Організація безпечних цифрових комунікацій на основі месенджера з AES-шифруванням

Максим Сорокін
здобувач освітньої програми «Комп'ютерні науки»,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
e-mail: sorokinmv@krok.edu.ua
Олександр Орлов
здобувач освітньої програми «Комп'ютерні науки»,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
e-mail: orlovov@krok.edu.ua
Віра Ткаченко
к.ф.-м.н., доцент, доцент кафедри інформаційного,
менеджменту, математики та статистики,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
e-mail: tkachenkov@krok.edu.ua,
ORCID: 0000-0001-6064-5474

У сучасних умовах цифрової трансформації бізнес-процесів усе більшої актуальності набуває питання організації безпечної внутрішньої комунікації в установах та організаціях. Широке використання сторонніх комунікаційних сервісів, які не завжди гарантують належний рівень конфіденційності, створює ризики витоку чутливої інформації, зокрема у корпоративному середовищі. Тому впровадження захищених засобів комунікації, орієнтованих на локальне використання, є доцільним і своєчасним кроком у сфері інформаційного менеджменту.

Метою дослідження стало створення корпоративно-орієнтованого месенджера з відкритим вихідним кодом та реалізацією наскрізного шифрування за допомогою алгоритму AES, що забезпечує відповідність сучасним вимогам інформаційної безпеки та дозволяє повністю контролювати передачу даних без залучення сторонніх сервісів. У процесі розробки здійснено аналіз існуючих рішень, таких як IRC, XMPP та Matrix, що дало змогу виявити низку їхніх обмежень: відсутність сучасного шифрування, застарілий або перевантажений інтерфейс, складність налаштування серверної частини або ненадійність інфраструктури.

Основні вимоги до програмного забезпечення було сформульовано з урахуванням потреб корпоративного користувача. Функціональною основою є забезпечення високого рівня безпеки переданих даних, можливості реєстрації, авторизації, персоналізації профілю, створення та адміністрування чатів, обміну повідомленнями, файлами та медіа в режимі реального часу. Нефункціональні вимоги включають стабільну роботу клієнта, зручність інтерфейсу та його адаптивність до різних пристроїв. Особливістю реалізації шифрування є генерація окремого AES-ключа для кожного чату, що унеможливлює доступ до повідомлень сторонніми особами, навіть у разі компрометації серверної частини.

Для реалізації програмного забезпечення використовувались мова

програмування Python, бібліотека cryptography для шифрування, а також засоби розробки інтерфейсу на основі Tkinter і ttkbootstrap. У процесі реалізації виконано моделювання структури бази даних, розроблено протокол взаємодії між клієнтом і сервером.

Окрему увагу приділено дослідженню майбутньої користувацької аудиторії: сформовано орієнтовний портрет типового користувача, проаналізовано його очікування та ключові потреби в контексті щоденної комунікації в корпоративному середовищі. На основі отриманих даних створено макет інтерфейсу, який спочатку було реалізовано у вигляді низькодеталізованого прототипу у Figma, а згодом зверстано та інтегровано у функціональну програмну частину застосунку.

При розробці UI/UX-дизайну безпосередньо враховувались результати дослідження користувацької аудиторії та загальні принципи сучасної побудови інтерфейсів: логічне розташування елементів, мінімалістичний стиль, підтримка темного та світлого режимів, а також використання анімацій і підказок, орієнтованих на нових користувачів. Особлива увага приділялася доступності та зменшенню когнітивного навантаження під час навігації між чатами, налаштуваннями профілю та повідомленнями. Інтерфейс забезпечує швидкий доступ до основних функцій і дозволяє легко орієнтуватися в системі навіть користувачам без спеціальної підготовки.

Розроблений застосунок дозволить забезпечити безпечну та ефективну взаємодію всередині організацій, мінімізуючи ризики витоку інформації, що передається, та сприятиме підвищенню рівня цифрової зрілості установ у частині інформаційної безпеки. У подальшому можливе розширення функціональності, інтеграція з іншими системами підприємства та масштабування на рівні розподілених організаційних структур.

Ключові слова: кібербезпека, месенджер, AES, AES-256, шифрування, UI/UX дизайн, інформаційний менеджмент.

Список використаних джерел

1. Intel. Securing the Enterprise with Intel AES-NI [Електронний ресурс]. – Режим доступу: https://www.intel.in/content/dam/doc/white-paper/enterprise-security-aes-ni-white-paper.pdf. – Дата звернення: 10.03.2025.

2. Splashtop. AES Encryption: How it works, Benefits, and Use Cases [Електронний ресурс]. – Режим доступу: https://www.splashtop.com/blog/aes-encryption?srsltid=AfmBOoq8JKcQPR06303OfTrbuMBR7lS0ABIXkz3SW90GXG0G2xm59fzv. – Дата звернення: 10.03.2025.

3. Justinmind. UI design principles: guidelines [Електронний ресурс]. – Режим доступу: https://www.justinmind.com/ui-design/principles. – Дата звернення: 20.03.2025.