показників. Ці дані використовуються для оптимізації роботи системи та формування аналітичних звітів про ефективність комунікацій.

Така інтеграція технологій штучного інтелекту в систему корпоративних комунікацій створює потужний інструмент для автоматизації процесів аналізу інформації та підтримки прийняття управлінських рішень. Постійний розвиток можливостей Gemini API та вдосконалення механізмів його використання дозволяють системі адаптуватися до нових потреб користувачів та забезпечувати все більш якісну аналітику комунікаційних даних.

4.7 Інтеграційні технології

Для забезпечення ефективної взаємодії між різними компонентами системи та можливості підключення зовнішніх сервісів реалізовано комплекс інтеграційних технологій. Основою інтеграційного шару є REST API, розроблений з використанням Spring Web MVC, що забезпечує стандартизований інтерфейс для взаємодії з системою.

REST API системи побудовано згідно з принципами RESTful архітектури та документовано за допомогою OpenAPI Specification (Swagger). Кожен endpoint має чітко визначений формат запитів та відповідей, що спрощує процес інтеграції та

розробки клієнтських додатків. API підтримує різні HTTP методи (GET, POST, PUT, DELETE) для виконання операцій з ресурсами системи.

Для забезпечення безпечної інтеграції реалізовано механізм JWT автентифікації. Кожен запит до API повинен містити валідний JWT токен у заголовку, що дозволяє ідентифікувати користувача та перевірити його права доступу. Токени мають обмежений термін дії та можуть бути відкликані адміністратором системи у разі необхідності.

Особливу роль в системі відіграє інтеграція з Gemini API для забезпечення функцій штучного інтелекту. Взаємодія з API реалізована через HTTP клієнт з використанням бібліотеки Axios. Система управляє квотами запитів, обробляє помилки та забезпечує retry-механізми для підвищення надійності взаємодії з зовнішнім API.

Для забезпечення обміну повідомленнями в реальному часі використовується окремий WebSocket сервер на базі Socket.io. Взаємодія між основним сервером та WebSocket сервером організована таким чином, щоб забезпечити надійну доставку повідомлень та синхронізацію даних між компонентами системи [10].

Важливим аспектом є інтеграція з базою даних PostgreSQL, яка реалізована через Spring Data JPA. Це забезпечує об'єктно-реляційне відображення та надає зручний інтерфейс для роботи з даними. Система підтримує транзакційність операцій та забезпечує цілісність даних при взаємодії різних компонентів.

Для забезпечення можливості масштабування та моніторингу система включає механізми збору метрик та логування. Використовується комбінація Logback для збору логів та Prometheus для збору метрик продуктивності. Це дозволяє відслідковувати стан системи та оперативно реагувати на можливі проблеми.

Така організація інтеграційних технологій забезпечує надійну взаємодію всіх компонентів системи та створює основу для подальшого розширення функціоналу через підключення нових сервісів та інтеграцій. Використання стандартних протоколів та форматів даних спрощує процес розробки та підтримки системи.

4.8 Діаграма діяльності

Діаграма діяльності відображає процес обміну повідомленнями в чаті системи захищеного обміну інформацією в офісі. Вона демонструє взаємодію між клієнтом, REST API та WebSocket сервером.

Процес починається з авторизації користувача через REST API. Для цього клієнт надсилає серверу логін та пароль. Сервер перевіряє отримані дані на відповідність збереженим у системі. Якщо логін та пароль збігаються, сервер генерує JWT токен і відправляє його клієнту, сигналізуючи про успішну авторизацію. У випадку, якщо дані не збігаються, сервер надсилає клієнту повідомлення про помилку, і процес авторизації завершується.

Після успішної авторизації клієнт намагається встановити WebSocket з'єднання із сервером. Сервер перевіряє валідність отриманого від клієнта JWT токена. Якщо токен є дійсним, сервер встановлює з'єднання та надсилає клієнту підтвердження про успішне встановлення з'єднання. Клієнт, отримавши це підтвердження, надсилає серверу запит на отримання історії повідомлень чату. Сервер здійснює пошук відповідних повідомлень у базі даних і відправляє їх клієнту, який, отримавши повідомлення, розшифровує їх та відображає користувачу [19].

Коли користувач створює нове повідомлення, клієнт спочатку шифрує його за допомогою транспортного ключа. Потім зашифроване повідомлення відправляється на сервер через встановлене WebSocket з'єднання. Сервер, отримавши повідомлення, розшифровує його транспортним ключем, а потім шифрує серверним ключем перед збереженням у базі даних. Після успішного збереження сервер шифрує повідомлення транспортним ключем і відправляє його всім клієнтам, підключеним до відповідного чату [18].

Клієнти, отримавши нове повідомлення, розшифровують його спочатку транспортним ключем, а потім серверним. Розшифроване повідомлення відображається користувачу в чаті.

Таким чином, діаграма діяльності ілюструє повний цикл обміну повідомленнями в системі захищеного обміну інформацією в офісі. Вона охоплює процеси авторизації користувача, встановлення WebSocket з'єднання, отримання історії повідомлень та відправки нових повідомлень з урахуванням двошарового шифрування для забезпечення безпеки комунікації.

Діаграма діяльності наведена у додатку А.

4.9 Діаграма варіантів використання

Діаграма варіантів використання відображає функціональні можливості системи захищеного обміну інформацією в офісі з точки зору трьох основних типів користувачів: адміністратора, менеджера та звичайного користувача.

Адміністратор, після успішної авторизації в системі, отримує можливість управляти користувачами. Це включає в себе реєстрацію нових користувачів, зокрема менеджерів, а також редагування та видалення існуючих облікових записів. Адміністратор має найвищий рівень доступу і відповідає за підтримку та керування системою в цілому.

Менеджер, авторизувавшись у системі, має змогу створювати нові департаменти та проєкти. Він відповідає за структурування та організацію робочих процесів у системі. Для кожного нового проєкту менеджер може створювати чати, призначені для комунікації між членами проєктної команди. Менеджер також має можливість додавати користувачів до відповідних департаментів та призначати їх на проєкти. Також менеджер може створювати та відправляти звіти, пов'язані з проєктом, використовуючи спеціальні функції системи.

Звичайний користувач, зареєструвавшись у системі та пройшовши авторизацію, отримує доступ до базових функцій. Він може бути доданий до певного департаменту та призначений на проєкти менеджером. У рамках проєкту користувач може приєднуватися до чатів, створених менеджером, та обмінюватися повідомленнями з іншими учасниками проєкту. Користувач має доступ до історії повідомлень у чатах проєктів, до яких він належить.

Отже, діаграма варіантів використання наочно демонструє розподіл ролей та функціональних можливостей між адміністратором, менеджером та звичайним користувачем у системі захищеного обміну інформацією в офісі. Вона відображає ієрархію доступу та основні дії, які можуть виконувати користувачі відповідно до їх ролі в системі.

Діаграма варіантів використання наведена у додатку Б.

4.10 ER-діаграма бази даних

ER-діаграма бази даних відображає структуру бази даних системи захищеного обміну інформацією в офісі та зв'язки між її основними сутностями.

У центрі діаграми знаходиться сутність "users", яка представляє користувачів системи. Кожен користувач має унікальний ідентифікатор (id), ім'я (first_name), прізвище (last_name), електронну пошту (email), пароль (password), роль (role), посаду (position), дату створення (created_at) та дату останнього входу (last_login). Користувач також пов'язаний з департаментом (department) через зовнішній ключ department_id.

Сутність "departments" представляє департаменти в системі. Кожен департамент має унікальний ідентифікатор (id) та назву (name). Між сутностями "users" та "departments" встановлено зв'язок один-до-багатьох, оскільки кожен користувач може належати лише до одного департаменту, тоді як департамент може містити багатьох користувачів.

Сутність "projects" відповідає за проєкти в системі. Кожен проєкт має унікальний ідентифікатор (id), назву (name), зв'язок з департаментом через зовнішній ключ department_id та зв'язок з менеджером через зовнішній ключ manager_id. Між сутностями "departments" та "projects" встановлено зв'язок один-до-багатьох, оскільки кожен проєкт належить до певного департаменту, а департамент може містити декілька проєктів.

Сутність "chats" представляє чати в системі. Кожен чат має унікальний ідентифікатор (id), назву (name) та зв'язок з проєктом через зовнішній ключ

project_id. Між сутностями "projects" та "chats" встановлено зв'язок один-до-багатьох, де кожен чат належить до певного проєкту, а проєкт може містити кілька чатів.

Сутність "messages" відповідає за повідомлення в чатах. Кожне повідомлення має унікальний ідентифікатор (id), текст (text), мітку часу (timestamp) та зв'язки з чатом (chat_id) і користувачем (user_id) через відповідні зовнішні ключі. Між сутностями "chats" та "messages" встановлено зв'язок один-до-багатьох, де кожне повідомлення належить до певного чату, а чат може містити багато повідомлень. Аналогічно, між сутностями "users" та "messages" також встановлено зв'язок один-до-багатьох, оскільки кожне повідомлення відправляється певним користувачем, а користувач може відправити багато повідомлень.

Додатково, між сутностями "chats" та "users" існує зв'язок багато-до-багатьох, реалізований через допоміжну таблицю "chat_users". Ця таблиця містить зовнішні ключі chat_id та user_id, що дозволяє встановити зв'язок між чатами та користувачами, які беруть у них участь.

Отже, діаграма бази даних надає чітке уявлення про структуру бази даних системи, відображаючи основні сутності (користувачі, департаменти, проєкти, чати та повідомлення) та зв'язки між ними. Вона є фундаментом для правильної організації та ефективного функціонування системи захищеного обміну інформацією в офісі.

ER-діаграма бази даних наведена у додатку В.

4.11 Структурна схема

Структурна схема відображає високорівневу структуру системи захищеного обміну інформацією в офісі, показуючи основні компоненти та їх взаємодію.

Система складається з трьох основних частин: клієнтської частини (Client), серверної частини (Server) та зовнішніх сервісів (External Services).

Клієнтська частина включає в себе компоненти, з якими безпосередньо взаємодіє користувач. Сюди входить користувацький інтерфейс (User Interface),

який забезпечує візуальне представлення системи та можливість взаємодії з нею. Користувацький інтерфейс побудований з використанням фреймворку React та складається з маршрутизатора (Router), сторінок (Pages) та окремих компонентів (Components). Клієнтська частина також містить сервіс для взаємодії з API (API Interaction), який відповідає за комунікацію з серверною частиною.

Серверна частина є основою системи і складається з кількох ключових компонентів. Контролер (Controller) обробляє вхідні запити від клієнтської частини та передає їх на відповідні сервіси. Сервісний шар (Service Layer) містить бізнес-логіку системи і відповідає за обробку даних та виконання необхідних операцій. Він включає в себе такі компоненти, як репозиторій (Repository) для взаємодії з базою даних, конфігурацію (Config) для налаштування системи, сервіс безпеки (Security) для забезпечення автентифікації та авторизації, а також допоміжні утиліти (Utils).

Окремим компонентом серверної частини є WebSocket контролер (WebSocket Controller), який відповідає за обробку повідомлень у реальному часі. Він використовує обробник WebSocket (WebSocket Handler) для встановлення та підтримки з'єднання з клієнтами, а також сервіс чату (Chat Service) для обробки повідомлень та управління чатами.

Зовнішні сервіси включають в себе сторонні системи та API, які використовуються для розширення функціональності системи. Сюди входить Google Gemini API для інтелектуального аналізу текстових даних, хмарне сховище S3 для зберігання файлів та базу даних PostgreSQL для збереження структурованих даних.

Взаємодія між компонентами системи здійснюється через чітко визначені інтерфейси та протоколи. Клієнтська частина комунікує з серверною частиною за допомогою HTTP запитів через API. Серверна частина обробляє ці запити, використовуючи відповідні контролери та сервіси, а також взаємодіє з базою даних та зовнішніми сервісами для отримання та збереження необхідних даних. WebSocket з'єднання забезпечує обмін повідомленнями в реальному часі між клієнтами та сервером.

Отже, структурна схема надає чіткий огляд структури системи захищеного обміну інформацією в офісі, демонструючи основні компоненти, їх взаємозв'язки та розподіл функціональності між клієнтською та серверною частинами. Вона є основою для розуміння принципів роботи системи та її подальшого розвитку.

Структурна схема наведена у додатку Г.

4.12 Діаграма послідовності

Діаграма послідовності відображає процес взаємодії між користувачем, клієнтською частиною, серверною частиною, базою даних та системою штучного інтелекту (AI) в рамках системи захищеного обміну інформацією в офісі.

Процес починається з того, що користувач надсилає запит на авторизацію (login request) до клієнтської частини системи. Клієнтська частина, в свою чергу, передає цей запит на серверну частину (authentication request). Серверна частина перевіряє надані користувачем облікові дані (verify credentials) і, у разі їх коректності, генерує JWT токен (JWT token) та повертає його клієнтській частині. Клієнтська частина зберігає отриманий токен і сигналізує користувачу про успішну авторизацію (login success).

Після успішної авторизації користувач може надсилати повідомлення (send message) через клієнтський додаток. Клієнтська частина відправляє повідомлення (encrypted message) на серверну частину, де воно зберігається в базі даних (store message). Після успішного збереження серверна частина надсилає повідомлення (message stored) системі штучного інтелекту (AI) для аналізу його вмісту (analyze message content). Система AI виконує аналіз повідомлення і повертає результати (analysis results) на серверну частину, яка зберігає їх у базі даних (store analysis).

Після завершення аналізу та збереження результатів серверна частина надсилає повідомлення (message delivered) клієнтській частині, яка, в свою чергу, відображає його користувачу та сигналізує про успішну доставку (delivery confirmation).

Користувач також має можливість запросити звіт (request report) через клієнтський додаток. Запит на формування звіту (report request) надсилається на серверну частину, яка виконує вибірку необхідних повідомлень з бази даних (fetch messages). Отримані дані повідомлень (messages data) передаються системі AI для генерації звіту (generate report). Система AI формує вміст звіту (report content) на основі аналізу повідомлень і надсилає його назад на серверну частину. Серверна частина виконує остаточне форматування звіту (formatted report) і передає його клієнтській частині, яка відображає звіт користувачу (display report).

Отже, діаграма послідовності демонструє покроковий процес взаємодії між різними компонентами системи захищеного обміну інформацією в офісі. Вона охоплює такі ключові етапи, як авторизація користувача, відправка та збереження повідомлень, аналіз вмісту повідомлень за допомогою штучного інтелекту, а також формування і відображення звітів. Ця діаграма надає чітке розуміння послідовності дій та обміну даними між компонентами системи під час виконання основних операцій.

Діаграма послідовності наведена у додатку Д.

4.13 Діаграма об’єктів

Діаграма об'єктів ілюструє приклад взаємозв'язків між конкретними об'єктами в рамках системи захищеного обміну інформацією в офісі в певний момент часу.

На діаграмі зображено об'єкт класу Department з назвою "Development" та унікальним ідентифікатором 1. Цей об'єкт представляє конкретний департамент в організації.

Департамент "Development" містить два об'єкти класу User: user1 та user2. Об'єкт user1 представляє користувача з ім'ям "John Smith", який має роль менеджера проекту (MANAGER), унікальний ідентифікатор 1, електронну пошту "john@company.com" та інші атрибути, такі як ім'я користувача, посада, статус активності тощо. Об'єкт user2 представляє користувача з ім'ям "Alice Johnson", яка

має роль розробника (DEVELOPER), унікальний ідентифікатор 2, електронну пошту "alice@company.com" та відповідні атрибути.

Об'єкт класу Project з назвою "Project X" та унікальним ідентифікатором 1 представляє конкретний проект в системі. Цей проект належить до департаменту "Development" та має зв'язок з об'єктом user1, який виступає менеджером проекту.

В рамках проекту "Project X" існує об'єкт класу Chat з назвою "Team Chat" та унікальним ідентифікатором 1. Цей чат призначений для командної комунікації в межах проекту.

Об'єкт класу Message з унікальним ідентифікатором 1 представляє конкретне повідомлення в чаті. Він містить текст повідомлення "Meeting at 2 PM", має зв'язок з об'єктом user1, який є відправником повідомлення, та належить до об'єкту chat1.

Діаграма об'єктів демонструє зв'язки між об'єктами різних класів в системі. Департамент "Development" зв'язаний з об'єктами користувачів user1 та user2 через зв'язок "employs". Проект "Project X" зв'язаний з департаментом "Development" через зв'язок "belongs to" та з об'єктом user1 через зв'язок "managed by". Чат "Team Chat" зв'язаний з проектом "Project X" через зв'язок "belongs to" та з об'єктами користувачів user1 та user2 через зв'язок "includes". Повідомлення з текстом "Meeting at 2 PM" зв'язане з об'єктом user1 через зв'язок "sent by" та з об'єктом chat1 через зв'язок "belongs to".

Ця діаграма об'єктів надає наочний приклад того, як виглядають конкретні екземпляри класів та їх взаємозв'язки в системі в певний момент часу. Вона допомагає краще зрозуміти структуру даних та взаємодію між об'єктами в реальному контексті використання системи.

Діаграма об'єктів наведена у додатку Е.

4.14 Діаграма пакетів серверної частини

Діаграма пакетів відображає організацію програмних компонентів системи захищеного обміну інформацією в офісі та їх взаємозв'язки.

На верхньому рівні діаграми знаходиться пакет API, який містить компоненти, відповідальні за взаємодію з клієнтською частиною системи. Цей пакет включає в себе підпакети DTO (Data Transfer Object), що визначають структуру даних для обміну між клієнтом і сервером, Interfaces для опису контрактів взаємодії, а також Types, що містять спільні типи даних та константи.

Пакет Controller відповідає за обробку вхідних запитів від клієнта та делегування їх відповідним сервісам для подальшої обробки. Він використовує компоненти з пакету API для отримання та валідації вхідних даних.

Пакет Service містить бізнес-логіку системи та забезпечує виконання основних операцій. Сервіси взаємодіють з компонентами доменної моделі (Domain) для виконання необхідних дій та обробки даних. Вони також можуть використовувати зовнішні сервіси та бібліотеки для реалізації специфічних функцій, таких як взаємодія з базою даних чи інтеграція з іншими системами.

Доменна модель (Domain) є центральною частиною системи та містить основні сутності та бізнес-правила. Вона включає в себе підпакети Entity для опису структури даних та взаємозв'язків між ними, а також Enum для визначення фіксованих наборів значень.

Пакет Repository відповідає за взаємодію з базою даних та надає методи для збереження, отримання та маніпулювання даними. Він використовує компоненти доменної моделі для визначення структури даних та взаємодіє з обраною технологією доступу до бази даних.

Пакет Exception містить класи та механізми для обробки виняткових ситуацій, які можуть виникнути під час роботи системи. Він дозволяє централізовано обробляти помилки та надавати інформативні повідомлення про них.

Окремо винесений пакет Security, який відповідає за реалізацію функцій безпеки, таких як автентифікація користувачів, авторизація доступу та захист даних. Він може взаємодіяти з іншими компонентами системи для забезпечення безпечної роботи.

Діаграма пакетів надає загальне уявлення про структуру програмних компонентів системи та їх організацію. Вона допомагає розробникам розуміти, які частини системи відповідають за певні функції та як вони взаємодіють між собою. Це сприяє кращому розумінню архітектури системи та полегшує її супровід та масштабування.

Діаграма пакетів наведена у додатку Ж.

4.15 Діаграма класів

Діаграма класів демонструє структуру основних класів та їх взаємозв'язки в рамках системи захищеного обміну інформацією в офісі.

Центральним класом на діаграмі є клас User, який представляє користувача системи. Він містить основні атрибути, такі як унікальний ідентифікатор (id), ім'я користувача (username), електронну пошту (email), ім'я (firstName) та прізвище (lastName), посаду (position), роль (role), статус активності (isActive), дату створення (createdAt) та дату останнього входу (lastLogin). Клас User також має методи для отримання прав доступу (getAuthorities), перевірки блокування облікового запису (isAccountNonLocked) тощо.

Клас Department представляє департамент в системі і містить атрибути, такі як унікальний ідентифікатор (id) та назву (name). Він має зв'язок "один до багатьох" з класом User, оскільки кожен департамент може містити багатьох користувачів, але кожен користувач належить лише до одного департаменту.

Клас Project відображає проект в системі і містить атрибути, такі як унікальний ідентифікатор (id), назву (name), а також зв'язки з класами User (manager) та Department. Кожен проект має одного менеджера, який є користувачем системи, та належить до певного департаменту.

Клас Chat представляє чат в системі і містить атрибути, такі як унікальний ідентифікатор (id), назву (name), а також зв'язки з класами Project та User. Кожен чат належить до певного проекту та може містити багатьох учасників (користувачів).

Клас Message представляє повідомлення в чаті і містить атрибути, такі як унікальний ідентифікатор (id), текст повідомлення (text), зв'язки з класами User (відправник) та Chat, а також мітку часу створення (timestamp).

Окрім основних класів, на діаграмі також присутні класи-DTO (Data Transfer Object), такі як UserDto, ChatDto та MessageDto, які використовуються для передачі даних між клієнтом та сервером. Вони містять необхідні атрибути для представлення відповідних сутностей у спрощеному вигляді.

Класи ChatService, UserService та MessageService представляють сервісний рівень системи і містять методи для виконання бізнес-логіки, такі як створення чату, отримання списку користувачів, збереження повідомлення тощо. Вони взаємодіють з репозиторіями (UserRepository, ChatRepository, MessageRepository) для доступу до даних та виконання операцій з базою даних.

Клас AuthenticationService відповідає за автентифікацію користувачів та містить методи для входу (login), реєстрації (register), перевірки токена (validateToken) та отримання ролі користувача (getRole).

На діаграмі також присутні перерахування (enum) Role та Permission, які визначають можливі ролі користувачів та дозволи доступу в системі.

Діаграма класів надає детальне уявлення про структуру та взаємозв'язки основних компонентів системи на рівні класів. Вона допомагає розробникам розуміти, які класи відповідають за певні функції, які атрибути та методи вони містять, а також як вони співвідносяться між собою. Це полегшує розробку, супровід та розширення функціональності системи.

Діаграма класів наведена у додатку И.

4.16 Керівництво користувача

При першому вході в систему користувач потрапляє на сторінку авторизації, де необхідно ввести свої облікові дані - логін та пароль. Інтерфейс сторінки авторизації представлено на рисунку 4.1.

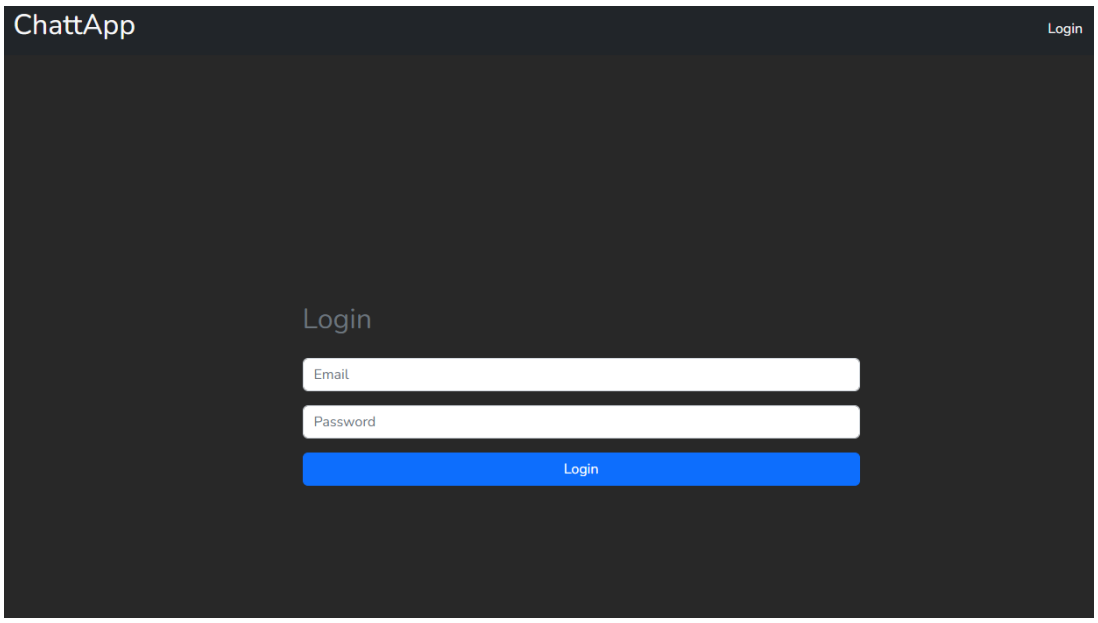

Рисунок 4.1 – Сторінка авторизації

Реєстрація нових користувачів здійснюється адміністратором або менеджером системи через спеціальну форму. При створенні облікового запису необхідно вказати основні дані про користувача, включаючи ім'я, прізвище, email та роль в системі, як показано на рисунку 4.2.

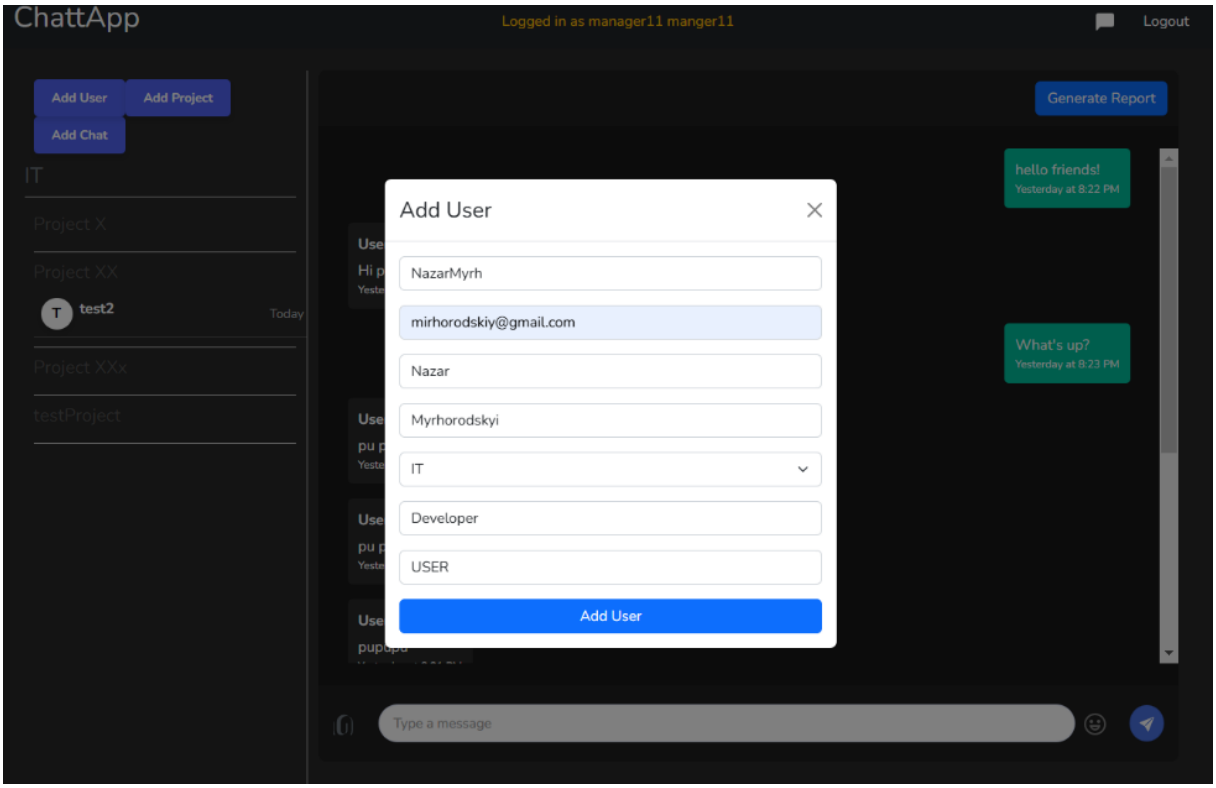

Рисунок 4.2 – Форма реєстрації користувача

Після реєстрації користувача системою, на вказану електронну пошту автоматично надсилається пароль для входу в систему. Приклад листа з паролем для доступу до системи продемонстровано на рисунку 4.3.

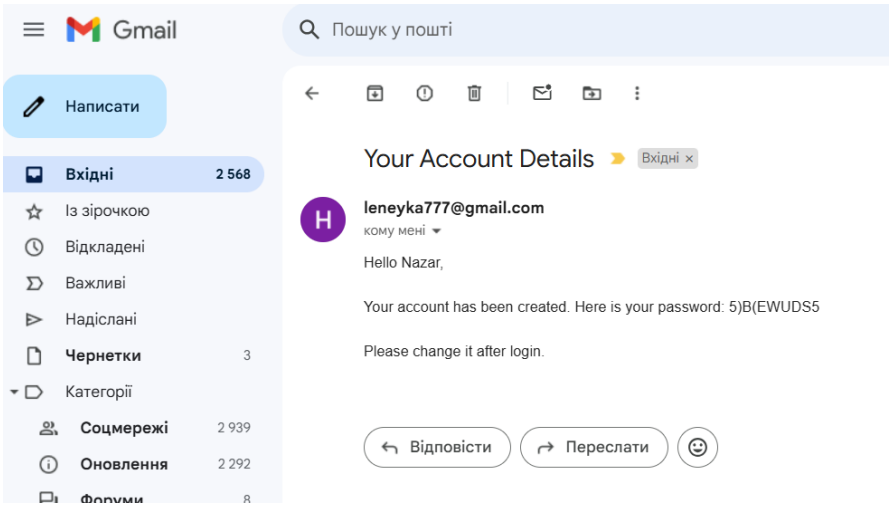

Рисунок 4.3 – Отримання паролю користувача

Для створення нового проєкту в системі менеджер використовує спеціальну форму, де вказує назву проєкту та інші необхідні параметри. Інтерфейс створення проєкту представлено на рисунку 4.4.

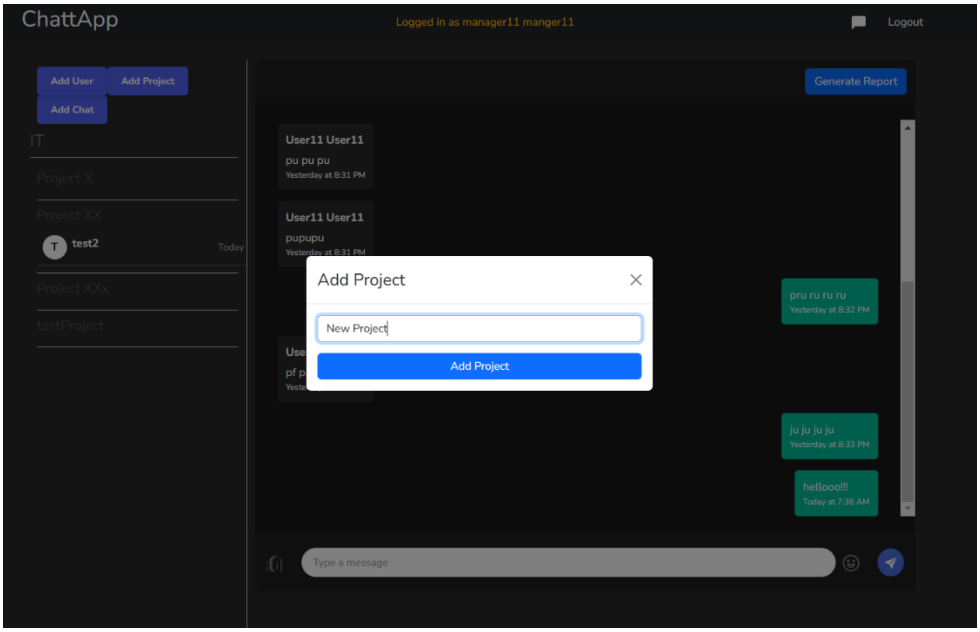

Рисунок 4.4 – Форма створення проєкту

В рамках кожного проєкту можна створювати окремі чати для комунікації команди. Форма створення чату дозволяє вказати назву чату та обрати учасників з числа працівників, залучених до проєкту. Приклад форми створення чату показано на рисунку 4.5.

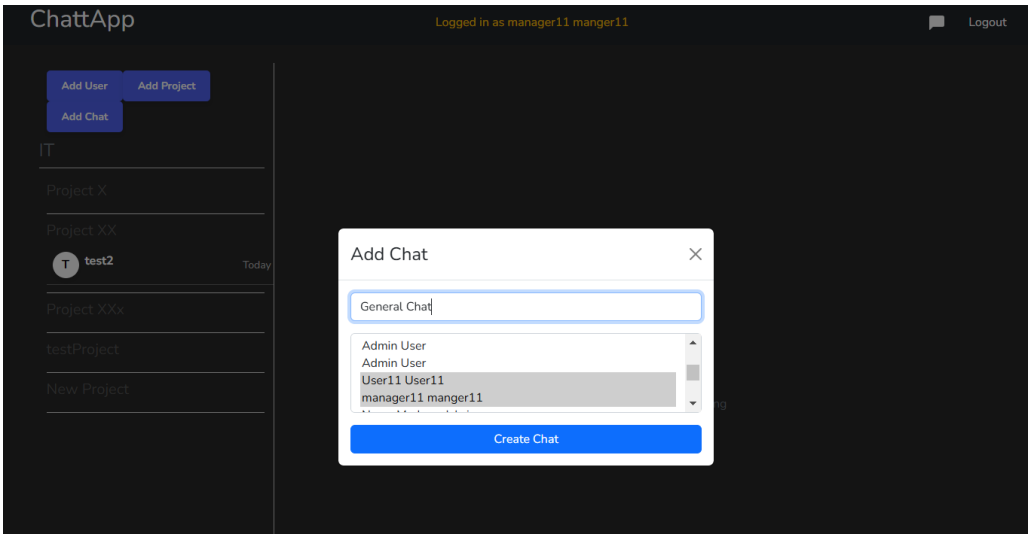

Рисунок 4.5 – Форма створення чату

Після створення чату менеджер отримує доступ до розширеного інтерфейсу вікна чату з можливістю керування учасниками та налаштуваннями. Інтерфейс чату з точки зору менеджера представлено на рисунку 4.6.

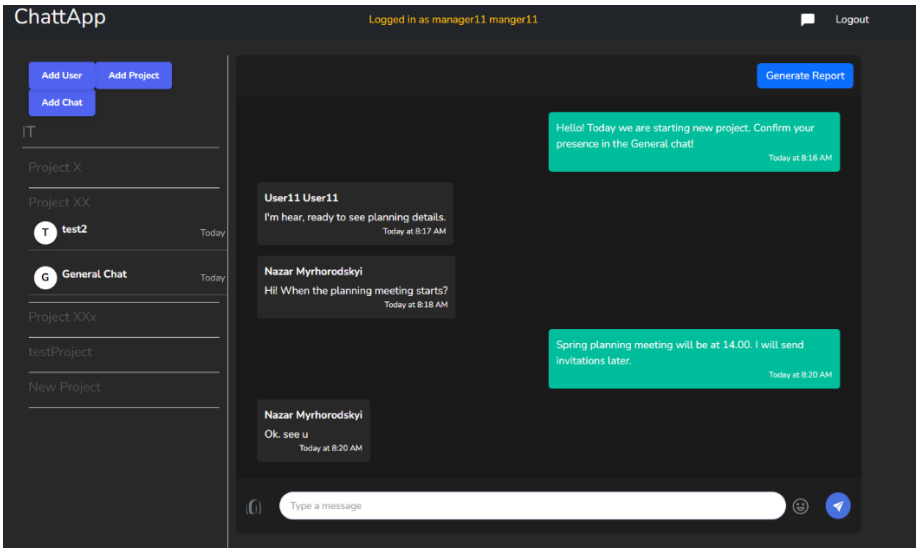

Рисунок 4.6 – Інтерфейс вікна чату менеджера

Звичайні користувачі мають доступ до базового інтерфейсу чату, який дозволяє обмінюватися повідомленнями та файлами з іншими учасниками проєкту. Вигляд вікна чату для звичайного користувача показано на рисунку 4.7.

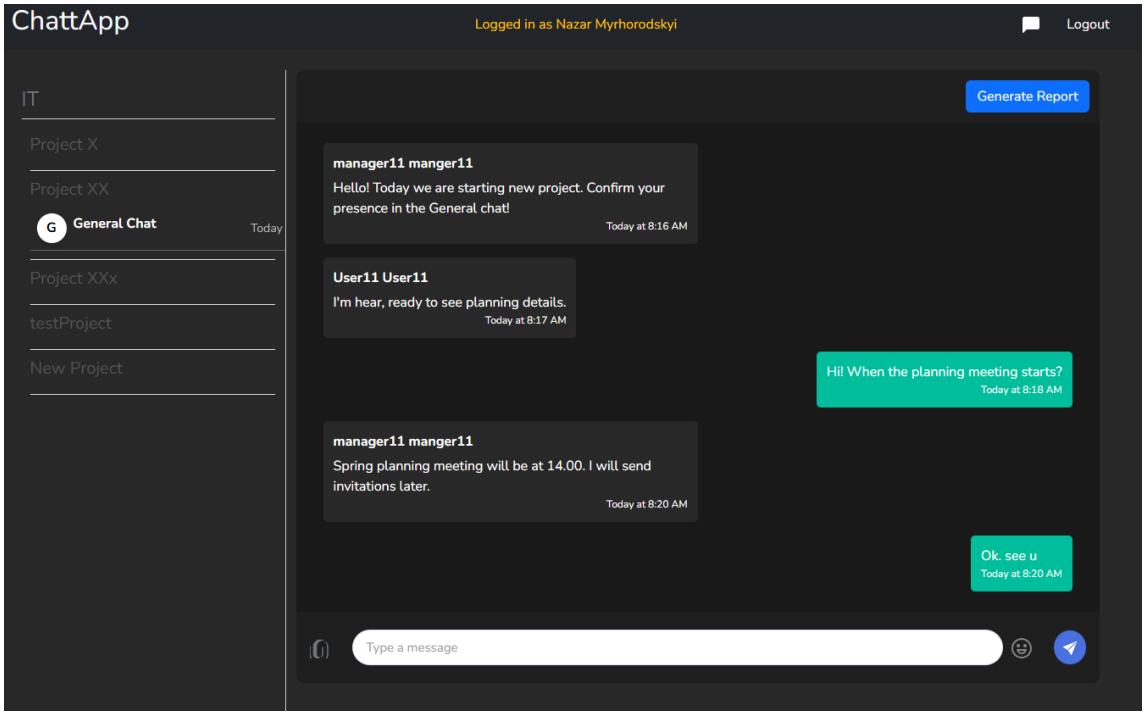

Рисунок 4.7 – Інтерфейс вікна чату користувача

Система надає можливість автоматичної генерації звітів на основі аналізу комунікацій в чатах з використанням штучного інтелекту. Приклад згенерованого системою звіту по проєкту представлено на рисунку 4.8.

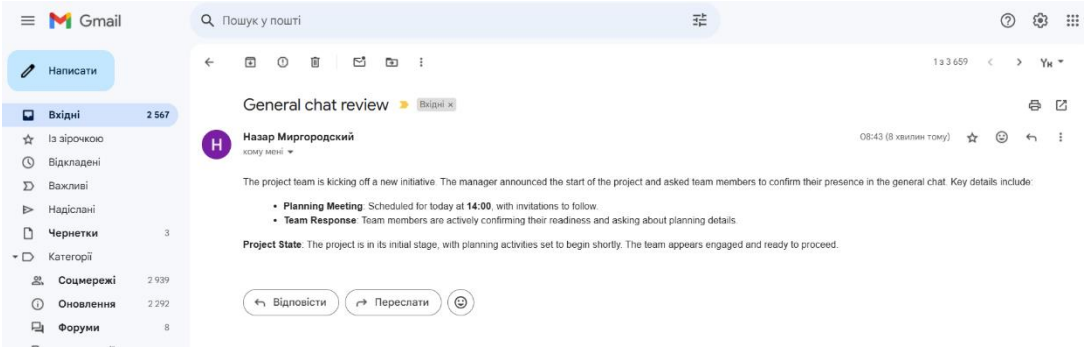

Рисунок 4.8 – Результат генерації звіту

Висновки до розділу 4

У даному розділі було детально розглянуто програмне та технічне забезпечення системи захищеного обміну інформацією в офісі. Обрана розподілена архітектура, що складається з двох незалежних серверних компонентів та клієнтської частини, забезпечує необхідну гнучкість та масштабованість системи.

Основний серверний компонент, реалізований на базі Spring Framework, забезпечує базову бізнес-логіку системи, включаючи автентифікацію користувачів, управління даними та взаємодію з базою даних PostgreSQL. Для забезпечення комунікації в реальному часі розроблено окремий WebSocket сервер на базі WebSocket.io, що відповідає за обмін повідомленнями між користувачами. Таке розділення функціоналу дозволяє оптимізувати роботу кожного компонента під його специфічні задачі та забезпечити високу продуктивність системи в цілому.

Значну увагу в системі приділено безпеці даних через реалізацію двошарового шифрування. Серверний рівень шифрування захищає дані при їх зберіганні, в той час як транспортний рівень забезпечує безпеку при передачі даних між компонентами системи. Використання JWT токенів та ролевої моделі доступу гарантує надійну автентифікацію та авторизацію користувачів системи.

Клієнтська частина системи, розроблена з використанням React, забезпечує зручний та інтуїтивно зрозумілий інтерфейс користувача. Застосування Redux для управління станом додатку та Socket.IO для обміну повідомленнями в реальному часі створює комфортне середовище для корпоративних комунікацій. Інтерфейс адаптовано під різні ролі користувачів, надаючи менеджерам розширені можливості для управління проектами та командами.

Важливим досягненням є впровадження технологій штучного інтелекту через інтеграцію з Gemini API, що дозволило реалізувати функції автоматичного аналізу комунікацій та генерації звітів. При цьому особлива увага приділяється забезпеченню конфіденційності даних при їх обробці AI-моделями, що відповідає високим вимогам до безпеки корпоративних комунікацій.

Реалізовані інтеграційні механізми, що включають REST API та WebSocket протоколи, забезпечують надійну взаємодію між компонентами системи та створюють можливості для подальшого розширення функціоналу. Використання Docker контейнеризації значно спрощує процеси розгортання та масштабування системи, забезпечуючи гнучкість у виборі інфраструктури.

Обрані технології та архітектурні рішення формують надійну та безпечну платформу для корпоративних комунікацій, що відповідає сучасним вимогам до продуктивності, безпеки та зручності використання. Система має значний потенціал для подальшого розвитку та адаптації до нових потреб користувачів, що робить її перспективним рішенням для організації захищених корпоративних комунікацій.

5 СТАРТАП ПРОЄКТ

5.1 Опис ідеї проєкту

Для оцінки ринкових перспектив стартап-проєкту було проведено аналіз його основної ідеї, напрямків застосування та вигод для кінцевих користувачів. Такий підхід дозволяє отримати цілісне уявлення про потенціал розробки та виділити ключові переваги, які вона пропонує. Узагальнені результати подано в таблиці 5.1, що демонструє зміст ідеї, можливі напрями її реалізації та користь для споживачів.

Таблиця 5.1 – Опис ідеї проєкту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Система захищеного обміну інформацією в офісі з функціями AI-аналітики для автоматизації формування звітності	Захищені корпоративні комунікації	Безпечний обмін конфіденційною інформацією між співробітниками, захист від витоків даних
	Управління проектною інформацією	Структурована організація даних по проектах, автоматичне збереження історії комунікацій та файлів
	Автоматизована аналітика та звітність	AI-генерація тижневих звітів по проектах на основі аналізу всіх комунікацій, економія часу керівників
	Інтеграція з корпоративними системами	Єдиний захищений простір для всіх корпоративних комунікацій, синхронізація з існуючими системами

Для оцінки конкурентоспроможності проєкту створення системи захищеного обміну інформацією в офісі було проведено аналіз існуючих платформ для

корпоративних комунікацій. Основна мета аналізу - визначити ключові переваги і недоліки конкурентів, зрозуміти їхній вплив на ринок та підкреслити унікальні можливості запропонованої системи.

Ринок корпоративних комунікацій активно розвивається, але більшість платформ використовують традиційні підходи до організації обміну інформацією, що створює можливість для інноваційних рішень, таких як інтеграція AI-аналітики та автоматизованої звітності. Конкурентів було обрано з урахуванням локальних та міжнародних учасників, які мають популярність серед корпоративних користувачів.

Microsoft Teams та Slack є одними з провідних платформ для корпоративних комунікацій. Вони пропонують базові функції обміну повідомленнями та файлами, але не мають вбудованих можливостей для глибокого аналізу комунікацій та автоматизованого формування звітності. Telegram Enterprise, хоча і забезпечує високий рівень безпеки, також не надає інструментів для AI-аналітики корпоративних комунікацій.

У таблиці 5.2 проведено оцінку конкурентоспроможності проєкту.

Таблиця 5.2 – Визначення сильних, слабких та нейтральних характеристик ідеї проєкту

№ п/п	Техніко-економічні характеристики ідеї	Продукти/концепції конкурентів			W	N	S
		Проєкт	MS Teams	Slack			
1	AI-аналітика комунікацій	+	-	+/-			+
2	Автоматизована звітність	+	-	-			+
3	Захищений обмін даними	+	+	+		+	

№ п/п	Техніко-економічні характеристики ідеї	Продукти/концепції конкурентів			W	N	S
		Проєкт	MS Teams	Slack			
4	Інтеграція з корпоративними системами	+	+	+		+	
5	Гнучкість налаштування	+	+/-	+		+	
6	Масштабованість	+	+	+		+	
7	База користувачів	-	+	+	+		
8	Вартість впровадження	+	-	-			+

Аналіз таблиці показує, що система має значні конкурентні переваги за рахунок впровадження AI-аналітики комунікацій та автоматизованої звітності. Ці функції відсутні або обмежено представлені у конкурентів, що створює унікальну ринкову позицію. Також важливою перевагою є нижча вартість впровадження порівняно з великими корпоративними рішеннями.

Слабкою стороною проєкту є відсутність сформованої бази користувачів, що потребуватиме додаткових зусиль для виходу на ринок та залучення клієнтів. Нейтральні характеристики, такі як захищений обмін даними та інтеграційні можливості, знаходяться на рівні конкурентів, що є достатнім для забезпечення базових потреб користувачів.

Цей аналіз дозволяє зробити висновок про потенційну конкурентоспроможність проєкту на ринку корпоративних комунікацій, особливо в сегменті компаній, які зацікавлені в автоматизації процесів аналізу інформації та формування звітності.

5.2 Технологічний аудит ідеї проєкту

Проведено аналіз технологій, необхідних для реалізації ідеї створення системи захищеного обміну інформацією в офісі з функціями автоматизованої аналітики. Основна увага зосереджена на технологічній здійсненності проєкту, доступності та готовності існуючих рішень до впровадження. Отримані результати наведено у таблиці 5.3.

Таблиця 5.3 – Технологічна здійсненність ідеї проєкту

№ п/п	Ідея продукту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Захищений обмін інформацією	Spring Security, JWT-токени для автентифікації	Наявна	Доступні через відкриті бібліотеки
2	AI-аналітика комунікацій	OpenAI API, власні алгоритми обробки даних	Наявні	Доступні через API та власну розробку
3	Автоматизована звітність	Apache POI для генерації звітів, Spring Batch для обробки даних	Наявні	Доступні через Maven репозиторій
4	Зберігання та індексація даних	PostgreSQL, Elasticsearch	Наявні	Доступні як open-source рішення
5	Інтеграція з корпоративними системами	REST API, Spring Integration	Наявні	Доступні через Spring Framework

За результатами проведеного аудиту встановлено, що всі необхідні базові технології для реалізації проєкту є наявними та доступними авторам проєкту. Це підтверджує можливість технологічної реалізації ідеї. Основний шлях

впровадження буде базуватися на використанні відкритих технологій та фреймворків з доробкою власних компонентів для специфічних функцій системи.

Особливу увагу слід приділити розробці компонентів AI-аналітики, де потрібна доробка існуючих рішень під специфічні потреби проєкту. Проте наявність доступу до API провідних AI-платформ та можливість розробки власних алгоритмів робить це завдання цілком здійсненним.

Таким чином, технологічний аудит підтверджує можливість реалізації проєкту з використанням доступних технологій та інструментів розробки. Обрані технології формують збалансований стек, який забезпечує всі необхідні функціональні можливості системи, залишаючись при цьому відносно простим у впровадженні та підтримці.

5.3 Аналіз ринкових можливостей запуску стартап-проєкту

Для оцінки потенційного ринку стартапу з впровадження системи захищеного обміну інформацією в офісі проведено аналіз попиту та стану ринкового середовища. Метою аналізу є визначення привабливості ринку, ключових можливостей для розвитку та потенційних загроз для успішної реалізації проєкту.

Таблиця 5.4 містить попередню характеристику потенційного ринку стартап-проєкту, що ґрунтується на аналізі кількості конкурентів, обсягу ринку, його динаміки, можливих обмежень для входу та рентабельності в галузі.

Таблиця 5.4 – Попередня характеристика потенційного ринку стартап-проєкту

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	5-7 основних гравців на ринку корпоративних комунікацій (Microsoft Teams, Slack, Zoom, тощо)

№ п/п	Показники стану ринку (найменування)	Характеристика
2	Загальний обсяг продаж, грн/ум.од	Світовий ринок корпоративних комунікацій оцінюється в $50+ млрд, з яких український сегмент складає близько 1-2%
3	Динаміка ринку (якісна оцінка)	Зростає. Щорічний приріст 15-20% через збільшення попиту на цифрові рішення
4	Наявність обмежень для входу	Високі вимоги до безпеки даних, необхідність відповідності регуляторним нормам, значні інвестиції в розробку
5	Специфічні вимоги до стандартизації та сертифікації	Відповідність стандартам безпеки даних (GDPR, ISO 27001), сертифікація для роботи з персональними даними
6	Середня норма рентабельності в галузі, %	25-30% для успішних проєктів після виходу на планову потужність

Ринок корпоративних комунікаційних систем демонструє стабільне зростання, особливо враховуючи тенденцію до цифровізації бізнес-процесів та збільшення кількості віддалених працівників. Хоча існують значні бар'єри входу у вигляді високих вимог до безпеки та необхідності значних інвестицій, унікальність пропонованого рішення з AI-аналітикою створює потенціал для успішного входження на ринок.

Для успішного впровадження стартап-проєкту в сфері корпоративних захищених комунікацій важливо не лише оцінити ринкові можливості, але й детально вивчити потенційні групи клієнтів та їхні вимоги до продукту. Ключовим аспектом є розуміння того, хто є основними споживачами послуг і яким чином вони визначають свої потреби.

Таблиця 5.5 містить характеристику потенційних клієнтів стартап-проєкту, на основі якої можна сформувати орієнтовний перелік вимог до товару для кожної цільової групи.

Таблиця 5.5 – Характеристика потенційних клієнтів стартап-проєкту

№ п/п	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
1	Захищений обмін конфіденційною інформацією	Середні та великі підприємства з розподіленими командами	Різний рівень технічної підготовки, різні вимоги до безпеки даних	Високий рівень захисту даних; простий інтерфейс; Надійність роботи
2	Автоматизація аналізу комунікацій та звітності	IT-компанії та проєктні організації	Високі вимоги до функціоналу, потреба в кастомізації	Гнучкість налаштувань; інтеграція з існуючими системами; точність AI-аналізу
3	Централізоване управління	Фінансові установи та організації з	Підвищені вимоги до відповідності	Відповідність регуляторним вимогам;

	корпоративними комунікаціями	суворими регуляторними вимогами	стандартам та аудиту	можливість аудиту; контроль доступу
4	Оптимізація внутрішніх комунікаційних процесів	Швидкозростаючі компанії та стартапи	Потреба в швидкому масштабуванні та адаптації	Швидке розгортання; масштабованість; доступна ціна

Згідно з результатами аналізу, необхідно зосередитись на забезпеченні:

- Високого рівня безпеки та захисту даних;
- простоти використання при збереженні потужного функціоналу;
- гнучкості налаштувань для різних сценаріїв використання;
- надійності та стабільності роботи системи.

Після визначення потенційних груп клієнтів для стартап-проєкту в сфері захищених корпоративних комунікацій важливо здійснити аналіз ринкового середовища. Це включає оцінку факторів, що можуть сприяти або перешкоджати успішному впровадженню проєкту. Для цієї мети формуються таблиці, які містять ключові фактори загроз та можливостей, що визначають шанси для розвитку бізнесу. Фактори загроз наведені у Таблиці 5.6.

Таблиця 5.6 – Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1	Посилення конкуренції	Вихід на ринок нових гравців з аналогічними AI-рішеннями	Посилення унікальних характеристик продукту, розширення функціоналу, покращення якості обслуговування
2	Зміни в законодавстві	Нові регуляторні вимоги щодо захисту	Оперативна адаптація продукту, отримання

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
		даних та використання AI	необхідних сертифікатів, консультації з регуляторами
3	Технологічні зміни	Швидкий розвиток AI-технологій може зробити поточні рішення застарілими	Постійний моніторинг технологій, інвестиції в R&D, оновлення технологічного стеку
4	Економічна нестабільність	Зменшення IT-бюджетів компаній через економічну кризу	Розробка гнучких цінових моделей, фокус на ROI для клієнтів, оптимізація витрат
5	Проблеми з безпекою	Можливі витоки даних або вразливості в системі	Регулярний аудит безпеки, впровадження додаткових рівнів захисту, швидке реагування на інциденти

Фактори можливостей наведені у Таблиці 5.7

Таблиця 5.7 – Фактори можливостей

№ п/п	Фактор	Зміст можливості	Можлива реакція компанії
1	Зростання попиту на віддалену роботу	Збільшення потреби в захищених комунікаційних системах	Розширення функціоналу для віддалених команд, активне просування продукту, створення спеціальних пропозицій
2	Розвиток AI-технологій	Поява нових можливостей для аналізу та обробки даних	Впровадження нових AI-моделей, розширення

			аналітичних можливостей, створення унікальних функцій
3	Підвищення вимог до безпеки даних	Зростання інтересу до захищених комунікацій	Посилення функцій безпеки, отримання сертифікацій, маркетинг безпекових функцій
4	Інтеграційні можливості	Зростання попиту на інтеграцію з існуючими системами	Розробка нових конекторів, створення API, партнерства з іншими вендорами
5	Державні ініціативи цифровізації	Підтримка впровадження цифрових рішень на державному рівні	Участь у державних програмах, адаптація продукту для держсектору, отримання необхідних сертифікатів

Аналіз факторів загроз та можливостей виявляє складну динаміку ринку корпоративних комунікаційних систем. З одного боку, існують значні ризики, пов'язані з швидкими технологічними змінами та посиленням конкуренції. Особливу увагу слід приділити загрозам у сфері безпеки даних та відповідності регуляторним вимогам, оскільки ці фактори можуть суттєво вплинути на довіру клієнтів та репутацію продукту.

Водночас, ринок демонструє значний потенціал для розвитку, особливо в контексті зростаючого попиту на рішення для віддаленої роботи та захищених комунікацій. Розвиток AI-технологій відкриває нові можливості для вдосконалення продукту та створення унікальних конкурентних переваг. Важливим фактором є також державна підтримка цифровізації, що може створити додаткові можливості для розширення ринку.

Для успішного розвитку проєкту необхідно розробити комплексну стратегію, яка дозволить:

- мінімізувати виявлені ризики через постійний моніторинг ринку та проактивну адаптацію продукту;

– максимально використати ринкові можливості через розвиток інноваційних функцій та активний маркетинг;

– забезпечити відповідність продукту регуляторним вимогам та високим стандартам безпеки;

– підтримувати конкурентоспроможність через постійне вдосконалення технологічної бази та якості обслуговування.

У Таблиці 5.8 наведено ступеневий аналіз конкуренції на ринку.

Таблиця 5.8 – Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
Тип конкуренції: монополістична конкуренція	На ринку присутні кілька великих гравців (Microsoft Teams, Slack) та багато дрібних компаній, кожна з яких має свої особливості	Фокус на унікальних властивостях продукту (AI-аналітика, автоматизована звітність), створення власної ніші на ринку
За рівнем конкурентної боротьби - міжнародний	Конкуренція відбувається на міжнародному рівні, оскільки більшість рішень доступні глобально	Локалізація продукту, врахування місцевих особливостей ринку, забезпечення конкурентних переваг на локальному рівні
За галузевою ознакою - внутрішньогалузева	Конкуренція між компаніями в межах галузі корпоративних	Постійний моніторинг галузевих трендів, впровадження інновацій, підтримка високих стандартів якості

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
	комунікаційних систем	
Конкуренція за видами товарів - товарно-видова	Конкуренція між різними видами корпоративних комунікаційних систем з подібним функціоналом	Розвиток унікальних функцій, покращення користувацького досвіду, створення додаткової цінності через AI-функціонал
За характером конкурентних переваг - нецінова	Конкуренція базується на технологічних перевагах, функціоналі та якості обслуговування	Інвестиції в розвиток технологій, покращення якості сервісу, розширення функціоналу системи
За інтенсивністю - марочна	Бренд має значення при виборі корпоративних рішень	Розвиток бренду, створення репутації надійного постачальника, активний маркетинг та PR

Цей аналіз показує, що ринок корпоративних комунікаційних систем характеризується високим рівнем конкуренції з акцентом на технологічні інновації та якість обслуговування. Для успішної конкуренції компанія повинна зосередитися на розвитку унікальних властивостей продукту, особливо в області

AI-аналітики та автоматизованої звітності, які можуть стати ключовими конкурентними перевагами.

Важливим фактором є також здатність адаптуватися до локальних ринків при збереженні глобальних стандартів якості. Особлива увага має приділятися розвитку бренду та створенню репутації надійного постачальника рішень для корпоративних комунікацій.

У таблиці 5.9 наведено аналіз конкуренції в галузі за М.Портером.

Таблиця 5.9 – Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Визначення та аналіз факторів
Прямі конкуренти в галузі	Microsoft Teams, Slack, Zoom. Високий рівень конкуренції, але є можливості для інновацій
Потенційні конкуренти	Нові стартапи у сфері AI-комунікацій, великі технологічні компанії. Є загроза входу нових гравців, особливо з потужними AI-рішеннями
Постачальники	Провайдери хмарних послуг, постачальники AI-технологій. Невелика кількість постачальників AI-технологій може диктувати умови
Клієнти	Середній та великий бізнес, державні установи. Клієнти вимагають високої якості та безпеки
Товари-замінники	Традиційні засоби комунікації, email-системи. Існуючі рішення мають обмежений функціонал AI-аналітики

За результатами аналізу таблиці можна зробити висновок, що ринок має потенціал для входу нового гравця, незважаючи на наявність сильних конкурентів. Основними факторами успіху можуть стати:

- унікальні технологічні переваги в області AI-аналітики та автоматизованої звітності;
- висока якість захисту даних та відповідність регуляторним вимогам;
- гнучкість у задоволенні специфічних потреб клієнтів;
- конкурентна цінова політика та прозора модель монетизації.

Ці характеристики враховуються при формуванні конкурентоспроможної стратегії виходу на ринок та розвитку продукту. Особливу увагу слід приділити створенню сильних технологічних переваг, які будуть складно відтворити потенційним конкурентам.

На основі проведеного аналізу конкурентного середовища, характеристик проєкту та вимог споживачів, сформовано перелік факторів конкурентоспроможності рішення.

У таблиці 5.10 наведено обґрунтування факторів конкурентоспроможності.

Таблиця 5.10 – Обґрунтування факторів конкурентоспроможності

№ п/п	Фактор конкурентоспроможності	Обґрунтування
1	Інтегрована AI-аналітика	Унікальна можливість автоматичного аналізу корпоративних комунікацій та генерації звітів, що відсутня у більшості конкурентів та значно підвищує ефективність роботи керівників
2	Високий рівень безпеки	Комплексний підхід до захисту даних, що включає шифрування, контроль доступу та відповідність регуляторним вимогам
3	Гнучкість та масштабованість	Можливість легкого масштабування системи та адаптації під потреби різних типів організацій
4	Простота використання	Інтуїтивно зрозумілий інтерфейс та автоматизація рутинних процесів, що знижує поріг входу для користувачів

№ п/п	Фактор конкурентоспроможності	Обґрунтування
5	Інтеграційні можливості	Широкі можливості інтеграції з існуючими корпоративними системами та сервісами
6	Економічна ефективність	Оптимальне співвідношення ціни та функціональності, прозора модель ціноутворення
7	Технічна підтримка	Професійна підтримка та консультації щодо впровадження та використання системи
8	Постійне оновлення	Регулярні оновлення функціоналу та вдосконалення AI-моделей на основі зворотного зв'язку від користувачів

Ці фактори формують комплексну конкурентну перевагу рішення на ринку корпоративних комунікацій. Особливо важливим є поєднання інноваційного AI-функціоналу з високим рівнем безпеки та простотою використання, що відповідає ключовим вимогам цільової аудиторії.

За всіма визначеними факторами проєкт має значні переваги або знаходиться на рівні з конкурентами, що створює міцну основу для успішного виходу на ринок та подальшого розвитку.

На основі визначених факторів конкурентоспроможності проведемо детальний аналіз сильних та слабких сторін стартап-проєкту порівняно з основними конкурентами. Цей аналіз допоможе краще зрозуміти конкурентну позицію проєкту та визначити напрямки для подальшого розвитку.

Порівняльний аналіз сильних та слабких сторін Системи захищеного обміну інформаціює в офісі наведено у таблиці 5.11.

Таблиця 5.11 – Порівняльний аналіз сильних та слабких сторін Системи захищеного обміну інформаціює в офісі

№ п/п	Фактор конкурентоспроможності	Бали 1-20	Рейтинг товарів-конкурентів						
			-3	-2	-1	0	1	2	3
1	Інтегрована AI-аналітика	18			+				+
2	Високий рівень безпеки	17						+	
3	Гнучкість та масштабованість	16					+		
4	Простота використання	15			+				
5	Інтеграційні можливості	14				+			
6	Економічна ефективність	19	+						
7	Технічна підтримка	15				+			
8	Постійне оновлення	16					+		

Аналіз показує, що проєкт має найсильніші позиції в сферах інтегрованої AI-аналітики та економічної ефективності, де значно випереджає конкурентів. Це пов'язано з унікальним підходом до автоматизації аналізу комунікацій та оптимальною ціновою політикою. Також сильними сторонами є високий рівень безпеки та інтеграційні можливості.

Водночас, у таких аспектах як технічна підтримка та простота використання, проєкт знаходиться приблизно на одному рівні з конкурентами або має незначне відставання. Це вказує на необхідність додаткової уваги до розвитку служби підтримки та вдосконалення користувацького інтерфейсу.

Загалом, аналіз підтверджує конкурентоспроможність проєкту на ринку, особливо завдяки унікальним технологічним перевагам та оптимальному співвідношенню ціна/якість. Для підтримки та посилення конкурентних позицій необхідно продовжувати розвиток AI-функціоналу та покращувати якість обслуговування клієнтів.

Для стартап-проєкту який є унікальним продуктом на українському ринку, SWOT-аналіз дозволяє краще оцінити його потенціал та ризики в контексті

специфіки локального середовища. Унікальність продукту як першого на ринку платформи оренди житла із застосуванням блокчейн-технологій створює як конкурентні переваги, так і виклики, пов’язані з впровадженням інновацій. Результати аналізу наведені в таблиці 5.12.

Таблиця 5.12 – SWOT-аналіз стартап-проєкту

Сильні сторони: – унікальна AI-аналітика корпоративних комунікацій; – високий рівень безпеки та шифрування даних; – оптимальне співвідношення ціна/якість; – гнучкість та масштабованість системи; – інтеграція з існуючими корпоративними системами	Слабкі сторони: – відсутність сформованої клієнтської бази; – обмежені фінансові ресурси на початковому етапі; – менший досвід на ринку порівняно з конкурентами; – залежність від зовнішніх постачальників AI-технологій; – потреба у значних інвестиціях у розвиток продукту
Можливості: – зростання попиту на захищені комунікаційні системи; – розвиток технологій AI для покращення аналітики; – збільшення кількості компаній з віддаленими командами – державні програми підтримки цифровізації; – зростання інтересу інвесторів до AI-проєктів	Загрози: – вихід на ринок нових конкурентів з аналогічними рішеннями; – зміни в регуляторних вимогах щодо захисту даних; – економічна нестабільність та зменшення IT-бюджетів; – швидка зміна технологій може вимагати значних інвестицій; – можливі проблеми з безпекою та витоки даних

На основі SWOT-аналізу розроблено три альтернативні стратегії розвитку проєкту. Перша стратегія спрямована на посилення позицій та передбачає використання сильних сторін, зокрема унікальної AI-аналітики та високої безпеки, для максимального використання можливостей зростаючого ринку. Також вона включає розвиток партнерств з постачальниками технологій для зменшення залежності та активне залучення інвестицій для швидкого масштабування.

Друга стратегія фокусується на компенсації слабких сторін через формування клієнтської бази шляхом активного маркетингу та демонстрації

унікальних переваг продукту. Важливими елементами цієї стратегії є залучення досвідчених фахівців для посилення експертизи та розробка власних AI-компонентів для зменшення залежності від зовнішніх постачальників.

Третя стратегія спрямована на нейтралізацію загроз та включає постійний моніторинг і адаптацію до регуляторних змін, створення фінансового резерву для стабільного розвитку в умовах економічної нестабільності, а також впровадження додаткових рівнів безпеки для запобігання можливим витокам даних.

Проведений SWOT-аналіз показує значний потенціал проєкту для успішного розвитку, особливо враховуючи його сильні технологічні сторони та сприятливі ринкові можливості. При цьому необхідно приділяти постійну увагу мінімізації виявлених ризиків та компенсації слабких сторін для забезпечення стабільного росту та розвитку проєкту.

На основі проведеного SWOT-аналізу розробимо можливі альтернативи ринкової поведінки для успішного виведення нашого проєкту на ринок, що зображені у Таблиці 5.13.

Таблиця 5.13 – Альтернативи ринкового впровадження стартап-проєкту

№ п/п	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
1	Швидкий вихід на ринок з базовим функціоналом та поступове додавання AI-можливостей	Висока (потребує мінімальних початкових інвестицій)	6-8 місяців
2	Фокус на великих корпоративних клієнтах з повним набором функцій	Середня (потребує значних ресурсів на розробку)	12-15 місяців
3		Висока (взаємовигідна співпраця)	4-6 місяців

№ п/п	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
	Партнерство з існуючими провайдерами корпоративних рішень		
4	Створення free-версії для швидкого залучення користувачів	Висока (мінімальні витрати на початковому етапі)	3-4 місяці
5	Розвиток через галузеву спеціалізацію (фокус на конкретних індустріях)	Середня (потребує глибокого вивчення галузевих потреб)	8-10 місяців

З наведених альтернатив найбільш привабливою видається стратегія партнерства з існуючими провайдерами корпоративних рішень. Ця альтернатива має високу ймовірність отримання необхідних ресурсів та відносно короткі строки реалізації. Партнерство дозволить використати існуючі канали дистрибуції та клієнтську базу партнерів, одночасно пропонуючи їм додаткову цінність через наші AI-можливості.

Другою за привабливістю є стратегія створення free-версії, яка дозволить швидко набрати користувацьку базу та отримати цінний зворотний зв'язок для подальшого розвитку продукту. Ця стратегія також має високу ймовірність реалізації та короткі строки впровадження.

Інші альтернативи, хоча і мають потенціал, вимагають більше часу та ресурсів для реалізації, що підвищує ризики проєкту на початковому етапі.

5.4 Розроблення ринкової стратегії проєкту

На основі проведеного аналізу ринку та потенційних споживачів, важливо визначити стратегію охоплення ринку для системи захищеного обміну інформацією в офісі. Правильний вибір цільових груп споживачів та стратегії роботи з ними є критично важливим для успішного впровадження проєкту на ринку.

Ринок корпоративних комунікаційних систем характеризується різноманітністю потенційних споживачів - від малих компаній до великих корпорацій, кожна з яких має свої специфічні потреби та вимоги. При цьому важливо враховувати готовність різних сегментів до впровадження інноваційних технологій, зокрема систем з інтегрованою AI-аналітикою.

При виборі цільових груп необхідно оцінити не лише їх потенційний попит, але й готовність до впровадження нових технологій, інтенсивність конкуренції в кожному сегменті та складність входу в нього. Це дозволить визначити найбільш перспективні напрямки для розвитку проєкту та оптимальну стратегію роботи з кожною групою споживачів. Результати аналізу потенційних груп споживачів представлено в таблиці 5.14.

Таблиця 5.14 – Вибір цільових груп потенційних споживачів

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи	Інтенсивність конкуренції в сегменті	Простота входу в сегмент
1	Середні та великі підприємства з розподіленими командами	Висока, через зростаючу потребу в захищених комунікаціях та аналітиці	Значний, особливо в умовах тренду на віддалену роботу	Середня, через специфічність AI-функціоналу	Середня, потрібна демонстрація переваг системи

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи	Інтенсивність конкуренції в сегменті	Простота входу в сегмент
2	IT-компанії та технологічні стартапи	Висока, через технологічну обізнаність та готовність до інновацій	Високий, через активне використання цифрових комунікацій	Висока, через технологічну грамотність клієнтів	Висока, швидке прийняття нових технологій
3	Фінансові установи та організації з суворими регуляторними вимогами	Середня, через консервативність та високі вимоги до безпеки	Стабільний, через постійну потребу в захищених комунікаціях	Низька в сегменті AI-аналітики	Низька, через суворі вимоги до безпеки
4	Державні установи та організації	Низька через бюрократичні процедури та обмежені бюджети	Потенційно високий через масштаб сектору	Низька, особливо в сегменті AI-рішень	Складна через специфіку держзакупівель
Для цільових груп буде розроблено стратегію диференційованого маркетингу, яка враховує специфіку кожного сегмента. У фокусі – залучення широкої аудиторії через інформаційні кампанії, просування переваг безпеки та інноваційності.					

Основною цільовою аудиторією обрано середні та великі підприємства з розподіленими командами та IT-компанії (групи 1 та 2), оскільки вони:

- демонструють високу готовність до впровадження нових технологій;
- мають значний попит на подібні рішення;
- здатні швидко оцінити переваги AI-аналітики;

- мають достатній бюджет для впровадження.

За результатами аналізу груп споживачів та їх характеристик доцільно обрати стратегію диференційованого маркетингу. Така стратегія дозволить:

- адаптувати продукт під специфічні потреби кожного сегмента;
- розробити окремі програми просування для різних цільових груп;
- забезпечити максимальне охоплення цільової аудиторії;
- підвищити ефективність маркетингових зусиль через фокусування на конкретних перевагах продукту для кожного сегмента.

Таке рішення обґрунтовано різними потребами та характеристиками обраних сегментів, що вимагає індивідуального підходу до кожної групи клієнтів.

На основі проведеного аналізу цільових груп споживачів та специфіки продукту необхідно визначити базову стратегію розвитку проєкту. Правильний вибір базової стратегії є критично важливим для успішного позиціонування на ринку та досягнення конкурентних переваг.

Враховуючи унікальність пропонованого рішення, зокрема наявність інтегрованої AI-аналітики та функцій автоматизованої звітності, а також орієнтацію на специфічні потреби корпоративних клієнтів, доцільно розглянути можливі стратегічні альтернативи розвитку.

Результати аналізу та вибору базової стратегії розвитку представлено в таблиці 5.15.

Таблиця 5.15 – Визначення базової стратегії розвитку

№ п/п	Обрана альтернатива розвитку проєкту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
1	Створення інноваційної системи корпоративн	Диференційований маркетинг	Унікальний AI-функціонал для аналізу комунікацій, високий рівень	Стратегія диференціації

№ п/п	Обрана альтернатива розвитку проєкту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
	их комунікацій з інтегрованою AI-аналітикою		безпеки та захисту даних, автоматизована генерація звітності, гнучкість налаштування під потреби клієнта, інтеграція з існуючими корпоративними системами	

Обрана стратегія диференціації базується на наступних конкурентних перевагах:

- унікальність пропонованого рішення з точки зору AI-функціоналу;
- висока цінність продукту для корпоративних клієнтів;
- можливість встановлення преміальної ціни за рахунок унікальних характеристик;
- створення сильного бренду в сегменті корпоративних комунікацій.

Така стратегія дозволить компанії зайняти сильні позиції на ринку та забезпечити високу рентабельність за рахунок унікальних властивостей продукту, які цінуються цільовою аудиторією.

У таблиці 5.16 представлено аналіз для вибору базової стратегії конкурентної поведінки.

Таблиця 5.16 – Вибір базової стратегії конкурентної поведінки

№ п/п	Чи є проєкт «першопрохідцем» на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки
1	Ні, на ринку існують рішення для корпоративних комунікацій, але без розвинутої AI-аналітики	Компанія буде як залучати нових споживачів, так і пропонувати рішення існуючим користувачам інших систем	Базовий функціонал комунікацій буде схожим з існуючими рішеннями, але з унікальними інноваціями в області AI-аналітики та автоматизованої звітності	Стратегія виклику лідера

Хоча проєкт не є першопрохідцем на ринку корпоративних комунікацій, він пропонує інноваційний підхід через інтеграцію AI-технологій для аналізу комунікацій та автоматизації звітності. Стратегія виклику лідера базується на пропозиції більш технологічно досконалого рішення, що дозволить ефективно конкурувати з існуючими гравцями ринку.

При цьому компанія зберігає стандартний базовий функціонал, необхідний для корпоративних комунікацій, доповнюючи його унікальними можливостями, що створює додаткову цінність для користувачів. Така стратегія дозволить залучати як нових клієнтів, так і переконувати існуючих користувачів інших систем перейти на більш функціональне рішення.

На основі проведених раніше досліджень можемо визначити стратегію позиціонування системи захищеного обміну інформацією в офісі. Важливо сформувати чітку ринкову позицію, яка відображатиме ключові переваги продукту та відповідатиме очікуванням цільової аудиторії.

Користуючись даними про вимоги споживачів, обрану стратегію розвитку та конкурентної поведінки, розроблено комплекс рішень щодо позиціонування проєкту на ринку. Результати представлено у таблиці 5.17.

Таблиця 5.17 – Визначення стратегії позиціонування

№ п/п	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап-проєкту	Вибір асоціацій, які мають сформувати комплексну позицію власного проєкту (три ключових)
1	Високий рівень безпеки та захисту даних, простота використання	Стратегія диференціації	Інтегрована AI-аналітика для автоматичного аналізу корпоративних комунікацій, надійна система шифрування даних	Інновації, безпека, ефективність
2	Автоматизація рутинних процесів, економія часу керівників	Стратегія диференціації	Автоматична генерація звітів та аналітики на основі комунікацій, інтуїтивно зрозумілий інтерфейс	Автоматизація, зручність, продуктивність
3	Інтеграція з існуючими системами, масштабованість	Стратегія диференціації	Гнучка система налаштувань, широкі можливості інтеграції з корпоративними системами	Інтеграція, надійність, масштабованість

Така система рішень щодо ринкової поведінки дозволить компанії сформувати сильну позицію на ринку корпоративних комунікаційних систем. Обрана стратегія позиціонування відповідає очікуванням цільової аудиторії та підкреслює унікальні переваги продукту, зокрема в області AI-аналітики та автоматизації процесів.

Важливим аспектом реалізації стратегії стане послідовна комунікація обраних позицій через всі маркетингові канали. Це дозволить сформувати чітке сприйняття бренду серед потенційних клієнтів та забезпечити стійкі конкурентні переваги на ринку.

Розроблена стратегія враховує як технологічні переваги продукту, так і специфічні потреби корпоративних клієнтів, що створює міцну основу для успішного розвитку проєкту на ринку захищених корпоративних комунікацій.

5.5 Розроблення маркетингової програми стартап-проєкту

На основі проведеного аналізу конкурентоспроможності у таблиці 5.18 визначено ключові переваги системи, які отримають споживачі.

Таблиця 5.18 – Визначення основних переваг концепції потенційного товару

№ п/п	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентом
1	Захищений обмін корпоративною інформацією	Комплексна система безпеки з шифруванням даних та контролем доступу	Інтеграція сучасних методів шифрування з гнучким управлінням правами доступу, що забезпечує вищий рівень захисту порівняно з типовими рішеннями
2	Автоматизація аналізу комунікацій	Вбудована AI-аналітика для обробки всіх типів	Унікальна можливість автоматичного аналізу та узагальнення інформації з різних

№ п/п	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентом
		корпоративних комунікацій	каналів комунікації, відсутня у конкурентів
3	Автоматизована звітність	Автоматична генерація структурованих звітів на основі аналізу комунікацій	Значна економія часу керівників на підготовку звітності завдяки використанню AI для обробки та узагальнення даних
4	Інтеграція з існуючими системами	Гнучкі можливості інтеграції з корпоративними системами через API	Розширені можливості налаштування та адаптації під існуючу IT-інфраструктуру клієнта
5	Простота використання	Інтуїтивно зрозумілий інтерфейс та автоматизація рутинних операцій	Мінімальний час на навчання користувачів та висока ефективність щоденної роботи з системою

Запропонована система надає користувачам комплексне рішення для організації захищених корпоративних комунікацій з унікальними можливостями AI-аналітики. Ключові переваги перед конкурентами базуються на інноваційному підході до автоматизації процесів аналізу інформації та формування звітності, що суттєво підвищує ефективність роботи користувачів. При цьому система забезпечує високий рівень безпеки та зручності використання, що відповідає основним вимогам корпоративних клієнтів.

У Таблиці 5.19 визначено цінові межі для системи захищеного обміну інформацією в офісі, базуючись на аналізі ринку та цільової аудиторії.

Таблиця 5.19 – Визначення меж встановлення ціни

№ п/п	Рівень цін на послуги замінники	Рівень цін на товари аналоги	Рівень доході в цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
1	Microsoft Teams: $8-20 за користувача/місяць	Системи з базовою AI-аналітикою: $15-35 за користувача/місяць	Середній та великий бізнес з IT-бюджетом від $100,000 на рік	Нижня межа: $12 за користувача/місяць
2	Slack: $6.67-12.50 за користувача/місяць	Enterprise-рішення для захищених комунікацій: $25-50 за користувача/місяць	Середній та великий бізнес з IT-бюджетом від $100,000 на рік	Верхня межа: $30 за користувача/місяць

При встановленні цінових меж враховувались наступні фактори:

- ціни існуючих рішень на ринку корпоративних комунікацій;
- додаткова цінність, яку створює AI-аналітика та автоматизована звітність;
- платоспроможність цільової аудиторії;
- витрати на розробку та підтримку системи;
- необхідність забезпечення конкурентоспроможності продукту;

Запропонований ціновий діапазон дозволяє позиціонувати продукт як преміальне рішення з унікальним функціоналом, залишаючись при цьому конкурентоспроможним відносно існуючих enterprise-рішень. Гнучка цінова

політика передбачає можливість формування індивідуальних пропозицій для великих клієнтів та спеціальних умов при довгостроковій співпраці.

Аналіз цільових груп клієнтів показує, що основними потребами, які формують ринковий попит, є:

- аабезпечення надійного захисту конфіденційної інформації при корпоративних комунікаціях;
- автоматизація аналізу комунікацій та формування звітності;
- централізоване управління корпоративними комунікаціями з дотриманням регуляторних вимог.

Для успішного впровадження стартап-проекту необхідно ретельно продумати систему збуту продукту, яка буде оптимальною для даної системи. Проаналізувавши специфіку ІТ-галузі та особливості ринку корпоративних комунікаційних систем, сформовано рекомендації щодо системи збуту, представлені в Таблиці 5.20.

Таблиця 5.20 – Формування системи збуту

№ п/п	Специфіка закупівельної поведінки цільових клієнтів	Функції які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
1	Корпоративні клієнти (середні та великі компанії) приймають рішення про закупівлю на основі комплексного аналізу функціональності, безпеки, можливостей інтеграції з існуючими системами. Процес	Проведення демонстрацій та надання пробного періоду використання; консультування щодо інтеграції з існуючими системами; навчання	Прямий продаж кінцевому споживачу, особливо на етапі виведення продукту на ринок.	Власна система збуту, яка передбачає прямі продажі через відділ продажів компанії та її сайт. На початкових етапах це дозволить краще контролювати

№ п/п	Специфіка закупівельної поведінки цільових клієнтів	Функції які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
	прийняття рішення достатньо тривалий і вимагає залучення різних департаментів (IT, безпеки, фінансів).	користувачів; надання цілодобової технічної підтримки; оперативне усунення можливих проблем в роботі системи.		процес продажів, отримувати зворотній зв'язок від клієнтів та гнучко адаптувати продукт під їх потреби.

На основі аналізу специфіки закупівельної поведінки цільових клієнтів та функцій, які має виконувати постачальник, рекомендовано використовувати власну систему збуту з прямими продажами корпоративним клієнтам.

Враховуючи складність продукту та необхідність тісної взаємодії з клієнтом на етапі впровадження, використання посередників на початковому етапі є недоцільним. В майбутньому, при розширенні клієнтської бази, можливе залучення сертифікованих партнерів для масштабування збуту, але з обов'язковим контролем якості з боку компанії.

Сформована система збуту відповідає ринковим реаліям та дозволить стартапу ефективно виводити продукт на ринок, контролювати процес продажів та налагоджувати тісні зв'язки з клієнтами для подальшого розвитку.

Останнім етапом формування маркетингової програми є розробка концепції маркетингових комунікацій. Вона базується на попередньо обраній стратегії позиціонування, особливостях закупівельної поведінки цільових клієнтів, а також

враховує специфіку ринку корпоративних комунікаційних систем. Розроблена концепція представленя у Таблиці 5.21.

Таблиця 5.21 – Концепції маркетингових комунікацій

№ п/п	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції обрані для позиціонування	Завдання рекламного повідомлення
1	Рішення про впровадження нової корпоративної системи приймається колегіально з урахуванням думки різних департаментів (IT, безпеки, фінансів); ключову роль відіграє можливість інтегрувати рішення з існуючою інфраструктурою	Професійні IT видання та блоги, галузеві конференції, прямі переговори та презентації, рекомендації колег та партнерів	Інноваційна система корпоративних комунікацій з вбудованою AI-аналітикою для автоматичного аналізу комунікацій та генерації звітів; високий рівень безпеки, простота інтеграції з існуючими системами	Донести ключові переваги системи, продемонструвати, як вона допоможе підвищити ефективність комунікацій, спростити процес аналізу даних та прийняття рішень, забезпечуючи при цьому високий рівень безпеки та конфіденційності

№ п/п	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції обрані для позиціонування	Завдання рекламного повідомлення
	та навчити співробітників роботі з ним			

Враховуючи цільову аудиторію проекту - середні та великі підприємства, а також ІТ-компанії, основний фокус маркетингових комунікацій має бути на донесенні реальної цінності та переваг продукту для бізнесу.

Канали комунікації мають включати як онлайн, так і офлайн інструменти. Зокрема, ефективними будуть публікації та реклама в професійних ІТ виданнях, участь у галузевих конференціях та виставках, проведення вебінарів та прямих презентацій для потенційних клієнтів. Важливу роль відіграватиме також робота з лідерами думок в індустрії, партнерський маркетинг та програми референтних клієнтів.

Загалом, розроблена концепція маркетингових комунікацій дозволить ефективно донести ключові переваги продукту до цільової аудиторії, сформувати правильне позиціонування та сприйняття бренду, а також стимулювати попит та залучення нових клієнтів. В поєднанні з іншими елементами маркетингової програми це створить міцну основу для успішного виходу стартапу на ринок.

Висновки до розділу 5

У цьому розділі було детально розглянуто концепцію стартап-проєкту, спрямованого на створення системи захищеного обміну інформацією в офісі з інтегрованими функціями AI-аналітики. Проведений аналіз дозволив визначити основні переваги ідеї, такі як безпека, автоматизація рутинних процесів, зокрема підготовка звітності, а також гнучка інтеграція з корпоративними системами. Увага до потреб кінцевих користувачів, які орієнтуються на захищеність і простоту використання, сприяє формуванню сильних ринкових позицій.

Особливу увагу було приділено аналізу конкурентного середовища, включаючи оцінку основних гравців на ринку корпоративних комунікацій, таких як Microsoft Teams, Slack та Zoom, а також їх обмеження у сфері автоматизованої AI-аналітики. Це дозволяє системі проєкту позиціонувати себе як інноваційне рішення з унікальним функціоналом, яке відповідає сучасним викликам цифровізації бізнесу.

Крім того, у розділі наведено обґрунтування ринкової стратегії, яка охоплює як вибір цільових груп споживачів, так і методи просування продукту. Використання сценаріїв швидкого виходу на ринок із базовим функціоналом, поступового впровадження AI-можливостей та адаптації до потреб галузевих клієнтів створює основу для довгострокового розвитку стартапу.

Отже, сформульовані у розділі висновки та пропозиції демонструють готовність стартапу до впровадження інноваційної системи на конкурентному ринку, що забезпечить його технологічну перевагу та сталий розвиток.

ВИСНОВКИ

В результаті виконання магістерської дисертації було розроблено систему захищеного обміну інформацією в офісі з інтегрованими функціями штучного інтелекту для автоматизації аналізу комунікацій та формування звітності. В ході роботи було досягнуто всіх поставлених цілей та вирішено ключові завдання проєкту.

Проведений аналіз існуючих рішень у сфері корпоративних комунікацій виявив суттєві обмеження сучасних платформ, особливо в контексті автоматизованої обробки та аналізу інформації. Хоча такі системи як Microsoft Teams, Slack та інші забезпечують базові потреби в комунікації, вони не надають інструментів для глибокого аналізу комунікаційних даних та автоматизованого формування аналітичної звітності. Це створило передумови для розробки інноваційного рішення, що поєднує функції захищених комунікацій з можливостями штучного інтелекту.

Розроблена система базується на сучасній розподіленій архітектурі, що забезпечує високу надійність та масштабованість. Використання Spring Framework для серверної частини та React для клієнтського інтерфейсу дозволило створити гнучку та ефективну платформу. Особливу увагу приділено безпеці даних через впровадження двошарового шифрування, де серверний рівень захищає дані при зберіганні, а транспортний – при передачі.

Ключовою інновацією розробленої системи є інтеграція з Google Gemini API для реалізації функцій штучного інтелекту. Це дозволило автоматизувати процеси аналізу комунікацій та формування звітності, що суттєво підвищує ефективність роботи керівників та проєктних команд. Система здатна автоматично виявляти ключові теми обговорень, відслідковувати прогрес проєктів та генерувати структуровані звіти на основі аналізу всіх каналів комунікації.

Реалізована система ролей та прав доступу забезпечує гнучке управління користувачами та їх повноваженнями. Адміністратори та менеджери мають розширені можливості для управління проєктами та командами, в той час як

звичайні користувачі отримують зручний інтерфейс для щоденної роботи та комунікації. Використання JWT токенів та надійних механізмів автентифікації гарантує безпечний доступ до системи.

В процесі розробки було реалізовано ефективні механізми інтеграції з корпоративними системами через REST API та WebSocket протоколи. Це створює можливості для розширення функціоналу та адаптації системи під специфічні потреби різних організацій. Використання контейнеризації на базі Docker спрощує процеси розгортання та масштабування системи.

Розроблена система має значний комерційний потенціал, що підтверджується результатами аналізу ринку та розробленим стартап-проєктом. Унікальне поєднання функцій захищених комунікацій з можливостями AI-аналітики створює сильні конкурентні переваги на ринку корпоративних комунікаційних систем.

Подальший розвиток системи може включати вдосконалення алгоритмів AI-аналізу, розширення можливостей інтеграції та впровадження додаткових функцій автоматизації бізнес-процесів. Особлива увага буде приділена розвитку механізмів машинного навчання для покращення якості аналізу та персоналізації роботи системи під потреби конкретних організацій.

В цілому, розроблена система представляє собою інноваційне рішення, що відповідає сучасним вимогам до корпоративних комунікацій та створює нові можливості для підвищення ефективності роботи організацій через автоматизацію процесів аналізу інформації та прийняття рішень.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Microsoft Teams Documentation. URL: https://learn.microsoft.com/en-us/microsoftteams/

2. Slack Developer Documentation. URL: https://api.slack.com/docs/

3. Mattermost Documentation. URL: https://docs.mattermost.com/

4. Symphony Developer Documentation. URL: https://docs.developers.symphony.com/

5. Zoom Developer Documentation. URL: https://developers.zoom.us/docs/

6. Telegram Enterprise Documentation. URL: https://core.telegram.org/

7. Spring Framework Documentation. URL: https://docs.spring.io/spring-framework/reference/

8. PostgreSQL Documentation. URL: https://www.postgresql.org/docs/

9. Google Gemini API Documentation. URL: https://ai.google.dev/docs

10. WebSocket.io Documentation. URL: https://socket.io/docs/v4/

11. JWT Authentication Guide. Auth0 Documentation. URL: https://auth0.com/docs/authenticate

12. Docker Documentation. URL: https://docs.docker.com/

13. Redux Documentation. URL: https://redux.js.org/

14. Gerald Beuchelt. Enterprise Security Architecture: A Guide to Infrastructure Protection. CRC Press, 2023. 328 p.

15. Michael T. Simpson. Hands-On Cybersecurity for Architects: Plan and design robust security architectures. Packt Publishing, 2023. 574 p.

16. Tailwind CSS Documentation. URL: https://tailwindcss.com/docs

17. Node.js Documentation. URL: https://nodejs.org/docs/latest/api/

18. WebSocket Protocol RFC 6455. URL: https://tools.ietf.org/html/rfc6455

19. Basics of Cryptographic Algorithms. URL: https://www.geeksforgeeks.org/basics-of-cryptographic-algorithms/