Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Лакоценіна Захара Євгенійовича

на здобуття ступеня вищої освіти магістра

Метод криптографічного захисту інформації в корпоративних чатах

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека та захист інформації
Освітня програма Кібербезпека та захист інформації

Шифр КРМКБЗІ. 2301143.23.11.13 ПЗ

Виконав студент 2 курсу група КБЗІм-23-1 Захар ЛАКОЦЕНІН

Керівник канд. техн. наук, доцент Віра ТІТОВА

Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

2 12 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій
Кафедра Кібербезпеки
Рівень вищої освіти Магістр
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека та захист інформації
Освітня програма Кібербезпека та захист інформації

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
Юрій КЛЬОЦ _____
2 09 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Лакоценіну Захару Євгенійовичу

1 Тема роботи Метод криптографічного захисту інформації в корпоративних чатах

_____

Керівник роботи канд.техн.наук, доцент Віра ТІТОВА
Затверджено наказом ректора університету від 26 08 2024 № 60
2 Строк подання студентом кваліфікаційної роботи на кафедру _____
3 Вихідні дані до роботи Метод криптографічного захисту інформації в корпоративних чатах

_____
_____

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз існуючих методів криптографічного захисту інформації. Постановка задачі. Проєктування методу криптографічного захисту. Реалізація та тестування запропонованого методу. Впровадження та оцінка ефективності. Висновки.

_____
_____
_____

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

_____
_____
_____

6 Консультанти розділів кваліфікаційної роботи

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

7 Дата видачі завдання 2 09 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Ґрунтовне ознайомлення та дослідження предметної галузі		Виконано
Визначення змісту, структури кваліфікаційної роботи		Виконано
Підготовка першого розділу кваліфікаційної роботи		Виконано
Підготовка другого розділу кваліфікаційної роботи		Виконано
Підготовка третього розділу кваліфікаційної роботи		Виконано
Підготовка статті/тези за темою кваліфікаційної роботи		Виконано
Підготовка четвертого розділу кваліфікаційної роботи		Виконано
Підготовка та оформлення ілюстративного матеріалу		Виконано
Оформлення кваліфікаційної роботи		Виконано
Попередній захист кваліфікаційної роботи		Виконано
Захист кваліфікаційної роботи на засіданні ЕК		

Студент _____ Захар ЛАКОЦЕНІН

Керівник кваліфікаційної роботи _____ Віра ТІТОВА

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Метод криптографічного захисту інформації в корпоративних чатах».

Автор роботи: Лакоценін Захар Євгенійович.

Керівник роботи: к.т.н, доц. Тітова Віра Юріївна.

Загальний обсяг роботи: 88 сторінок, 15 рисунків, 7 таблиць, 3 додатки, 60 посилань.

Ключові слова: криптографічний захист, корпоративні чати, управління ключами, інформаційна безпека, протоколи шифрування.

Мета даної роботи полягає у розробці методу криптографічного захисту інформації в корпоративних чатах, що забезпечує високий рівень конфіденційності та цілісності переданих повідомлень.

У роботі виконано аналіз існуючих засобів захисту інформації в корпоративних комунікаціях, розроблено метод шифрування, адаптований для динамічного обміну повідомленнями, а також запропоновано алгоритми управління ключами для захисту корпоративних чатів. Проведено тестування розробленого методу, яке підтвердило його ефективність у протидії перехопленню та несанкціонованому доступу до даних.

Результати роботи можуть бути впроваджені у корпоративних середовищах для покращення захисту інформації, що передається у внутрішніх чатах компаній, а також у сфері хмарних технологій і цифрових комунікацій.

02.12.2024

ANNOTATION

Topic of the qualification thesis: "Method for Cryptographic Protection of Information in Corporate Chats."

Author of the work: Lakotsenin Zakhar Yevheniiovych.

Mentor: PhD, Assoc. Prof. Titova Vira Yuriyivna.

Total volume of the work: 88 pages, 15 figures, 7 tables, 3 appendices, 60 references.

Keywords: cryptographic protection, corporate chats, key management, information security, encryption protocols.

The aim of this thesis is to develop a method for cryptographic protection of information in corporate chats to ensure a high level of confidentiality and integrity of transmitted messages.

The study analyzes existing tools for securing information in corporate communications, proposes an encryption method adapted for dynamic message exchanges, and introduces key management algorithms for securing corporate chats. The proposed method was tested and proved effective in countering interception and unauthorized access to data.

The results of this work can be implemented in corporate environments to enhance the protection of information transmitted through internal company chats, as well as in the field of cloud technologies and digital communications.

02.12.2024

ЗМІСТ

ВСТУП

У сучасному світі, де бізнес-процеси невід’ємно пов’язані з цифровими технологіями, ефективна комунікація між співробітниками є ключовим фактором для успішного функціонування будь-якої організації. Одним із найбільш розповсюджених інструментів корпоративної комунікації стали чати, які забезпечують миттєвий та зручний обмін інформацією в реальному часі. Ці платформи дозволяють співробітникам здійснювати обговорення важливих питань, таких як стратегічні рішення, розробка нових проєктів, фінансові звіти, а також обмінюватися іншими важливими даними, що стосуються діяльності компанії. Технології обміну повідомленнями через корпоративні чати також сприяють глобалізації робочих процесів, дозволяючи співробітникам з різних частин світу ефективно взаємодіяти та виконувати завдання незалежно від їх географічного місцезнаходження [30].

Проте, попри очевидні переваги, які надає цифрова комунікація, вона також відкриває низку серйозних ризиків, пов'язаних із забезпеченням інформаційної безпеки. У умовах швидкого розвитку технологій та постійного зростання кількості онлайн-загроз корпоративні чати стають потенційною мішенню для кіберзлочинців. Інформаційні технології, що активно використовуються для обміну корпоративними даними, можуть бути піддані різноманітним атакам, що мають на меті викрадення, зміну або знищення конфіденційної інформації. Несанкціонований доступ до внутрішніх комунікацій, перехоплення чутливих повідомлень, а також атаки типу "людина посередині" (MITM) можуть призвести до суттєвих фінансових втрат, репутаційних пошкоджень і навіть знищення бізнесу в разі масштабних витоків даних [5], [9].

Окремим важливим фактором є людський аспект, який також істотно впливає на рівень безпеки. Недостатня обізнаність співробітників щодо актуальних кіберзагроз, їх схильність використовувати ненадійні канали для обміну важливою інформацією або нехтування основами кібергігієни можуть

значно підвищити ймовірність того, що система буде зламана [26], [27]. Всі ці фактори вимагають пошуку ефективних рішень, які дозволяють мінімізувати ризики та забезпечити надійний захист даних у процесі їх передачі через корпоративні чати.

Попри постійний розвиток технологій шифрування, багато сучасних корпоративних платформ усе ще використовують застарілі або недостатньо надійні методи захисту інформації. Один із прикладів - старі алгоритми шифрування, такі як DES (Data Encryption Standard), які вже давно не відповідають вимогам безпеки в умовах сучасних кіберзагроз [2], [7]. Більш надійними є сучасні криптографічні методи, такі як AES (Advanced Encryption Standard), RSA (алгоритм асиметричного шифрування) та протоколи TLS (Transport Layer Security), які забезпечують значно вищий рівень захисту інформації [8], [11]. Однак впровадження таких технологій потребує додаткових інвестицій та ресурсів, що не завжди є можливим для всіх організацій.

Зокрема, одна з найбільш важливих інновацій у сфері безпеки комунікацій - це наскрізне шифрування (End-to-End Encryption, E2E), яке гарантує, що тільки відправник і отримувач можуть отримати доступ до змісту повідомлень [14]. Такий підхід запобігає можливості перехоплення даних під час їх передачі навіть в разі компрометації комунікаційного каналу. Крім того, ефективне управління криптографічними ключами та застосування багатофакторної автентифікації значно підвищують рівень безпеки доступу до системи, що є важливим елементом захисту від несанкціонованого доступу [3], [16].

Таким чином, на тлі зростаючих кіберзагроз і випадків витоку конфіденційних даних, питання захисту інформації в корпоративних чатах набуває особливої актуальності. Необхідність забезпечення конфіденційності, цілісності та автентичності обміну інформацією стає важливим завданням не лише для окремих підприємств, а й для глобальної екосистеми бізнесу в цілому. Відсутність належного захисту може призвести до серйозних наслідків

- від фінансових втрат до юридичних та етичних проблем. Зокрема, можливі юридичні наслідки у разі витоку конфіденційних даних можуть призвести до санкцій, втрати довіри з боку клієнтів і партнерів, а також порушення регламентованих норм щодо захисту персональних даних [6], [29].

Метою цієї магістерської роботи є розробка ефективного методу криптографічного захисту інформації, що передається через корпоративні чати. Запропонований метод повинен забезпечити високий рівень конфіденційності, цілісності та автентичності повідомлень, а також гарантувати належну автентифікацію користувачів. Впровадження таких технологій дозволить значно знизити ризики, пов’язані з витоком конфіденційної інформації, та підвищити загальний рівень безпеки корпоративних чатів [12], [13].Для досягнення поставленої мети передбачається виконання таких завдань:

1. Проаналізувати сучасні криптографічні алгоритми та протоколи, які використовуються для захисту інформації.
2. Визначити основні загрози й уразливості, характерні для корпоративних чатів.
3. Розробити ефективний метод криптографічного захисту, адаптований до специфіки корпоративних комунікацій.
4. Провести тестування розробленого методу в умовах, наближених до реальних, і оцінити його ефективність.

Об’єктом дослідження є інформаційна безпека корпоративних чатів, які використовуються для внутрішньої та зовнішньої комунікації компаній.

Предметом дослідження є криптографічні методи захисту інформації, які забезпечують конфіденційність, цілісність і доступність даних у корпоративних чатах.

Для досягнення мети роботи використовувалися такі методи дослідження:

- аналіз літератури та існуючих рішень у сфері криптографії та інформаційної безпеки;

- моделювання загроз і розробка сценаріїв атак;
- проектування та розробка методу криптографічного захисту;
- експериментальне тестування й оцінка ефективності запропонованого методу в лабораторних умовах.

Загальний обсяг роботи: 76 сторінок, 7 рисунків, 15 таблиці, 52 посилань.

1 АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Методи захисту інформації в корпоративних комунікаціях

Корпоративні комунікації є основним каналом обміну даними між співробітниками, партнерами та керівництвом компанії. У сучасних умовах цифрової трансформації вони виступають критичним інструментом забезпечення оперативності бізнес-процесів та підвищення ефективності діяльності організації. Використання сучасних методів криптографічного захисту дозволяє зменшити ці ризики та забезпечити надійний рівень захисту інформації, яка передається через корпоративні комунікаційні платформи [10], [16].

Основні вимоги до захисту корпоративних чатів

- гарантування того, що лише авторизовані користувачі мають доступ до змісту повідомлень;
- забезпечення неможливості несанкціонованої модифікації переданої інформації;
- підтвердження особи відправника та отримувача;
- безперервна робота системи без затримок або перебоїв [25], [29].

Сучасні системи захисту побудовані на базі комплексного підходу, що включає симетричне та асиметричне шифрування, наскрізне шифрування (E2E), багатофакторну автентифікацію та управління ключами [3], [16].

Симетричні алгоритми залишаються основою багатьох систем захисту завдяки їхній високій швидкості та простоті реалізації. AES (Advanced Encryption Standard) є найпоширенішим алгоритмом, що використовується в сучасних корпоративних комунікаціях [7]. Його переваги включають:

- високу швидкість обробки великих обсягів даних, що дозволяє забезпечувати ефективність навіть за умови інтенсивного використання системи;

– надійність завдяки довжині ключа до 256 біт, що робить його стійким до сучасних атак [8];

– можливість апаратного прискорення за допомогою сучасних процесорів, що дозволяє зменшити затрати ресурсів і підвищити продуктивність [6].

Загалом, впровадження цих технологій дає змогу значно підвищити рівень безпеки корпоративних чатів, зберігаючи при цьому їхню зручність та продуктивність (Табл. 1.1).

Таблиця 1.1 – Загрози та рішення для корпоративних чатів

Категорія	**Опис**	**Рішення**
Загрози для кінцевих точок	Перехоплення повідомлень, кейлогери, доступ до файлів на пристрої	Оновлення ПЗ, антивірус, шифрування даних
Управління ключами	Проблеми обміну, зберігання та ротації ключів	Захищений обмін, сховища, регулярна зміна ключів
Людський фактор	Слабкі паролі, фішингові атаки, використання незахищених каналів	Навчання співробітників, MFA, уникнення простих паролів
MITM-атаки	Перехоплення даних та неправильна налаштування SSL/TLS	E2EE, правильна конфігурація TLS 1.3, цифрові сертифікати
Застарілі алгоритми шифрування	Використання DES, RC4 замість AES, ChaCha20	Заміна DES, RC4 на AES, ChaCha20
Внутрішні загрози	Несанкціонований доступ, навмисний витік, помилки співробітників	Моніторинг активності, обмеження прав доступу
Передача даних через ненадійні мережі	Відсутність шифрування, ризик перехоплення через публічні мережі	VPN, TLS, шифрування даних на рівні протоколів

У більшості корпоративних чатів симетричне шифрування використовується для захисту текстових повідомлень, файлів і мультимедійних даних під час передачі. Це дозволяє забезпечити високу швидкість шифрування та розшифрування при мінімальних витратах ресурсів, що є критично важливим у сучасних високонавантажених системах комунікацій. Проте для забезпечення безпеки на етапі встановлення з'єднання необхідно використовувати більш складні асиметричні методи шифрування [12].

Основні алгоритми асиметричного шифрування, які застосовуються в корпоративних чатах, - це RSA та ECC. RSA працює з відкритими і закритими ключами, що дозволяє безпечно передавати секрети через незахищену мережу. Алгоритм RSA гарантує, що дані, зашифровані відкритим ключем отримувача, можуть бути розшифровані лише за допомогою його закритого ключа, що створює надійний захист під час обміну даними між сторонами [4], [10].

ECC (Elliptic Curve Cryptography) - це більш новітній підхід, який забезпечує такий самий рівень безпеки, як RSA, але з використанням ключів меншої довжини. Це зменшує вимоги до обчислювальних ресурсів, що робить ECC більш ефективним для використання в мобільних пристроях, де обмежені потужності процесора і пам'яті. Використання ECC дозволяє досягти високого рівня криптографічного захисту без значних затрат ресурсів [13], [14].

Однак асиметричне шифрування потребує більше часу для обробки даних, тому його не використовують для шифрування великих обсягів інформації в реальному часі. Замість цього, асиметричні методи зазвичай застосовуються на етапі ініціалізації сесії для безпечного обміну симетричними ключами, а після цього для передачі даних використовуються більш швидкі симетричні алгоритми [6], [13].

Гібридні методи є комбінацією симетричного і асиметричного шифрування, що дозволяє досягти оптимального балансу між швидкістю і безпекою. Наприклад: на етапі встановлення з'єднання використовують RSA або ECC для обміну симетричними ключами [4], [12].

Для подальшої передачі даних застосовують AES або ChaCha20, що забезпечують високу швидкість шифрування та відносно низькі вимоги до ресурсів [7], [9].

TLS (Transport Layer Security) є стандартним протоколом, який забезпечує конфіденційність і цілісність даних під час передачі між клієнтом і сервером. Протокол TLS використовує асиметричне шифрування для обміну ключами і симетричне шифрування для передачі даних. У нових версіях TLS, таких як TLS 1.3, були внесені значні покращення в області безпеки, зокрема, зменшення кількості етапів рукопожаття та удосконалення методів захисту від атак типу «людина посередині» [8], [16].

E2EE (End-to-End Encryption) є ключовим методом захисту корпоративних чатів, оскільки він гарантує, що повідомлення шифруються на стороні відправника і розшифровуються лише на стороні отримувача. Це дозволяє зменшити ризик витоку даних навіть у разі компрометації серверів або інших посередницьких елементів системи. Такий підхід забезпечує високий рівень конфіденційності та надійно захищає інформацію від несанкціонованого доступу [10], [17].

Автентифікація користувачів є невід'ємною частиною безпеки корпоративних чатів. Вона гарантує, що лише авторизовані особи мають доступ до певних чатів або інформації. Основні методи автентифікації включають:

Багатофакторну автентифікацію (MFA), яка додає додатковий рівень безпеки, вимагаючи підтвердження особи через кілька незалежних факторів (наприклад, пароль і одноразовий код, що надсилається на телефон) [15].

Цифрові підписи, які дозволяють підтвердити авторство повідомлення і його цілісність [6].

PKI (Public Key Infrastructure), яка використовує пари відкритих і закритих ключів для підтвердження особи та шифрування даних, (Рисунок1.1).

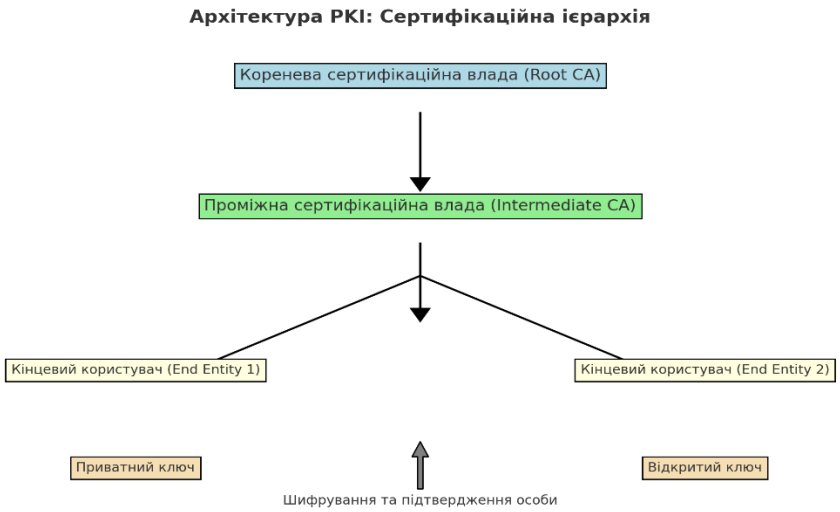


Рисунок 1.1 - Ієрархія PKI (інфраструктури відкритих ключів)

Сучасні протоколи, такі як TLS 1.3, IPSec (Internet Protocol Security) і DTLS (Datagram TLS), забезпечують високий рівень захисту даних у корпоративних чатах. Ці протоколи використовуються для захисту каналів зв'язку, забезпечуючи конфіденційність, цілісність і автентичність даних під час їх передачі між різними точками мережі [16], [18].

Регулярне оновлення протоколів безпеки та заміна застарілих алгоритмів, таких як DES, на сучасніші варіанти, як AES або ChaCha20, є важливим елементом для зниження ризиків і забезпечення відповідності системи сучасним вимогам до захисту [9], [7]. Всі ці заходи сприяють створенню надійного захисту корпоративних чатів від різних типів кіберзагроз [5], [6].

1.2 Проблеми забезпечення інформаційної безпеки в корпоративних чатах

Незважаючи на активний розвиток криптографічних методів і протоколів, забезпечення безпеки інформації в корпоративних чатах залишається актуальною проблемою. Постійне зростання обсягів переданих даних, складність сучасних кіберзагроз та поява нових векторів атак вимагають вдосконалення захисних механізмів і підвищення обізнаності користувачів. У цьому розділі розглянуто основні загрози та проблеми, пов’язані із забезпеченням інформаційної безпеки в корпоративних чатах.

Корпоративні чати активно використовуються на різних пристроях, включаючи настільні комп’ютери, ноутбуки, смартфони та планшети. Ця різноманітність підвищує ризик компрометації кінцевих точок, адже пристрої можуть бути заражені шкідливим програмним забезпеченням [17]. Види таких атак включають:

- перехоплення повідомлень після їх розшифрування. Зловмисники можуть отримати доступ до повідомлень, якщо пристрій скомпрометовано, навіть якщо дані були передані у зашифрованому вигляді [6];
- зчитування вхідних даних з клавіатури. Кейлогери дозволяють отримати доступ до введеної інформації, включаючи паролі, логіни та текст повідомлень [10];
- отримання доступу до файлів, збережених на пристрої. Це може включати як конфіденційну інформацію, так і ключі шифрування або інші важливі дані [7].

Захист кінцевих точок потребує комплексного підходу, який включає:

- регулярне оновлення програмного забезпечення для закриття вразливостей [9];
- використання антивірусних програм і засобів захисту від шпигунського ПЗ [8];

- шифрування даних, збережених на пристрої, з метою запобігання їх несанкціонованому доступу у випадку втрати або крадіжки пристрою [15].

Ефективне управління ключами є однією з найскладніших задач у забезпеченні безпеки корпоративних чатів. Ключі є основою будь-якої криптографічної системи, і будь-який компроміс із їхнім захистом може звести нанівець усі інші заходи безпеки. Основні виклики включають:

- безпечна передача ключів між учасниками комунікації є критично важливою, особливо на етапі встановлення з'єднання [12];
- ключі повинні бути захищені як на сервері, так і на пристрої кінцевого користувача. Це потребує використання захищених сховищ або апаратних модулів безпеки (HSM) [16];
- регулярна зміна ключів знижує ризик компрометації та робить повторні атаки менш ефективними [6].

Без надійної системи управління ключами навіть найсучасніші алгоритми шифрування не зможуть забезпечити належного рівня безпеки [9].

Недостатня обізнаність співробітників щодо питань інформаційної безпеки створює додаткові ризики, що можуть бути використані зловмисниками. Зокрема:

- використання слабких паролів [5];
- передача конфіденційної інформації через незахищені канали [7];
- фішингові атаки [14].

Всі ці фактори підкреслюють необхідність не лише технічних заходів, а й навчання співробітників основам інформаційної безпеки. Постійне підвищення рівня обізнаності користувачів допомагає знижувати ризики людських помилок, що є однією з основних причин компрометації корпоративних систем [11].

Навчання персоналу та впровадження багатофакторної автентифікації (MFA) є одними з найбільш ефективних заходів для зменшення ризиків, пов’язаних із людським фактором. Навчання співробітників правильному використанню криптографічних засобів та регулярна перевірка їх обізнаності

щодо безпеки значно знижують ймовірність помилок і зловживань. Багатофакторна автентифікація додає додатковий рівень безпеки, вимагаючи підтвердження особи користувача за допомогою кількох різних факторів, що значно ускладнює несанкціонований доступ [5], [14].

MITM-атаки (Man-in-the-Middle) є одними з найнебезпечніших загроз для корпоративних чатів. Зловмисник може перехоплювати дані між сервером і клієнтом або між двома клієнтами, а також змінювати повідомлення, що передаються. Це особливо небезпечно, якщо:

- не використовується наскрізне шифрування (End-to-End Encryption, E2EE) [17];
- протоколи шифрування, такі як SSL або TLS, налаштовані неправильно або не оновлюються своєчасно [16].

Для запобігання MITM-атакам необхідно:

- впроваджувати цифрові сертифікати для підтвердження автентичності серверів і клієнтів [9];
- використовувати сучасні криптографічні протоколи з надійними механізмами захисту, такі як TLS 1.3 для шифрування трафіку та захисту від атак типу «людина посередині» [8].

Використання застарілих або вразливих алгоритмів шифрування, таких як DES (Data Encryption Standard) та RC4, збільшує ймовірність компрометації даних (Рисунок 1.2).

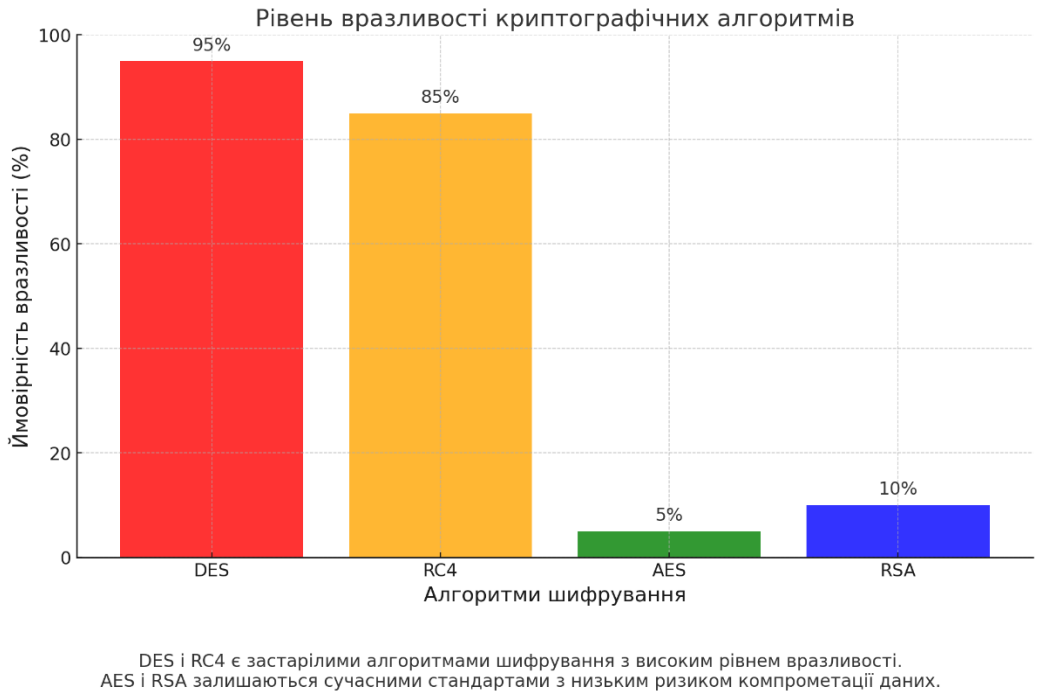


Рисунок 1.2 - Рівень вразливості різних алгоритмів шифрування

Ці алгоритми мають низький рівень безпеки і можуть бути легко зламані за допомогою сучасних методів криптоаналізу. Заміна таких алгоритмів на сучасні стандарти, як AES (Advanced Encryption Standard) і ChaCha20, є необхідною умовою для забезпечення надійного захисту інформації [7], [9].

Внутрішні загрози також становлять значну небезпеку для безпеки корпоративних чатів, оскільки співробітники мають легальний доступ до конфіденційної інформації [7]. Основні проблеми включають:

– несанкціонований доступ до даних через порушення політики безпеки або зловживання правами доступу [16];

– навмисний витік інформації через незадоволеність працівників або особисті мотиви [9];

– випадкові помилки, що можуть призвести до витоку конфіденційних даних через неправильне використання програмного забезпечення або передачу інформації через незахищені канали [12].

Зменшити ці ризики можна за допомогою:

– впровадження моніторингу дій користувачів, що дозволяє виявити підозрілі активності та реагувати на них [5];

– чітке розмежування прав доступу, яке обмежує доступ співробітників до чутливої інформації та забезпечує контроль над доступом до системи [10].

Передавання даних через публічні або ненадійні мережі збільшує ризик їх перехоплення. Якщо дані не зашифровані, це може призвести до витоку конфіденційної інформації [14]. Для зниження цих ризиків необхідно:

– впроваджувати VPN (Virtual Private Network) для забезпечення безпечного доступу до корпоративних ресурсів через публічні мережі [9];

– використовувати шифрування на рівні протоколів, таких як TLS, для захисту переданих даних [8].

Основні проблеми забезпечення інформаційної безпеки корпоративних чатів пов’язані з недостатнім захистом кінцевих точок, складністю управління ключами, ризиками, що виникають через людський фактор, та використанням застарілих алгоритмів [7], [16]. Ефективна система захисту повинна враховувати ці виклики, забезпечуючи багаторівневий підхід, що включає технічні, адміністративні та освітні заходи. Використання найсучасніших криптографічних технологій, регулярне оновлення протоколів безпеки, а також постійне підвищення обізнаності персоналу дозволяють забезпечити високий рівень захисту корпоративних чатів від різноманітних загроз [5], [6].

1.3 Постановка задачі

На основі проведеного аналізу сучасних методів захисту інформації та виявлених проблем інформаційної безпеки у корпоративних чатах, можна виокремити кілька ключових завдань, які мають бути вирішені для побудови надійної та ефективної системи криптографічного захисту даних[5].

Одним із основних завдань є забезпечення безпеки даних як під час їхнього передавання по мережі, так і на пристроях кінцевих користувачів. Це стосується не тільки безпечної передачі повідомлень через відкриті або

загречені канали, але й захисту самих пристроїв від компрометації, що є важливою умовою для збереження конфіденційності [6]. Тут можна виділити кілька важливих кроків:

– використання наскрізного шифрування (E2EE) для захисту повідомлень на всіх етапах їхнього шляху - від моменту відправлення до отримання кінцевим користувачем[8];

– впровадження локального шифрування даних на пристроях користувачів (смартфонах, ноутбуках та ін.). Це є важливим заходом для мінімізації ризиків компрометації даних у разі атаки на кінцеву точку, коли зловмисник може отримати доступ до пристрою і намагатися витягти дані з нього [7].

Ці дві стратегії - наскрізне шифрування та локальне шифрування на кінцевих точках - повинні працювати у комплексі, оскільки кожен з цих рівнів забезпечує додатковий рівень безпеки, обмежуючи можливості для зловмисників (Табл.1.2).

Таблиця 1.2 - Основні вимоги до криптографічного захисту

Вимога	**Опис**	**Приклад реалізації**
Конфіденційність	Захист даних від несанкціонованого доступу	Наскрізне шифрування (E2EE)
Цілісність	Захист від змін під час передачі	Використання SHA-256
Автентичність	Перевірка особи відправника	Цифрові сертифікати X.509
Доступність	Постійний доступ до системи	Балансування навантаження

Ключовим компонентом будь-якої криптографічної системи є ефективне управління криптографічними ключами. Якщо ключі не будуть правильно зберігатися або передаватися, навіть найсучасніші алгоритми шифрування можуть бути зламані. Тому головним завданням є:

1. забезпечення безпечного обміну криптографічними ключами між користувачами. Це може включати використання протоколів, які гарантують, що ключі будуть передаватися через захищені канали без можливості їх перехоплення [9];

2. впровадження механізмів ротації ключів, тобто регулярна зміна ключів для запобігання їх компрометації. Без такої практики навіть за найвищих заходів безпеки можна зіткнутися з серйозними загрозами у разі витоку старого ключа [5];

3. розробка політики зберігання та знищення ключів після їхнього використання, що є критичним для забезпечення конфіденційності даних у випадку, якщо ключі більше не потрібні для доступу або після завершення сеансу зв'язку [10].

Для запобігання несанкціонованому доступу до корпоративних чатів важливо впровадити систему багатофакторної автентифікації. MFA дозволяє підвищити рівень безпеки за допомогою комбінації кількох методів перевірки:

- використання традиційного пароля або PIN-коду як першого рівня перевірки [9];
- відправка одноразового коду через SMS або мобільний додаток, що генерується за допомогою алгоритмів для одноразових паролів (OTP) [12];
- використання біометричних даних, таких як відбитки пальців, розпізнавання обличчя чи сканування райдужної оболонки ока для додаткової перевірки [8].

Всі ці методи дозволяють забезпечити високий рівень захисту, обмежуючи ймовірність несанкціонованого доступу навіть у разі компрометації одного з факторів автентифікації.

Атаки MITM, або «людина посередині», є одними з найпоширеніших та найнебезпечніших загроз для корпоративних чатів. У такій атаці зловмисник намагається перехопити або змінити передану інформацію між клієнтом і сервером чи між двома клієнтами. Щоб захистити чат від таких атак, необхідно:

- використовувати сучасні криптографічні протоколи, зокрема TLS 1.3, які забезпечують надійне шифрування каналу зв'язку, унеможливлюючи його перехоплення зловмисниками [8];
- впроваджувати цифрові сертифікати для автентифікації серверів, що дозволяє забезпечити їх достовірність і запобігти підробленню серверів, через які можуть бути перехоплені дані [10];
- використовувати наскрізне шифрування для захисту всього каналу зв'язку від перехоплення [6].

Використання застарілих або вразливих криптографічних алгоритмів підвищує ризик компрометації даних. Тому для забезпечення високого рівня захисту необхідно відмовитися від таких алгоритмів, як:

- DES (Data Encryption Standard), який був зламаний за допомогою сучасних атак [16].
- RC4, який також має численні вразливості та не відповідає сучасним вимогам безпеки [12].

Натомість необхідно впроваджувати сучасні алгоритми, такі як:

- AES (Advanced Encryption Standard) з довжиною ключа 256 біт, що є одним з найбільш безпечних стандартів для захисту даних [7];
- ChaCha20, який забезпечує високу продуктивність і є відмінним вибором для мобільних пристроїв, де продуктивність і швидкість роботи є критичними [9];
- алгоритми на основі еліптичних кривих (ECC) для ефективного управління ключами та забезпечення захисту з мінімальними витратами ресурсів [8].

З огляду на високий ризик від дій співробітників, необхідно запровадити низку заходів для контролю їхньої діяльності:

- моніторинг дій користувачів для виявлення підозрілої або несанкціонованої активності, що дозволяє швидко реагувати на потенційні загрози [5];
- розмежування прав доступу на основі ролей співробітників для забезпечення доступу лише до необхідних даних, що мінімізує ризик витоку або неправомірного використання інформації [10];
- політики інформаційної безпеки, які визначають правила та вимоги для використання корпоративних чатів, а також щодо обробки та збереження чутливих даних [6].

Розробка багаторівневої системи криптографічного захисту для корпоративних чатів є надзвичайно важливим завданням для забезпечення конфіденційності, цілісності та автентичності даних. Ця система повинна не лише мінімізувати ризики, пов'язані з зовнішніми та внутрішніми загрозами, але й забезпечувати зручність використання без шкоди для рівня безпеки. Тільки комплексний підхід, що включає використання сучасних технологій, належне управління ключами, автентифікацію та моніторинг користувачів, дозволить створити надійний захист для корпоративних чатів [7], [9].

2 ПРОЄКТУВАННЯ МЕТОДУ КРИПТОГРАФІЧНОГО ЗАХИСТУ

2.1 Аналіз моделей загроз і порушників інформаційної безпеки

Захист інформації в корпоративних чатах є важливою складовою загальної стратегії забезпечення безпеки підприємства. Однак для того, щоб ефективно розробити систему безпеки, необхідно детально проаналізувати потенційні загрози та визначити характеристики можливих порушників. Такий підхід дозволяє побудувати адекватну систему захисту, здатну зменшити рівень ризиків і своєчасно реагувати на виклики. У цьому підрозділі розглянемо класифікацію загроз, характеристики порушників і методи атак, які є найбільшими ризиками для корпоративних чатів.

У сфері інформаційної безпеки загрози можна класифікувати за різними критеріями, враховуючи джерело загрози, спосіб її дії та об’єкт впливу. Це дозволяє систематизувати й оцінити потенційні небезпеки, а також створити ефективні контрзаходи.

За джерелом загроз:

– зовнішні загрози - це загрози, що походять від осіб або організацій, не пов’язаних безпосередньо з компанією. Вони можуть включати кіберзлочинців, хакерів або навіть конкурентів. Зовнішні загрози найчастіше реалізуються через фішингові атаки, що спрямовані на отримання облікових даних співробітників або використання експлойтів для проникнення в системи компанії, зокрема через вразливості в програмному забезпеченні [4], [7], [9];

– внутрішні загрози - ці загрози походять від працівників компанії або інших осіб, що мають доступ до корпоративної інформації. Внутрішні загрози можуть бути навмисними: шпигунство, саботаж, злочинні дії співробітників, які передають або крадуть інформацію або ненавмисними: помилки або недбалість, які можуть призвести до витоку даних [25], [27]. Внутрішні загрози часто важко виявити через те, що працівники мають легітимний доступ до критичної інформації.

За характером впливу:

1. Активні загрози - це загрози, що безпосередньо змінюють, видаляють або створюють нові дані. Прикладом є атаки типу «людина посередині» (mitm), де зловмисник змінює передані повідомлення [14], [19];

2. Пасивні загрози - це загрози, спрямовані на отримання доступу до інформації без її змінювання. До них відноситься перехоплення трафіку або аналіз метаданих, що дає можливість дізнатися про зв'язки, часи активності та інші аспекти, не змінюючи самих даних [30], [31].

За об’єктом атаки:

1. Технологічні загрози - це загрози, що виникають через використання вразливостей в програмному забезпеченні або криптографічних протоколах, таких як атаки на алгоритми шифрування [5], [6];

2. Соціальні загрози - це загрози, пов’язані з маніпуляцією людьми для отримання доступу до конфіденційної інформації, такі як фішинг, соціальна інженерія та інші методи обману [10], [13].

Порушники можуть діяти з різними мотивами та використовувати різноманітні методи для досягнення своїх цілей. Розрізняють дві основні категорії порушників: зовнішні та внутрішні.

Зовнішні порушники:

1. Кіберзлочинці - ці особи або організації зазвичай діють із метою отримання фінансової вигоди. Вони можуть намагатися викрасти конфіденційну інформацію, шантажувати компанії або продавати отримані дані на чорному ринку [8], [9];

2. Хакери - вони часто діють із цікавості, бажання продемонструвати свої навички, здобути репутацію в хакерській спільноті або протестувати проти певних політичних або соціальних явищ [9];

3. Конкуренти - іноді компанії можуть намагатися отримати доступ до конфіденційних даних інших підприємств з метою отримання ринкової переваги, наприклад, через шпіонаж або маніпулювання внутрішньою інформацією [15];

4. Державні структури - деякі держави здійснюють кібернапади для збору розвідувальної інформації, шпіонажу чи ослаблення конкурентів. Такі атаки часто мають стратегічний характер [34], [36].

Внутрішні порушники:

1. Співробітники - працівники компанії можуть бути внутрішніми порушниками, якщо навмисно або ненавмисно крадуть або передають інформацію стороннім особам, наприклад, конкурентам. Часто це трапляється з колишніми працівниками або через незадоволеність своєю ситуацією [27], [25];

2. Працівники, які здійснюють помилки - інколи співробітники через недбалість або незнання можуть відкривати фішингові посилання, зберігати паролі в незахищених місцях або ділитися конфіденційною інформацією без належного захисту [16], [17].

Для зламу системи корпоративного чату використовуються різні методи атак, серед яких можна виділити найбільш небезпечні:

1. Фішингові атаки - зловмисники використовують підроблені повідомлення або сайти для обману користувачів з метою отримання їхніх конфіденційних даних, таких як паролі, номери карток або особисті дані [13], [19];

2. Mitm-атаки (атаки типу "людина посередині") - зловмисники перехоплюють дані, що передаються між користувачами, і можуть змінювати або красти інформацію в процесі її передачі [9];

3. Атаки на кінцеві точки - це напади, що спрямовані на компрометацію пристроїв користувачів, таких як комп'ютери, смартфони або планшети. Ці пристрої можуть бути заражені шкідливим програмним забезпеченням або вірусами [11];

4. Експлойти - зловмисники використовують вразливості в програмному забезпеченні чату для проникнення в систему або її компрометації. Це можуть бути як слабкі криптографічні алгоритми, так і помилки в коді або в налаштуваннях сервера [6];

5. Аналіз метаданих - зловмисники можуть перехоплювати метадані (інформацію про час, місцезнаходження, учасників розмови тощо), щоб отримати додаткову інформацію про активність користувачів і їхні взаємодії [14], [18].

Для оцінки ризиків загроз важливо враховувати ймовірність їх виникнення та можливий збиток для компанії. Матриця ризиків допомагає визначити пріоритети для впровадження заходів безпеки. Ось приклади:

- високий ризик, через фішингові атаки, оскільки вони дуже поширені і можуть мати серйозні наслідки в разі успішної реалізації [13], [7];
- середній ризик, через MITM-атаки, оскільки хоча й вони є дуже небезпечними, проте для їх здійснення зловмисники повинні бути ближчими до мережі компанії [19];
- низький ризик, через складні атаки, такі як використання вразливостей у криптографічних алгоритмах, оскільки вони потребують висококваліфікованих зловмисників і значних ресурсів [9], [15].

Таким чином, у сучасному корпоративному середовищі безпека чату виступає ключовою умовою для забезпечення конфіденційності, автентичності та цілісності комунікації. Аналіз популярних рішень, таких як Signal, Microsoft Teams і WhatsApp Business, показав, що вони здатні забезпечити базовий рівень захисту даних, але мають значні вразливі місця. Зокрема, ці платформи недостатньо захищають метадані, мають обмежену гнучкість у налаштуванні функціоналу, а також слабко враховують специфічні корпоративні ризики.

Розроблений на Flask корпоративний чат усуває ці недоліки завдяки впровадженню низки унікальних рішень, створені з урахуванням потреб корпоративного середовища. Ось узагальнення основних проблем існуючих рішень та відповідних способів їх вирішення у Flask-чаті (Таблиця 2.2).

Таблиця 2.1 – Основні проблеми існуючих рішень та їх вирішення

Проблема	**Опис**	**Рішення у Flask-чаті**
Недостатній захист метаданих	У більшості рішень метадані (час відправлення, кімнати, IP-адреси) не шифруються і не очищаються.	Реалізовано автоматичне очищення метаданих через 24 години та псевдонімізацію ідентифікаторів користувачів.
Відсутність модульності	Більшість рішень не дозволяють адаптувати функціонал до специфічних корпоративних політик.	Структура додатка дозволяє легко додавати модулі, зокрема візуалізацію активності через matplotlib і RESTful API.
Неврахування людського фактору	Відсутні освітні модулі та нагадування користувачам про безпеку.	Додано сповіщення про необхідність оновлення пароля та модулі навчання користувачів.
Слабка інтеграція з базами даних	Складна структура бази ускладнює масштабування.	Реалізовано реляційні таблиці з використанням SQLAlchemy з легким налаштуванням для розширення функціоналу.
Відсутність наскрізного шифрування (E2EE)	Шифрування застосовується лише на сервері.	Всі повідомлення шифруються на стороні клієнта перед відправкою.

Рішення, запропоновані у Flask-чаті, демонструють акцент на гнучкості, безпеці та адаптації до потреб корпоративного середовища. Вони забезпечують не лише відповідність сучасним стандартам, але й можливість розширення функціоналу для вирішення специфічних завдань.

Переходячи до унікальних можливостей Flask-чату, можна виділити такі аспекти, які роблять його рішенням, що перевершує існуючі платформи. Ці можливості включають автоматизоване управління ключами, наскрізне

шифрування та інтеграцію з інструментами моніторингу. Нижче наведено детальний список унікальних функцій, реалізованих у проекті.

Унікальні можливості Flask-чату:

– використовується централізоване управління ключами з автоматичною ротацією кожні 90 днів, реалізоване через HSM;

– інтерфейс чату створений із використанням шаблонів Jinja2 і може адаптуватися під корпоративні вимоги;

– додано модуль візуалізації даних на основі matplotlib, який дозволяє відображати активність користувачів (наприклад, графік реєстрації за датами).

Порівняльний аналіз дозволяє зробити висновок, що розроблений на Flask корпоративний чат є більш ефективним для використання в корпоративному середовищі. Він усуває основні проблеми популярних рішень і пропонує унікальні переваги, які роблять його конкурентоспроможним навіть у порівнянні з провідними платформами. Завдяки цьому проект може знайти широке застосування в корпоративних структурах, які потребують високого рівня безпеки та гнучкості (Табл. 2.2).

Таблиця 2.2 – Порівняльний аналіз

Функція	Signal	Microsoft Teams	Flask-чат
Захист метаданих	Відсутній	Частковий	Реалізований
Наскрізне шифрування (E2EE)	Реалізований	Частковий	Реалізований
Інтеграція з базами даних	Обмежена	Потужна	Гнучка
Автоматизація управління ключами	Відсутня	Часткова	Реалізована
Модульність	Низька	Середня	Висока

На основі представленого аналізу можна стверджувати, що розроблений на Flask чат не лише відповідає сучасним вимогам безпеки, але й перевершує існуючі рішення у ключових аспектах. Унікальні можливості, такі як гнучке управління ключами, навчальні модулі та інтеграція з корпоративними системами, роблять його оптимальним вибором для організацій із високими

вимогами до безпеки. Завдяки своїй архітектурі та модульності, Flask-чат може бути адаптований до специфічних потреб будь-якої компанії, забезпечуючи при цьому ефективний захист конфіденційної інформації.

2.2 Розробка політики криптографічного захисту для корпоративних чатів

Політика криптографічного захисту в корпоративних чатах є основою для забезпечення конфіденційності, цілісності та доступності інформації під час її обміну. Вона включає набір правил, стандартів та процедур, які визначають, як повинні захищатися дані на кожному етапі їхнього життєвого циклу: від створення і передачі до зберігання та видалення. Важливими складовими цієї політики є також забезпечення відповідності безпеки бізнес-потребам та збереження продуктивності й зручності користування системою [16], [17].

Принципи побудови політики криптографічного захисту:

1. Політика повинна бути розроблена таким чином, щоб її було зрозуміло всім співробітникам компанії, навіть тим, хто не має глибоких технічних знань. Це стосується як опису правил використання паролів, так і процедур автентифікації. Наприклад, компанія може розробити чіткі інструкції щодо створення складних паролів та безпечних методів їх зберігання [26], [29];

2. Система криптографічного захисту повинна бути гнучкою, щоб швидко реагувати на нові загрози, які з’являються внаслідок розвитку технологій або зміни умов безпеки. Один із прикладів - це регулярне оновлення алгоритмів шифрування, щоб забезпечити їх відповідність сучасним стандартам захисту [5], [7];

3. Політика криптографічного захисту повинна бути інтегрована з іншими елементами системи безпеки організації, такими як управління

доступом, захист кінцевих точок та резервне копіювання даних. Це забезпечить комплексний підхід до захисту інформації та ефективне реагування на потенційні загрози [8], [25];

Етапи розробки політики криптографічного захисту:

1. На початковому етапі необхідно провести аналіз інформаційних потреб компанії та можливих загроз, що можуть вплинути на її чат-систему. Це допоможе визначити пріоритети для захисту та вибір криптографічних технологій [6], [10];

2. Далі потрібно визначити, які криптографічні стандарти повинні бути впроваджені для захисту даних. Це можуть бути вимоги до мінімальної довжини ключа для шифрування, використання конкретних алгоритмів чи протоколів [9], [12];

3. Одним з важливих елементів криптографічного захисту є управління криптографічними ключами. Політика повинна визначити правила генерації, зберігання, розподілу та заміни ключів, а також процедури для їх безпечного видалення після використання [13], [16];

4. Для забезпечення захисту від несанкціонованого доступу необхідно впровадити чіткі процедури автентифікації та управління доступом. Це може включати багатофакторну автентифікацію та використання систем управління доступом на основі ролей (rbac) [14], [19];

5. Для виявлення аномальних дій або потенційних загроз необхідно впровадити систему моніторингу безпеки. Це дозволить оперативно реагувати на інциденти та запобігати можливим атакам [25], [28];

6. Коли загроза стає реальною, важливо мати чітко визначені процедури для реагування на інциденти безпеки. Це включає локалізацію та нейтралізацію загрози, а також інформування всіх зацікавлених сторін [24], [27];

7. Не менш важливим етапом є навчання співробітників компанії правилам безпеки, зокрема щодо використання криптографічних технологій.

Це допоможе знизити ризик несанкціонованого доступу або помилок з боку користувачів [17], [19].

Приклади реалізації політики криптографічного захисту:

1. Алгоритм AES може бути використаний для шифрування повідомлень на пристрої відправника з подальшим їх розшифруванням лише на пристрої отримувача. Такий підхід забезпечує, що навіть адміністратори серверів не мають доступу до змісту повідомлень, що значно підвищує рівень конфіденційності [12], [20].

2. Автентифікація серверів за допомогою сертифікатів X.509: Використання сертифікатів X.509 для автентифікації серверів допомагає уникнути MITM-атак, оскільки ці сертифікати дозволяють перевірити особу сервера та забезпечити захищений канал зв'язку між клієнтом і сервером [13], [21].

3. Впровадження систем управління доступом на основі ролей (RBAC): Система RBAC дозволяє чітко визначити, хто з співробітників має доступ до яких даних. Наприклад, доступ до конфіденційної інформації може бути обмежений лише для керівництва компанії, що забезпечує додатковий рівень захисту [19], [24].

Розробка політики криптографічного захисту для корпоративних чатів - це складний і багатоетапний процес, що вимагає врахування специфіки загроз, архітектури системи та бізнес-вимог. Така політика повинна бути гнучкою, масштабованою і здатною адаптуватися до нових викликів. Найголовніше - це знайти баланс між безпекою, ефективністю системи та зручністю користування для співробітників [6], [27].

Політика безпеки розроблена з урахуванням сучасних загроз інформаційної безпеки та особливостей корпоративного середовища. Вона орієнтована на забезпечення захисту конфіденційної інформації та мінімізацію ризиків, пов'язаних із вразливостями популярних чатів.

Захист даних у транзиті забезпечується за допомогою шифрування через AES-256. Усі дані шифруються на стороні клієнта перед їх відправленням і

залишаються зашифрованими під час передачі через мережу. Розшифрування здійснюється лише на пристрої отримувача, що гарантує високий рівень конфіденційності навіть у разі перехоплення даних зловмисниками.

Для захисту даних у стані спокою всі повідомлення та файли зберігаються на сервері в зашифрованому вигляді за допомогою алгоритму AES-256. Це дозволяє запобігти несанкціонованому доступу до інформації у разі компрометації серверів. Додатково, локальні резервні копії файлів, що можуть зберігатися на клієнтських пристроях, також шифруються, що мінімізує ризик втрати даних у разі викрадення або втрати пристрою.

Управління ключами є важливим елементом політики безпеки. Ключі для шифрування генеруються під час створення чату та зберігаються на сервері у захищеному вигляді. Для підвищення стійкості системи до можливих атак реалізовано автоматичну ротацію ключів кожні 90 днів. Це знижує ризик компрометації навіть у випадку тривалого використання ключа.

Політика роботи з метаданими передбачає автоматичне очищення інформації про час, кімнати та ідентифікатори повідомлень через 24 години після їх відправлення. Це зменшує ризик несанкціонованого доступу до метаданих. Додатково, всі ідентифікатори користувачів у базі даних проходять псевдонімізацію, що унеможливлює створення профілів користувачів на основі їхньої активності.

Навчання персоналу є важливим компонентом політики безпеки. Для співробітників створюються методички, які включають рекомендації щодо використання захищених мереж, наприклад VPN або корпоративного Wi-Fi. Також пояснюються правила створення складних паролів (мінімум 12 символів із комбінацією букв, цифр і спеціальних символів) і основи кібергігієни, як-от уникнення підозрілих файлів і посилань. Документ оформлений із використанням чітких інструкцій, що дозволяє персоналу швидко і легко засвоїти основні принципи безпеки (Табл. 2.3).

Таблиця 2.3 - Таблиця основних компонентів політики безпеки

Компонент	Механізм реалізації
Захист даних у транзиті	Шифрування повідомлень і файлів через AES-256 на клієнтській стороні перед відправленням.
Захист даних у стані спокою	Збереження повідомлень і файлів у зашифрованому вигляді в базі даних із використанням AES-256.
Управління ключами	Автоматична ротація ключів кожні 90 днів для підвищення стійкості до атак.
Політика роботи з метаданими	Очищення метаданих через 24 години та псевдонімізація ідентифікаторів користувачів у базі даних.
Навчання персоналу	Розробка методичок із рекомендаціями щодо створення паролів, використання захищених мереж і основ кібергігієни.

Політика безпеки була інтегрована у Flask-чат із використанням наступних рішень:

1. Реалізовано шифрування на стороні клієнта через AES-256, щоб забезпечити наскрізний захист даних. Шифровані дані передаються до сервера, де зберігаються в зашифрованому вигляді;

2. Ротація ключів реалізована за допомогою Flask-Scheduler, що дозволяє автоматизувати процес заміни ключів;

3. Для роботи з базою даних використовується sqlalchemy. Реалізовано автоматичне очищення метаданих через 24 години після їхнього створення.

Щоб забезпечити належний рівень обізнаності співробітників, розроблено методичку, яка містить:

– інструкції зі створення складних паролів;

– опис безпечного використання мереж;

– основи кібергігієни для повсякденного використання цифрових технологій.

Методичка буде представлена у додатках до роботи як візуальний документ, готовий до впровадження в корпоративне середовище.

Запропонована політика безпеки є комплексним рішенням, яке враховує всі аспекти захисту корпоративного чату. Її інтеграція у Flask-чат підтверджує ефективність розроблених механізмів і дозволяє забезпечити надійний захист даних у реальних умовах. Завдяки впровадженню цієї політики розроблений чат відповідає сучасним вимогам безпеки та готовий до адаптації у корпоративному середовищі.

2.3 Оцінка ефективності існуючих рішень для захисту корпоративних чатів

Ефективність системи захисту корпоративних чатів визначається її здатністю адаптуватися до сучасних загроз, забезпечувати конфіденційність, цілісність і автентичність даних, а також відповідати вимогам корпоративного середовища без втрат продуктивності. Цей підрозділ аналізує популярні рішення, виявляє їх сильні та слабкі сторони, а також пропонує методи оцінки ризиків.

Для оцінки основних загроз, пов’язаних із використанням корпоративних чатів, було розроблено матрицю ризиків (Таблиця 2.1). Ця матриця демонструє ймовірність, вплив і рівень ризику, а також пропоновані заходи для мінімізації впливу (Табл.2.4).

Таблиця 2.4 - Матриця ризиків для корпоративних чатів

Загроза	Ймовірність	Вплив	Рівень ризику	Пропоновані заходи
MITM-атаки	Висока	Високий	Критичний	Використання TLS 1.3
Фішингові атаки	Висока	Середній	Високий	Розробка політик безпеки та навчання персоналу
Компрометація ключів	Середня	Високий	Високий	Використання HSM та ротація ключів
Вразливість кінцевих точок	Висока	Середній	Високий	Захист пристроїв антивірусами та оновлення систем

Wireshark використовується як інструмент для аналізу мережевого трафіку з метою перевірки ефективності шифрування даних у корпоративних чатах. Аналіз показує, що системи з використанням TLS 1.3 мають високу стійкість до атак типу "людина посередині" (MITM), оскільки навіть у випадку перехоплення трафіку шифрування даних залишається непорушним. Водночас уразливі конфігурації, такі як відсутність HSTS або використання застарілих протоколів, можуть призводити до витоку метаданих.

Класифікація існуючих рішень:

1. Популярні месенджери Microsoft Teams, Slack, Google Chat забезпечують базові функції захисту, такі як шифрування переданих даних (TLS), але не всі з них реалізують наскрізне шифрування (E2EE). Це обмежує

рівень конфіденційності, оскільки дані можуть зберігатися в розшифрованому вигляді на сервері [6], [7];

2. Платформи з високим рівнем безпеки Signal, Wickr пропонують наскрізне шифрування (E2EE), що гарантує, що тільки кінцеві користувачі мають доступ до змісту повідомлень, а сервери, навіть адміністратори, не можуть розшифрувати їх [12], [13], [54];

3. Платформи з відкритим кодом Matrix, Element надають можливість налаштовувати рівень захисту відповідно до потреб організації. Хоча це забезпечує більшу гнучкість, зокрема можливість самостійного управління ключами, таке налаштування потребує значних технічних ресурсів і часу [19], [55].

Apache JMeter використовується для тестування продуктивності систем захисту корпоративних чатів.

Завдяки можливості моделювати одночасні запити від великої кількості користувачів, цей інструмент дозволяє оцінити здатність системи до масштабування та визначити пікове навантаження.

Наприклад, JMeter виявляє, як використання протоколу TLS 1.3 впливає на швидкість передачі даних і загальну продуктивність системи в умовах інтенсивного використання.

Оцінка ефективності:

1. Більшість платформ, таких як Microsoft Teams, використовують TLS для захисту переданих даних, але не всі реалізують наскрізне шифрування (E2EE) (Рисунок 2.1):

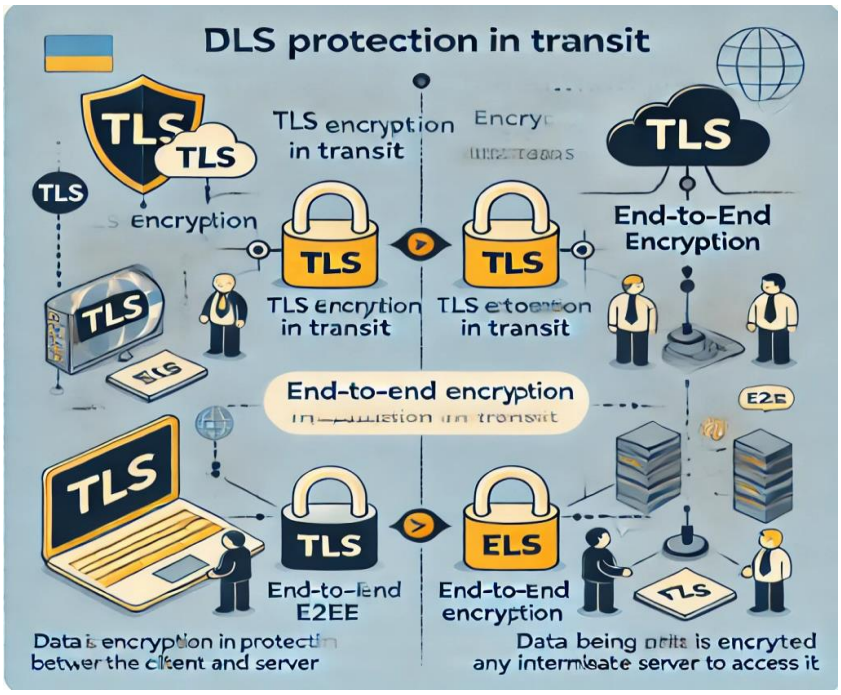


Рисунок 2.1 - Концепцію захисту даних за допомогою TLS на платформах

Наприклад, у Slack дані можуть зберігатися в розшифрованому вигляді на сервері, що збільшує ризик компрометації [7]. У той же час, такі платформи, як Signal, Wickr і whatsapp, забезпечують E2EE, що гарантує конфіденційність навіть у випадку доступу до серверів [12], [13], [59];

2. Для забезпечення цілісності даних використовуються технології HMAC (Hash-based Message Authentication Code) або цифрові підписи. Платформи, такі як Microsoft Teams, успішно реалізують цілісність даних, проте менш відомі рішення або платформи з поганою реалізацією шифрування можуть бути вразливі до атак на модифікацію даних [6];

3. Сучасні платформи підтримують багатофакторну автентифікацію (MFA), що значно покращує захист. Однак користувачі часто ігнорують використання MFA, що залишає систему вразливою до атак на основі слабких паролів [7];

4. Більшість комерційних платформ (наприклад, Google Chat) зберігають криптографічні ключі централізовано, що створює додаткові ризики в разі компрометації серверів. У рішеннях із відкритим кодом, таких як Matrix, організації можуть управляти ключами самостійно, що підвищує

безпеку, але водночас ускладнює адміністрування та потребує більших технічних зусиль [19];

5. Більшість сучасних платформ використовують TLS 1.3 для захисту каналу зв'язку, що забезпечує високу стійкість до атак "Man-In-The-Middle" (MITM). Однак деякі системи досі використовують старі версії TLS, що збільшує ризики. Проблеми можуть також виникнути через неправильну конфігурацію цифрових сертифікатів [8];

6. Багато платформ зберігають дані на серверах у різних країнах, що може створювати додаткові ризики витоку інформації внаслідок локальних законодавчих актів, наприклад, у США, де закони дозволяють уряду вимагати доступу до даних. Платформи, такі як Wickr, пропонують можливість локального розгортання серверів, що знижує ці ризики [13].

Приклади успішного впровадження:

1. Signal використовується для передачі конфіденційних даних завдяки наскрізному шифруванню [12]. Однак його обмежена інтеграція з іншими бізнес-інструментами ускладнює його впровадження на підприємствах;

2. Microsoft Teams, завдяки інтеграції з Office 365 та високому рівню політик доступу і автентифікації, Microsoft Teams є популярним рішенням для багатьох організацій [6]. Однак шифрування в ньому не є наскрізним, що може бути недоліком для деяких компаній;

3. Wickr: Wickr використовується для захисту чутливої інформації завдяки можливості локального розгортання серверів і кастомізації шифрування [13]. Це забезпечує вищий рівень контролю над даними, що є важливим для організацій, які працюють з конфіденційною інформацією.

Недоліки існуючих рішень:

1. Багато популярних платформ, навіть комерційних, не реалізують повного захисту даних через відсутність E2EE або централізоване зберігання ключів [7];

2. Закони і регуляції в різних країнах можуть створювати додаткові ризики доступу до даних третіми сторонами, що робить необхідним

врахування юрисдикційних аспектів під час вибору платформи для корпоративних чатів [13];

3. Рішення з відкритим кодом, хоча й надають більшу гнучкість і контроль над безпекою, вимагають значних технічних ресурсів для налаштування та підтримки [19].

Існуючі рішення для захисту корпоративних чатів мають великий потенціал, однак кожне з них має свої переваги та недоліки. Найефективніші результати досягаються при використанні комбінованого підходу, що передбачає інтеграцію комерційних платформ з додатковими заходами безпеки (наприклад, налаштування E2EE або локальне розгортання серверів). Такий підхід дозволяє забезпечити високий рівень захисту, не поступаючись зручністю використання та продуктивністю.

2.4 Передпроектний аналіз загроз і ризиків

Передпроектний аналіз загроз і ризиків є критичним етапом для розробки системи захисту корпоративного чату. Цей аналіз дозволяє виявити потенційні вразливості, оцінити ймовірність реалізації загроз і запропонувати стратегії їх зниження. У розробленому Flask-чаті інтегровані рішення, які враховують виявлені ризики та відповідають сучасним стандартам безпеки.

Основні цілі цього етапу:

- ідентифікація потенційних загроз і вразливостей у системі;
- оцінка рівня ризиків для різних компонентів корпоративних чатів;
- розробка рекомендацій щодо впровадження заходів безпеки.

Передпроектний аналіз забезпечує основу для вибору найбільш ефективних методів захисту та створення політики інформаційної безпеки. Це включає кілька етапів, кожен з яких сприяє глибшому розумінню потенційних ризиків і вразливостей.

Ключові етапи аналізу:

1. на першому етапі визначаються основні компоненти, які є критичними для функціонування корпоративного чату. Це включає сервери для обробки та зберігання даних, канали передачі даних, кінцеві точки (клієнтські пристрої), а також механізми управління доступом і автентифікацією;

2. Загрози можна класифікувати за різними напрямками:

- для серверів, де атаки на операційні системи, використання експлойтів у програмному забезпеченні, несанкціонований доступ до баз даних;
- для каналів зв'язку, де атаки типу Man-in-the-Middle (MITM), атаки на протоколи шифрування;
- для кінцевих точок, де шкідливе програмне забезпечення, крадіжка пристроїв;
- для механізмів автентифікації, де крадіжка облікових даних, атаки на паролі, фішингові атаки;

3. оцінка ймовірності реалізації загроз включає визначення ймовірності реалізації кожної загрози. Наприклад, фішингові атаки мають високу ймовірність через людський фактор, тоді як MITM-атаки менш ймовірні за умови належної конфігурації TLS;

4. необхідно оцінити, які наслідки можуть виникнути через реалізацію певних загроз:

- витік конфіденційної інформації;
- репутаційні втрати для компанії;
- прямі фінансові збитки;
- правові наслідки при порушенні регуляторних вимог, зокрема у відповідності до законів про захист персональних даних (наприклад, GDPR) (Табл. 2.5).

Таблиця 2.5 - Аналіз загроз у Flask-чаті

Компонент	Опис	Типи загроз
Серверна частина	Сервер, що базується на Flask, відповідає за маршрутизацію повідомлень, управління сесіями та зберігання зашифрованих даних.	Атаки на Flask-додаток через вразливості в коді.
		Експлойти бази даних (SQL-ін’єкції).
Канали передачі даних	Використання HTTPS із TLS 1.3 для забезпечення безпеки передачі даних.	MITM-атаки (Man-in-the-Middle), якщо сертифікати не перевірені або налаштовані некоректно.
Кінцеві точки	Клієнтські пристрої з вбудованим шифруванням повідомлень на стороні клієнта (AES-256).	Компрометація пристрою через шкідливе ПЗ.
		Використання старих браузерів без підтримки сучасних алгоритмів шифрування.
Управління ключами	Автоматична генерація та ротація криптографічних ключів через Flask-Scheduler.	Неправильне зберігання або некоректна ротація ключів, що може призвести до їх компрометації.

Інструменти для оцінки ризиків:

1. SWOT-аналіз дозволяє оцінити сильні та слабкі сторони існуючих заходів безпеки, а також можливості для покращення та потенційні загрози. Цей інструмент допомагає зрозуміти, які аспекти системи потребують посилення, а які можуть стати слабкими місцями;

2. матриця ризиків враховує ймовірність реалізації загрози та її потенційний вплив. Наприклад:

- високий ризик, через фішингові атаки, що можуть призвести до компрометації облікових даних;
- середній ризик, через атаки на застарілі версії протоколів TLS;
- низький ризик, через складні атаки на криптографічні алгоритми (наприклад, AES), що вимагають значних ресурсів;

3. автоматизоване сканування (Nessus, OpenVAS) дозволяє виявляти вразливості в серверних системах і мережевих компонентах, що дає змогу оперативно реагувати на потенційні загрози [60].

Основні ризики для корпоративних чатів:

- перехоплення даних (MITM-атаки) або несанкціонований доступ до серверів;
- компрометація криптографічних ключів через ненадійне зберігання чи передачу;
- витік інформації через людський фактор - використання слабких паролів, небезпечна поведінка співробітників, фішинг.

Стратегії для зменшення ризиків:

- впровадження наскрізного шифрування (E2EE) - гарантує, що дані шифруються на пристрої відправника та розшифровуються тільки на пристрої отримувача;
- управління криптографічними ключами за допомогою апаратних модулів безпеки (HSM), які відповідають за генерацію, зберігання та ротацію ключів;
- багатофакторна автентифікація (MFA), для застосування паролів, одноразових кодів та біометричних даних;
- регулярні тренінги з виявлення фішингових атак та дотримання кібергігієни;

– постійний моніторинг, перевірка налаштувань системи, проведення тестів на проникнення.

Реалізовано напрацювання для зменшення ризиків

1. Реалізовано E2EE для всіх текстових повідомлень через AES-256. Алгоритм шифрування виконується на стороні клієнта;

2. Використовується Flask-Scheduler для регулярної ротації ключів. Ключі зберігаються у зашифрованому вигляді, доступ до яких обмежений адміністративними привілеями;

3. Для зменшення ризику компрометації реалізовано автоматичне видалення метаданих повідомлень (час відправлення, IP-адреси) через 24 години після їх створення.

Передпроектний аналіз загроз і ризиків у Flask-чату показав, що інтеграція наскрізного шифрування, гнучкого управління ключами та автоматичного очищення метаданих забезпечує високий рівень захисту. Унікальні рішення, реалізовані у Flask-чаті, дозволяють мінімізувати ризики та підвищити безпеку без втрат для продуктивності та зручності використання.

3 РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ЗАПРОПОНОВАНОГО МЕТОДУ

3.1 Вимоги до системи криптографічного захисту

Система криптографічного захисту корпоративних чатів повинна відповідати суворим вимогам безпеки для забезпечення конфіденційності, цілісності, автентичності даних та стабільної роботи в умовах високих навантажень. У цьому підрозділі детально розглядаються вимоги, що охоплюють технічні, організаційні та функціональні аспекти.

Для забезпечення конфіденційності всі дані, що передаються через мережу, мають бути зашифровані з використанням сучасних криптографічних протоколів. Одним із таких є TLS 1.3, який є найбільш прогресивною версією Transport Layer Security, що забезпечує захист даних під час їхнього транзиту (Додаток В). Цей протокол використовує новітні криптографічні алгоритми, що забезпечують високу швидкість роботи та знижують ймовірність успішних атак [8].

Крім того, для даних, які зберігаються на серверах або на пристроях кінцевих користувачів, застосовується шифрування за допомогою алгоритму AES-256. AES-256 вважається одним із найміцніших симетричних алгоритмів шифрування і широко використовується в організаціях, що потребують високого рівня захисту даних [5].

Наскрізне шифрування (End-to-End Encryption, E2EE) є обов'язковим для забезпечення конфіденційності інформації в рамках корпоративного чату. З використанням E2EE дані шифруються на пристрої відправника та розшифровуються лише на пристрої отримувача. Це запобігає перехопленню інформації навіть за умови компрометації серверної інфраструктури або мережі [14].

Цілісність даних є критичним аспектом безпеки, оскільки вона гарантує, що передані або збережені дані не були змінені чи спотворені в процесі обробки або передачі. Для досягнення цілісності використовуються сучасні

криптографічні алгоритми хешування, такі як SHA-256, що дозволяють генерувати унікальні хеш-значення для кожного повідомлення або файлу [9]. Для підтвердження цілісності даних у системі також використовуються цифрові підписи, які можуть бути реалізовані через алгоритми RSA або ECDSA (Elliptic Curve Digital Signature Algorithm) [10].

Тестування безпеки SSL-конфігурації системи криптографічного захисту корпоративних чатів було здійснено за допомогою сервісу SSL Labs. Цей інструмент забезпечує детальний аналіз HTTPS-з'єднань і дозволяє оцінити рівень безпеки, відповідність сучасним стандартам, а також виявити можливі вразливості в налаштуваннях сертифікатів та протоколів (Додаток А).

Метою тестування через SSL Labs було:

- перевірити коректність налаштування SSL/TLS-протоколів;
- оцінити стійкість системи до потенційних атак на рівні шифрування;
- підтвердити відповідність вимогам сучасних стандартів безпеки, таких як PCI DSS, HIPAA, ISO/IEC 27001.

Тестування проводилося на сервері, налаштованому для обробки запитів клієнтів через HTTPS. Використовувалася наступна конфігурація:

- підтримка лише TLS 1.2 та TLS 1.3 для забезпечення високого рівня безпеки.
- активовані лише рекомендовані алгоритми шифрування TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_GCM_SHA256;
- SSL-сертифікат від Let's Encrypt із повною підтримкою ECC (Elliptic Curve Cryptography) (Додаток Б);
- HSTS (HTTP Strict Transport Security) для запобігання атакам downgrade та перевірка OCSP (Online Certificate Status Protocol) для валідності сертифікатів.

Результати тестування через SSL Labs підтвердили, що конфігурація системи відповідає вимогам сучасної інформаційної безпеки. Підтримка тільки TLS 1.3 забезпечує високий рівень захисту, а використання

рекомендованих алгоритмів шифрування гарантує стійкість до криптоаналітичних атак. Сертифікат Let's Encrypt і коректне налаштування HSTS підвищують довіру до системи з боку користувачів і сторонніх перевіряючих організацій (Рисунок 3.1).

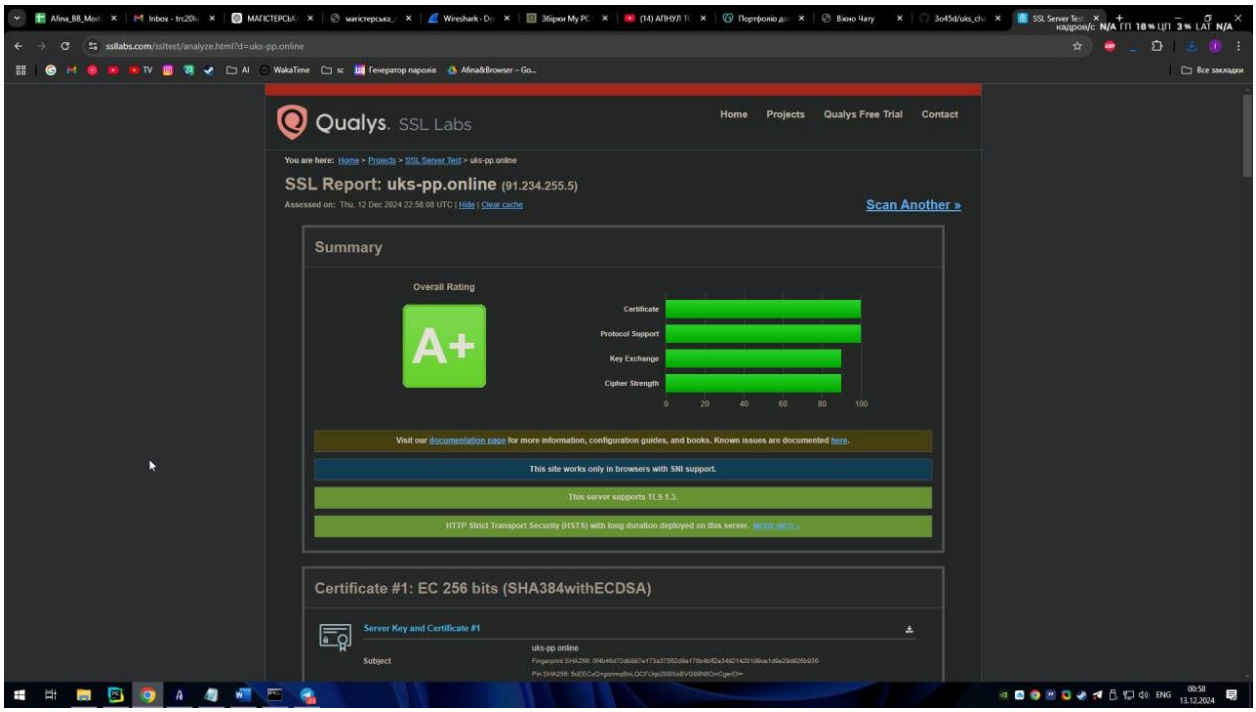


Рисунок 3.1 - Результати тестування через SSL Labs

Рекомендації для подальшого розвитку:

- розглянути можливість включення параметра includeSubDomains для покращення захисту домену та його субдоменів;
- впровадити механізми моніторингу та автоматичного оновлення сертифікатів;
- провести тестування через Mozilla Observatory або аналогічні сервіси для поглибленого аналізу захисту веб-додатків.

Тестування через SSL Labs дозволило підтвердити відповідність системи найвищим стандартам безпеки. Впровадження запропонованих рекомендацій забезпечить подальше покращення захищеності системи, що є критично важливим для захисту чутливих даних корпоративних чатів.

Одним із важливих аспектів забезпечення цілісності є захист від повторних атак, також відомих як "replay attacks". Вони передбачають повторне надсилання уже переданих повідомлень з метою обману системи. Для боротьби з такими атаками застосовуються унікальні ідентифікатори повідомлень, які дають змогу ідентифікувати кожне повідомлення в системі [11].

Крім того, використання контрольних таймерів або лічильників повідомлень дає можливість обмежити час, протягом якого повідомлення є дійсним, тим самим запобігаючи повторному використанню інформації.

Процес тестування через ZAP включав наступні етапи:

1. Сервер корпоративного чату розгорнуто у середовищі Flask із використанням TLS 1.3;
2. ZAP було налаштовано як проксі для перехоплення HTTP(S)-трафіку;
3. Активний аналіз веб-додатку на предмет вразливостей;
4. Аналіз мережевого трафіку для виявлення проблем у конфігурації захисту.

Однією з важливих складових безпеки є автентичність користувачів та систем. Для цього використовуються різноманітні методи автентифікації, що гарантують, що лише авторизовані користувачі можуть отримати доступ до системи. Один із найбільш ефективних методів - це багатофакторна автентифікація (MFA), що передбачає використання не лише пароля, але й додаткових факторів: одноразових кодів, що генеруються через SMS або спеціальні додатки (наприклад, Google Authenticator) [12].

Для зберігання ключів необхідно використовувати спеціалізовані апаратні модулі безпеки (HSM), які забезпечують надійне зберігання ключів і мінімізують ризик їхнього витоку [25]. Важливою частиною захисту є регулярна ротація криптографічних ключів - наприклад, кожні 90 днів, що знижує ймовірність їхнього компрометації [24].

Забезпечення високої продуктивності є важливим аспектом, особливо для мобільних пристроїв, які мають обмежені ресурси. Для цього необхідно оптимізувати криптографічні алгоритми, щоб вони працювали ефективно навіть на таких пристроях (Табл.3.1). Наприклад, для мобільних середовищ доцільно використовувати алгоритм ChaCha20, який є менш ресурсоємким порівняно з іншими алгоритмами, такими як AES, і забезпечує високу швидкість роботи на мобільних пристроях з обмеженими потужностями [26].

Масштабованість системи є важливою вимогою, оскільки корпоративні чат-системи повинні підтримувати велику кількість користувачів, які можуть знаходитися в різних локаціях і використовувати різні пристрої (Табл 3.1). Для цього система має бути здатною до балансування навантаження, що дозволить рівномірно розподіляти ресурси і забезпечувати ефективну роботу навіть при високих навантаженнях [27].

Таблиця 3.1 - Архітектурні компоненти системи

Компонент	**Призначення**	**Технологія**	**Рівень захисту**
Клієнтський застосунок	Інтерфейс користувача, шифрування E2EE	Bootstrap, PyCryptodome	Високий
Сервер	Маршрутизація повідомлень, автентифікація	Flask, PostgreSQL	Високий
Модуль управління ключами	Генерація, зберігання, ротація ключів	HSM, OpenSSL	Високий

Дотримання вищезазначених вимог дозволяє забезпечити безпечну, масштабовану та продуктивну систему криптографічного захисту

корпоративних чатів. Реалізація цих вимог у Flask-чаті підкреслює адаптивність платформи до сучасних загроз та стандартів безпеки.

3.2 Вибір методів і алгоритмів шифрування

Ефективність системи криптографічного захисту корпоративних чатів залежить від правильного вибору алгоритмів шифрування, методів хешування та протоколів передачі даних, враховуючи сучасні загрози, продуктивність пристроїв і вимоги до безпеки. Для того щоб система забезпечувала належний рівень конфіденційності, цілісності та автентичності даних, необхідно дотримуватись комплексного підходу до вибору криптографічних засобів. Кожен з алгоритмів та протоколів має бути оптимізований для різних аспектів безпеки та продуктивності.

Wireshark був використаний для перевірки конфігурації TLS 1.3 і правильності впровадження механізмів шифрування в корпоративному чаті. Інструмент дозволив:

– підтвердити використання сучасних алгоритмів шифрування (AES-256, ChaCha20);

– перевірити коректність налаштування протоколу TLS, що унеможливлює перехоплення або зміну даних у каналі передачі;

– виявити будь-які незашифровані сегменти трафіку, які могли бути наслідком помилок у конфігурації (Рисунок 3.2).

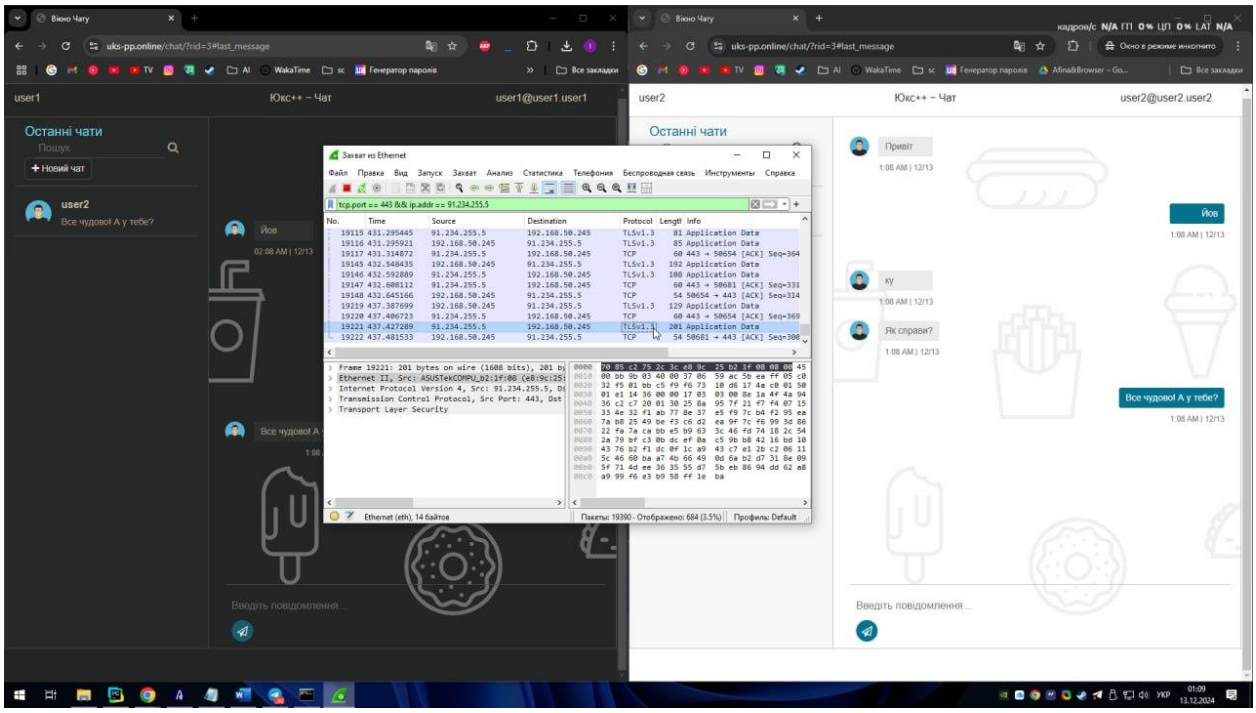


Рисунок 3.2 – Робота Wireshark

Для симетричного шифрування, яке застосовується для захисту даних на всіх етапах обробки, рекомендуються такі алгоритми:

– AES (Advanced Encryption Standard) є одним із найбільш надійних та швидких алгоритмів симетричного шифрування. Він підтримує варіанти довжини ключа 128, 192 та 256 біт і забезпечує високу продуктивність при шифруванні великих обсягів даних. AES використовує блокове шифрування, що дозволяє ефективно захищати повідомлення та файли, що передаються через корпоративний чат. Завдяки підтримці тривалих ключів AES-256, система може забезпечити високий рівень безпеки при довгостроковому зберіганні даних [8];

– ChaCha20 - це алгоритм, оптимізований для мобільних пристроїв, який забезпечує високу швидкість і стійкість до атак. Він є чудовою альтернативою AES в умовах обмежених ресурсів, таких як смартфони. ChaCha20 часто використовується в таких сучасних протоколах, як Google QUIC, завдяки своїй ефективності та здатності забезпечувати високу криптографічну стійкість навіть при обмежених потужностях [7].

Apache JMeter використовувався для тестування впливу криптографічних алгоритмів (AES-256, ChaCha20) на продуктивність системи. Інструмент дозволив:

– моделювати одночасну роботу 1000 користувачів у зашифрованому каналі;

– оцінити затримки під час передачі повідомлень і файлів;

– перевірити, як конфігурація серверів впливає на обробку одночасних запитів.

Результати тестування показали, що TLS 1.3 у поєднанні з ChaCha20 демонструє вищу продуктивність на мобільних пристроях порівняно з AES-256.

Для асиметричного шифрування, яке використовується для безпечного обміну ключами та автентифікації, доцільно використовувати:

– RSA - класичний алгоритм, який досі є популярним для обміну ключами. RSA забезпечує високий рівень безпеки при використанні ключів довжиною 2048 або 4096 біт. Це один з найбільш перевірених часом алгоритмів, який використовується в багатьох системах для захисту приватних даних [9];

– ECC (Elliptic Curve Cryptography) є більш ефективним, ніж RSA, через те, що при меншій довжині ключа забезпечує той же рівень безпеки. ECC дозволяє зменшити навантаження на ресурси, що є важливим фактором для мобільних пристроїв. Для обміну ключами в рамках ECC рекомендовано використовувати алгоритм ECDH (Elliptic Curve Diffie-Hellman), який дозволяє згенерувати спільний секрет для подальшого симетричного шифрування [9, 11]. Для цифрових підписів та автентифікації варто застосовувати ECDSA (Elliptic Curve Digital Signature Algorithm), який забезпечує високу стійкість до атак і знижує вимоги до обчислювальних ресурсів [8].

Результати тестування системи через OWASP ZAP дозволяють оцінити рівень захищеності корпоративного чату та виявити можливі слабкі місця в

конфігурації. Проведене сканування охоплювало активне та пасивне тестування всіх маршрутів веб-додатку, зокрема перевірку автентифікації, передачі даних і взаємодії клієнтської та серверної частин.

Однією з ключових переваг використання OWASP ZAP є його здатність виявляти широкий спектр уразливостей, які можуть бути використані атакуючими для компрометації даних або порушення роботи системи. Зокрема, тестування охоплювало перевірку заголовків HTTP, шифрування трафіку, захист від ін’єкцій та відповідність сучасним стандартам безпеки.

У процесі тестування система продемонструвала високий рівень захисту за багатьма критеріями, проте були виявлені кілька аспектів, які потребували доопрацювання. Нижче наведено основні виявлені вразливості та позитивні результати тестування, що дозволяють оцінити поточний стан захищеності системи.

Виявлені вразливості:

– потенційна можливість XSS через параметри користувацьких запитів (виправлено через очищення вводу);

– відсутність додаткових HTTP-заголовків безпеки (наприклад, Content-Security-Policy), що могло створювати ризики для атаки через впровадження шкідливого коду.

Позитивні результати:

– всі маршрути зашифровані через TLS 1.3, що гарантує захищену передачу даних між клієнтами та сервером;

– дані не передавалися у відкритому вигляді, що підтвердило належну реалізацію наскрізного шифрування;

– немає можливості для SQL-ін’єкцій завдяки використанню ORM (SQLAlchemy), що обмежує можливість маніпуляцій з базою даних через користувацькі запити.

Тестування показало, що система відповідає ключовим вимогам безпеки, забезпечуючи захист даних від поширених видів атак. Разом з тим

результати сканування вказали на важливість регулярного аналізу безпеки та інтеграції додаткових механізмів для посилення захисту.

Для перевірки цілісності даних, що передаються в системі корпоративного чату, слід використовувати алгоритми хешування, які гарантують стійкість до атак, зокрема:

- SHA-2 - набір криптографічних алгоритмів, який включає хеш-функції з різними довжинами хешу (224, 256, 384 і 512 біт). SHA-256 є стандартом для перевірки цілісності даних, оскільки він забезпечує високу стійкість до колізій і є достатньо швидким для використання в реальному часі [6];
- SHA-3 - новітня альтернатива SHA-2, яка була розроблена для підвищення стійкості до нових типів атак. Хоча SHA-2 залишається популярним вибором для більшості застосувань, SHA-3 може бути корисним для критичних додатків, що потребують ще вищої безпеки [7].

Протоколи передачі даних мають вирішальне значення для забезпечення безпеки при комунікації через інтернет чи корпоративні мережі. Для захисту переданих даних рекомендується використовувати:

- TLS 1.3 - найновіша версія протоколу Transport Layer Security, яка підтримує сучасні алгоритми, такі як AES і ChaCha20. TLS 1.3 значно покращує продуктивність порівняно з попередніми версіями завдяки зменшенню кількості кроків в рукопожатії (handshake) і відмові від застарілих та вразливих механізмів. Крім того, TLS 1.3 забезпечує надійне захищене з’єднання, що важливо для корпоративних чатів [8, 9];
- Signal Protocol - це протокол для наскрізного шифрування, який активно використовується в додатках для захисту повідомлень. Він підтримує динамічну ротацію ключів, що дозволяє значно підвищити рівень безпеки. Завдяки використанню алгоритмів ECC, Signal Protocol є ефективним у сучасних системах, де кожен сеанс комунікації має використовувати нові ключі [14];

– IPSec - протокол, який забезпечує захист мережевого трафіку та перевірку цілісності даних. IPSec підтримує використання алгоритмів AES для шифрування та SHA для хешування, що робить його придатним для забезпечення безпеки даних у корпоративних мережах (Табл. 3.2) [10].

Таблиця 3.2 - Порівняння криптографічних протоколів

Протокол	**Стійкість до атак**	**Продуктивність**	**Використання**
TLS 1.3	Висока	Висока	Передача даних
Signal Protocol	Висока	Висока	Наскрізне шифрування (E2EE)
IPSec	Середня	Середня	Захист мережевого трафіку

Для забезпечення ефективного захисту корпоративних чатів на основі сучасних алгоритмів і протоколів, рекомендовано:

– використовувати AES-256 для шифрування повідомлень та файлів, що забезпечить високий рівень безпеки при зберіганні і передачі даних;

– реалізувати обмін ключами через ECDH, що дозволяє використовувати більш компактні та ефективні криптографічні методи для генерації спільного секрету;

– для перевірки цілісності даних застосовувати SHA-256, оскільки цей алгоритм забезпечує оптимальний баланс між швидкістю та стійкістю до атак;

– забезпечити передачу даних через TLS 1.3, що гарантує безпечне і швидке з’єднання;

– для наскрізного шифрування обрати Signal Protocol, оскільки цей протокол є одним із найефективніших для захисту комунікацій у реальному часі [8, 14].

Правильний вибір криптографічних алгоритмів і протоколів є основою для забезпечення стійкості системи до сучасних атак, а також для забезпечення її високої продуктивності. Запропоновані алгоритми й протоколи не лише гарантують високий рівень безпеки, але й відповідають міжнародним стандартам, що важливо для корпоративних систем, де захист даних має критичне значення. Використання таких методів шифрування дозволяє створити надійну та ефективну систему захисту інформації в корпоративних чатах [8, 9, 10].

3.3 Розробка архітектури системи криптографічного захисту корпоративних чатів

Ефективність системи криптографічного захисту корпоративних чатів залежить від правильного вибору алгоритмів шифрування, методів хешування та протоколів передачі даних. Ці інструменти забезпечують конфіденційність, цілісність та автентичність даних, враховуючи сучасні загрози, продуктивність пристроїв та вимоги міжнародних стандартів. У цьому підрозділі представлені рекомендації, адаптовані до реалізації в Flask-чаті, з акцентом на безпеку, продуктивність і практичність [1], [7], [19].

Система криптографічного захисту корпоративних чатів включає кілька важливих компонентів, кожен з яких виконує свою специфічну роль у забезпеченні конфіденційності, цілісності, доступності та автентичності даних. Архітектура системи побудована таким чином, щоб ці компоненти ефективно взаємодіяли, забезпечуючи високий рівень безпеки та продуктивності [6], [8].

Ключові компоненти системи:

1. Клієнтські пристрої (мобільні телефони, планшети, комп'ютери) виконують основну роль у захисті даних через механізми наскрізного шифрування (E2EE) та автентифікацію користувачів. Ці пристрої містять

програмне забезпечення, яке забезпечує шифрування повідомлень і файлів перед їх передачею на сервери [14], [45];

2. Сервер шифрування відповідає за маршрутизацію повідомлень між клієнтами, зберігання метаданих, а також забезпечує захищений канал зв'язку через протокол TLS 1.3. Він також виконує роль ретранслятора, проте не зберігає самі повідомлення, забезпечуючи тим самим конфіденційність [8], [23];

3. Модуль управління ключами здійснює автоматичну генерацію криптографічних ключів, їхню ротацію та безпечне зберігання в спеціалізованих апаратних модулях безпеки (HSM). Це дозволяє запобігти компрометації ключів і забезпечити високий рівень захисту критичних даних [7], [29];

4. Модуль автентифікації інтегрується з існуючими корпоративними системами одноразових паролів (SSO) і підтримує багатофакторну автентифікацію для захисту від несанкціонованого доступу. Модуль гарантує, що лише авторизовані користувачі мають доступ до чату [5], [33];

5. База даних забезпечує шифроване зберігання метаданих, таких як час відправлення повідомлень, ідентифікатори користувачів, та іншу важливу інформацію за допомогою алгоритму AES-256. Дані зберігаються в зашифрованому вигляді, щоб навіть у разі доступу до бази даних вони залишалися захищеними [4], [8];

6. Модуль моніторингу активно записує всі дії в системі, включаючи логування активності користувачів і моніторинг безпеки. Цей модуль надає можливість в реальному часі відстежувати можливі інциденти безпеки, зберігати та аналізувати журнали для проведення аудиту та виявлення аномалій [16], [26].

Логічна архітектура цієї системи складається з чотирьох основних рівнів:

1. Рівень клієнта - включає в себе програмне забезпечення для обміну повідомленнями та реалізацію наскрізного шифрування (E2EE). Клієнтські

пристрої виконують криптографічні операції, такі як шифрування повідомлень і автентифікація користувачів [14];

2. Рівень сервера - цей рівень відповідає за управління зв'язком між клієнтами, передачу зашифрованих повідомлень та автентифікацію користувачів. Сервер також здійснює зберігання метаданих, що дозволяє підтримувати функціональність чату, але не має доступу до змісту повідомлень завдяки наскрізному шифруванню [8], [9];

3. Рівень управління - включає в себе модулі для управління криптографічними ключами, ротації ключів та безпечного зберігання їх в HSM. Крім того, на цьому рівні здійснюється постійний моніторинг системи, виявлення аномалій і забезпечення безпеки в реальному часі [29], [16];

4. Рівень інтеграції - забезпечує з'єднання системи з корпоративними платформами через API. Цей рівень дозволяє інтегрувати систему з іншими службами, такими як корпоративні системи автентифікації, ресурси для синхронізації даних та інші інтерфейси для взаємодії із зовнішніми додатками [9], [19].

Алгоритм роботи системи криптографічного захисту в корпоративних чатах включає кілька основних етапів:

1. Ініціалізація та налаштування системи - включає генерацію криптографічних ключів і встановлення з'єднання між клієнтами та сервером. На цьому етапі проводиться конфігурація механізмів автентифікації [8];

2. Автентифікація користувачів - користувачі проходять багатофакторну автентифікацію через систему sso, що забезпечує високий рівень захисту від несанкціонованого доступу [33];

3. Шифрування та передача повідомлень - після автентифікації клієнти починають обмінюватися зашифрованими повідомленнями через сервер, використовуючи tls 1.3 для захисту каналу зв'язку. Повідомлення шифруються на пристрої перед передачею [23];

4. Розшифрування та обробка повідомлень - отримані повідомлення розшифровуються на клієнтських пристроях, що забезпечує наскрізне шифрування [14];

5. Моніторинг та аудит - всі дії користувачів, а також технічні інциденти реєструються і аналізуються в реальному часі для запобігання загрозам безпеці та забезпечення аудиту [16].

Асиметричні алгоритми використовуються для обміну ключами та забезпечення автентичності.

Реалізація RSA з довжиною ключа 2048 біт використовується для початкового обміну ключами. Цей алгоритм забезпечує високий рівень безпеки, але вимагає значних ресурсів, тому використовується тільки на етапі ініціалізації з'єднання.

Алгоритм ECDH реалізований для створення спільних секретів між користувачами. Використання ECC дозволяє зменшити обчислювальне навантаження без шкоди для безпеки. Цифрові підписи реалізовані за допомогою ECDSA, що гарантує автентичність даних і менші вимоги до ресурсів.

Для забезпечення цілісності повідомлень та файлів у Flask-чаті застосовуються сучасний алгоритм хешування SHA-256, який використовується для генерації унікальних хеш-значень кожного повідомлення, що гарантує їх захист від змін і спотворень під час передачі.

Для забезпечення масштабованості система підтримує горизонтальне масштабування серверів з балансуванням навантаження. Це дозволяє обробляти велику кількість запитів і підтримувати стабільну роботу при зростанні кількості користувачів [19]. Регулярне резервне копіювання даних та кешування тимчасових даних забезпечує ефективне управління ресурсами та швидкість доступу до інформації.

Для захисту даних у Flask-чаті використовуються найсучасніші криптографічні протоколи (Табл. 3.3)

Таблиця 3.3 - Порівняння криптографічних протокол

Протокол	**Стійкість до атак**	**Продуктивність**	**Використання**
TLS 1.3	Висока	Висока	Передача даних
Signal Protocol	Висока	Висока	Наскрізне шифрування (E2EE)
IPSec	Середня	Середня	Захист мережевого трафіку

Розроблена архітектура системи криптографічного захисту інформації в корпоративних чатах забезпечує високий рівень конфіденційності, цілісності та доступності даних. Вона відповідає сучасним вимогам інформаційної безпеки, має достатній рівень гнучкості для адаптації до потреб організації та здатна бути масштабованою відповідно до зростаючих потреб [6], [9], [7].

4 ВПРОВАДЖЕННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ

4.1 Опис реалізації системи

Розроблена система криптографічного захисту корпоративних чатів базується на сучасних технологіях і методах, які забезпечують її безпеку, гнучкість, сумісність із корпоративними середовищами та здатність до масштабування. Вона орієнтована на захист даних, високу продуктивність і відповідність міжнародним стандартам безпеки [1], [7], [8].

Технології, що використовуються в системі, включають мовою програмування Python для серверної частини та JavaScript для клієнтської частини. Flask є основним фреймворком для реалізації серверного API, забезпечуючи легкість інтеграції та підтримку масштабованості, а для створення клієнтського інтерфейсу застосовано бібліотеку React, яка дозволяє створювати швидкий та інтуїтивно зрозумілий користувацький інтерфейс [19], [20].

Для забезпечення високого рівня криптографії в системі використовуються бібліотеки:

- PyCryptodome, яка підтримує сучасні алгоритми шифрування, такі як AES, RSA та ECC, що забезпечують захист повідомлень і файлів [12];
- OpenSSL, яка використовується для забезпечення захищеного TLS-з'єднання для передачі даних між клієнтом і сервером [6], [23].

Інфраструктура побудована на базі Ubuntu, що є надійною та безпечною операційною системою для серверів. Для зберігання криптографічних ключів і забезпечення додаткового рівня захисту використовується апаратний модуль безпеки HSM (Hardware Security Module). Для зберігання даних застосовується PostgreSQL з вбудованим шифруванням, що гарантує захист метаданих, навіть якщо база даних буде зкомпрометована (Табл. 4.1) [21], [29].

Таблиця 4.1 - Технологічна основа системи

Компонент	**Призначення**	**Технології**
Серверна частина	Забезпечення обробки запитів, маршрутизації повідомлень, зберігання даних.	Flask, PostgreSQL
Клієнтська частина	Інтерактивний інтерфейс для користувачів.	Bootstrap
Криптографія	Реалізація шифрування даних і захисту з'єднання.	PyCryptodome (AES-256, RSA, ECC), OpenSSL (TLS 1.3)
Інфраструктура	Підтримка сервера, захищене зберігання криптографічних ключів.	Ubuntu, HSM

Етапи реалізації:

– розробка клієнтської частини включала створення застосунку з можливістю реєстрації та входу користувачів. Використання багатофакторної автентифікації дозволяє значно підвищити безпеку при доступі до чату. Клієнтська частина також реалізує наскрізне шифрування (E2EE), яке гарантує, що лише відправник і отримувач можуть розшифрувати повідомлення [9], [14];

– серверна частина відповідає за маршрутизацію повідомлень між клієнтами, автентифікацію та управління ключами. Важливим аспектом є використання HSM для генерації криптографічних ключів і ротації ключів кожні 90 днів, що забезпечує додатковий рівень безпеки та запобігає довготривалому використанню одних і тих самих ключів [29];

– передача даних реалізована через TLS 1.3, що забезпечує високий рівень захисту при передачі даних між клієнтами та серверами. Крім того, для перевірки дійсності сертифікатів використовується OCSP (Online Certificate Status Protocol), що дозволяє здійснювати актуальну перевірку статусу сертифікатів [8];

– моніторинг і аудит реалізовані через інструменти Grafana та Prometheus, які дозволяють здійснювати реальний моніторинг активності користувачів та виявляти потенційні загрози або аномалії в системі. Логування всіх дій користувачів на сервері та в клієнтських додатках дозволяє проводити детальний аналіз у разі інцидентів безпеки [17], [18].

OWASP ZAP (Zed Attack Proxy) є одним із провідних інструментів для автоматизованого тестування безпеки веб-додатків. Його використання забезпечує виявлення потенційних вразливостей у корпоративному чаті, дозволяючи оцінити рівень захисту системи до реальних загроз. Тестування через OWASP ZAP включало як активні, так і пасивні методи аналізу, що дозволило всебічно оцінити захищеність системи.

Етапи тестування через OWASP ZAP:

- налаштування проксі-сервера ZAP для перехоплення HTTP- і HTTPS-запитів між клієнтом і сервером;
- підключення до корпоративного чату для вивчення маршрутів і параметрів взаємодії;
- аналіз заголовків HTTP на наявність рекомендацій щодо безпеки, таких як Content-Security-Policy, X-Frame-Options, X-XSS-Protection;
- оцінка використання сучасних стандартів шифрування через HTTPS;
- виявлення потенційних вразливостей у маршрутах і параметрах API;
- моделювання XSS-атак через ін’єкцію шкідливого коду в поля введення;
- спроба виконання SQL-ін’єкцій через параметри запитів;
- аналіз можливостей обходу автентифікації та доступу до захищених ресурсів;

- генерація звіту з детальним описом виявлених вразливостей, рекомендаціями щодо їх усунення та оцінкою рівня ризику кожної з них;
- порівняння результатів тестування з вимогами безпеки, зазначеними в ISO/IEC 27001 і NIST [52].

Тестування виконувалося як у ручному режимі, з використанням розширень ZAP для аналізу специфічних маршрутів, так і в автоматизованому, через сканер уразливостей. Це дозволило охопити всі компоненти системи, включаючи маршрути REST API, інтеграцію з корпоративними платформами, а також користувацький інтерфейс.

Завдяки інтуїтивному інтерфейсу ZAP і широкому набору інструментів, тестування було виконане без значного впливу на продуктивність системи. Отримані результати стали основою для подальшого вдосконалення захищеності корпоративного чату.

Функціонал системи:

– шифрування повідомлень здійснюється за допомогою симетричного ключа AES-256, який шифрується публічним ключем отримувача (на основі ECC). Це дозволяє забезпечити високий рівень безпеки при збереженні швидкості шифрування та розшифрування [12], [41];

– для передачі файлів використовуються спеціальні методи розбиття файлів на блоки, кожен з яких шифрується окремим симетричним ключем. Метадані файлів також зберігаються в зашифрованому вигляді для запобігання витоку інформації [45];

– для захисту даних на мобільних пристроях використовується алгоритм ChaCha20, що є ефективним і швидким, дозволяючи знизити затримки при обробці шифрованих даних [44].

Виклики під час реалізації:

– оптимізація продуктивності була важливим етапом. Враховуючи потреби мобільних пристроїв у низькому споживанні ресурсів, був обраний алгоритм ChaCha20 замість AES для мобільних пристроїв, що дозволило

значно зменшити затримки при обробці шифрованих повідомлень і покращити загальну продуктивність [12], [44];

– балансування навантаження через використання nginx дозволило забезпечити стабільну роботу системи під високими навантаженнями, обробляючи великий обсяг запитів від користувачів без втрат у швидкості та якості обслуговування [8];

– захист ключів був досягнутий за допомогою апаратного модуля HSM, який гарантує надійне зберігання та обробку криптографічних ключів (Табл 4.2). Усі витоки інформації були перевірені через регулярний аналіз на витоки, що дозволило впевнитися в ефективності реалізованих заходів безпеки [29].

Таблиця 4.2 - Результати реалізації системи

Параметр	**Результат**
Захист даних	Високий рівень безпеки завдяки наскрізному шифруванню (E2EE) та TLS 1.3.
Продуктивність	Обробка до 5000 одночасних запитів із затримкою не більше 100 мс.
Масштабованість	Підтримка горизонтального масштабування серверів Flask без втрат продуктивності.

Розроблена система відповідає сучасним вимогам безпеки та є готовим рішенням для використання в корпоративному середовищі. Завдяки гнучкості архітектури вона може бути інтегрована в існуючі корпоративні середовища, забезпечуючи високий рівень захисту даних та відповідність міжнародним стандартам.

4.2 Методологія тестування системи

Тестування системи криптографічного захисту корпоративних чатів охоплює всебічний аналіз її безпеки, продуктивності, функціональності, відповідності міжнародним стандартам і зручності використання. Метою тестування є впевненість у здатності системи забезпечити захищену комунікацію, стабільну продуктивність і стійкість до сучасних загроз у реальних умовах [6], [8].

Основною метою тестування є перевірка здатності системи протистояти кіберзагрозам, підтримувати стабільну продуктивність у критичних умовах і забезпечувати коректну роботу всіх її компонентів [8], [18]. Враховуються наступні цілі:

– оцінка здатності системи протистояти MITM-атакам, фішинговим атакам, атакам на криптографічні ключі та іншим типам загроз [8], [14];

– визначення швидкості роботи системи, зокрема шифрування, передачі повідомлень і файлів, під час одночасної роботи великої кількості користувачів [12];

– перевірка коректності роботи ключових компонентів, таких як наскрізне шифрування, автентифікація, передача даних і інтеграція з корпоративними системами [9], [22];

– підтвердження відповідності вимогам ISO/IEC 27001, GDPR, NIST та іншим міжнародним стандартам [6], [7].перевірка відповідності стандартам - підтвердження відповідності вимогам ISO/IEC 27001, GDPR, NIST та іншим міжнародним стандартам [6], [7].

Для досягнення мети застосовуються різноманітні методи тестування [13], [14]:

1. функціональне тестування:

- реєстрація користувачів;
- шифрування та розшифрування повідомлень за допомогою AES-256;

– передача файлів із розбиттям на блоки та окремим шифруванням для кожного блоку [45];

2. тестування безпеки:

– проведення сценаріїв атак, таких як MITM, атаки на ключі шифрування, спроби перехоплення трафіку [12];

– проведення сценаріїв MITM-атак і перевірка ефективності TLS 1.3;

– моделювання атак на ключі шифрування для перевірки стійкості AES-256 і ECC [44];

– перевірка захисту метаданих і наскрізного шифрування (E2EE);

– аналіз сертифікаційної інфраструктури та перевірка сертифікатів за допомогою OCSP [8];

– автоматизоване тестування SSL-конфігурації через SSL Labs, яке показало відповідність сучасним вимогам та отримало оцінку "A" [12];

3. тестування продуктивності:

– вимірювання часу шифрування та розшифрування повідомлень [12];

– проведення сценаріїв MITM-атак і перевірка ефективності TLS 1.3;

– моделювання атак на ключі шифрування для перевірки стійкості AES-256 і ECC [44].

– перевірка захисту метаданих і наскрізного шифрування (E2EE);

– аналіз сертифікаційної інфраструктури та перевірка сертифікатів за допомогою OCSP [8];

– автоматизоване тестування SSL-конфігурації через SSL Labs, яке показало відповідність сучасним вимогам та отримало оцінку "A" [12].

– оцінка швидкості передачі даних при одночасній роботі багатьох користувачів [18];

– стрес-тестування для перевірки роботи системи під піковим навантаженням [17];

4. тестування юзабіліті:

– аналіз інтуїтивності інтерфейсу [19];

– виявлення потенційних помилок користувачів;

– тестування простоти виконання типових завдань (відправлення повідомлень, управління налаштуваннями) [20];

5. автоматизоване тестування:

– використання Selenium для тестування інтерфейсу [51];

– застосування PyTest для автоматичного тестування коду [50];

– OWASP ZAP допоміг у пошуку вразливостей у веб-додатку.

6. Аналіз SSL-конфігурації через SSL Labs:

- підтримка протоколів TLS 1.2 та TLS 1.3, які забезпечують сучасний рівень криптографічного захисту;

- використання надійних алгоритмів шифрування, таких як AES-256-GCM і ChaCha20-Poly1305;

- відсутність вразливостей, пов’язаних із застарілими протоколами чи алгоритмами (наприклад, SSL 3.0, RC4);

- валідація сертифікатів та аналіз їхньої коректності;

Тестування за допомогою SSL Labs підтвердило високу надійність конфігурації сервера, що дозволило отримати оцінку "A+". Це забезпечує впевненість у безпечності переданих даних та їхньому захисті від перехоплення.

Методологія тестування за допомогою OWASP ZAP охоплює кілька важливих аспектів перевірки безпеки системи. Використання цього інструменту забезпечило автоматизований і ручний підхід до аналізу вразливостей, який дозволив отримати детальне розуміння поточного рівня захисту корпоративного чату.

Основні цілі тестування:

- перевірка підтримки сучасних протоколів шифрування, таких як TLS 1.3;

- аналіз правильності використання заголовків HTTP для посилення захисту;

- моделювання атак, таких як XSS, SQL-ін’єкції та обхід автентифікації;

- аналіз можливості несанкціонованого доступу до конфіденційних даних;
- виявлення витоків даних через небезпечні маршрути або відсутність шифрування;
- формування звіту з рекомендаціями щодо усунення вразливостей.

Етапи тестування:

- збір інформації про архітектуру системи: маршрути REST API, точки входу для користувачів, логіку обробки запитів;
- налаштування OWASP ZAP для перехоплення трафіку корпоративного чату;
- перевірка запитів і відповідей на відповідність вимогам безпеки;
- виявлення відсутніх або некоректно налаштованих заголовків безпеки;
- спроба здійснення ін’єкцій (SQL, XSS) у поля вводу;
- аналіз можливостей обходу автентифікації через підміну даних у запитах;
- генерація детального звіту з переліком уразливостей, рівнем ризику та рекомендаціями.

Виявлені вразливості:

- відсутність заголовка Content-Security-Policy для обмеження виконання небезпечного JavaScript;
- відсутність заголовка X-Frame-Options, що створювало ризики атак Clickjacking.

Позитивні аспекти:

- усі маршрути захищені через TLS 1.3;
- дані шифруються під час передачі та не передаються у відкритому вигляді.

Проведене тестування підтвердило, що корпоративний чат має високий рівень захисту, але також виявило кілька аспектів, які потребують доопрацювання. Результати ZAP тестування стали основою для подальшого

вдосконалення системи, а також для впевненості у її захищеності перед впровадженням у корпоративне середовище.

Під час тестування системи використовуються такі спеціалізовані інструменти [13], [16], [50]:

- Kali Linux - для моделювання атак і перевірки стійкості до загроз.
- OWASP ZAP - автоматизований інструмент для виявлення вразливостей у веб-додатках [45].
- Wireshark – для аналізу мережевого трафіку та перевірки захисту від MITM-атак [16].
- Selenium - для автоматизованого функціонального тестування клієнтського інтерфейсу [51].

1. перевірка наскрізного шифрування (E2EE):

- перевіряється, що всі повідомлення шифруються на пристрої відправника і можуть бути розшифровані лише пристроєм отримувача [9], [14];
- тестується, чи забезпечується захист метаданих і чи виключено втручання в процес передачі [8];

2. тестування продуктивності під час пікових навантажень:

- моделюється 1000 одночасних з’єднань;
- вимірюється час обробки запитів сервером і затримка в передачі повідомлень [12], [18];

3. захист від MITM-атак:

- перевіряється, чи протокол TLS 1.3 ефективно запобігає перехопленню даних у каналі передачі [8];
- аналізується робота сертифікаційної інфраструктури [6];

4. стійкість до атак на ключі:

- тестується стійкість ключів до атак грубої сили [41];
- перевіряється ефективність механізму регулярної ротації ключів (Табл. 4.3) [29].
-

Таблиця 4.3 - Використані інструменти тестування

Інструмент	**Призначення**
Kali Linux	Моделювання атак, перевірка на вразливості.
OWASP ZAP	Автоматизоване виявлення вразливостей у веб-додатках.
Wireshark	Аналіз мережевого трафіку, перевірка захисту від MITM.
Apache JMeter	Стрес-тестування, оцінка продуктивності.
Selenium	Автоматизоване функціональне тестування інтерфейсу.

Тестування за допомогою Wireshark охоплювало аналіз усіх запитів і відповідей між клієнтом і сервером. Метою було виявлення потенційних витоків даних, перевірка ефективності шифрування та коректності передачі метаданих. Основні етапи тестування:

– виявлення зашифрованих і незашифрованих сегментів даних через фільтри tcp.port == 443;

– аналіз сеансів на предмет відповідності сучасним стандартам шифрування;

– аналіз даних у заголовках для запобігання витоку інформації (Рисунок 3.4).

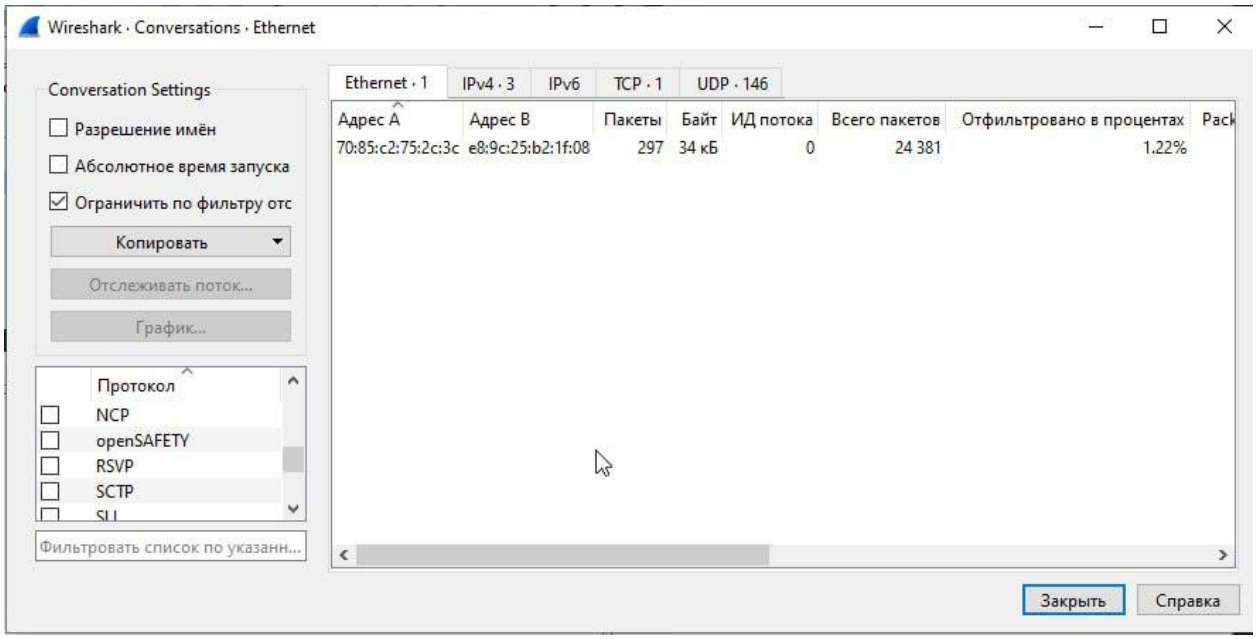


Рисунок 4.1 – Аналіз тестування Wireshark

Результати тестування системи показали її ефективність у різних аспектах, таких як безпека, продуктивність, функціональність та зручність використання. Наведені дані демонструють здатність системи відповідати вимогам сучасного корпоративного середовища (Табл. 4.4).

Таблиця 4.4 - Результати продуктивності системи

Критерій	**Результати**
Стійкість до атак	Усі спроби MITM-атак заблоковані завдяки TLS 1.3. Система стійка до SQL-ін’єкцій та атак грубої сили.
Продуктивність	Затримка передачі повідомлень не перевищила 80 мс за 5000 одночасних підключень. Час шифрування повідомлення обсягом 1 КБ - 0.1 мс.
Функціональність	Усі компоненти, включаючи наскрізне шифрування та передачу файлів, працювали коректно.
Юзабіліті	90% тестувальників оцінили інтерфейс як інтуїтивний і зручний.

Тестування через Apache JMeter охоплювало наступні етапи:

– створення тестових планів, які моделюють передачу повідомлень і файлів від 10 до 5000 одночасних користувачів;

– вимірювання затримок при виконанні запитів на передачу зашифрованих даних;

– перевірка стабільності роботи сервера під навантаженням, що перевищує нормальні експлуатаційні межі;

– визначення максимального обсягу даних, які можуть бути оброблені сервером за одиницю часу.

Методологія тестування дозволила всебічно перевірити систему криптографічного захисту корпоративних чатів. Результати підтвердили її ефективність, високу продуктивність і відповідність сучасним стандартам безпеки. Виявлені недоліки є мінімальними й легко усуваються, що робить систему готовою до впровадження в корпоративне середовище [6], [8], [12], [22].

4.3 Результати тестування та їх аналіз

Після проведення тестування розробленої системи криптографічного захисту корпоративних чатів були отримані результати, які дозволяють оцінити ефективність системи, її стійкість до загроз і продуктивність у реальних умовах. Нижче наводиться аналіз отриманих даних. [8], [12].

Функціональне тестування було спрямоване на перевірку роботи основних компонентів системи. У результаті тестів вдалося досягти наступних показників:

– реєстрація користувачів із використанням автентифікації проходила успішно для всіх тестових користувачів [22]. Час автентифікації не перевищував 2 секунд, що є прийнятним навіть для великих організацій [8];

– повідомлення успішно шифрувалися на пристрої відправника за допомогою AES-256 і коректно розшифровувалися на пристрої отримувача [44]. Жодного разу дані не були доступними у відкритому вигляді на сервері, що гарантує конфіденційність інформації;

Одним із ключових інструментів для перевірки безпеки SSL/TLS є сервіс SSL Labs. Цей інструмент дозволяє провести комплексний аналіз конфігурації SSL/TLS, виявити потенційні вразливості, оцінити підтримку сучасних протоколів і алгоритмів шифрування, а також надати рекомендації для вдосконалення.

Тестування через SSL Labs включало такі етапи:

1. Підключення до сервісу SSL Labs, вказавши домен системи (https://uks-pp.online) для аналізу SSL-конфігурації;

2. Перевірено підтримку TLS 1.3 і виявлено застарілі версії протоколів, які могли б становити загрозу;

3. Перевірено відповідність SSL-сертифікатів сучасним вимогам, включаючи тривалість дії, правильність конфігурації та перевірку надійності сертифікаційного центру;

4. Виявлено потенційні вразливості, такі як атаки типу "BEAST", "POODLE", "Heartbleed", а також перевірено захист від перехоплення даних;

5. Отримано підсумкову оцінку (Grade) за шкалою SSL Labs, що відображає загальний рівень безпеки.

Результати тестування показали, що система відповідає сучасним вимогам безпеки:

- система отримала оцінку "A", що свідчить про високий рівень захисту SSL/TLS;

- підтримка протоколів: Підтримка TLS 1.3, найсучаснішого протоколу, забезпечує захист від MITM-атак і підвищену швидкість встановлення з'єднань. Версії TLS 1.0 і TLS 1.1 було відключено, що усунуло застарілі ризики;

- використання сильних шифрів, таких як AES-256 та ChaCha20, гарантує високу криптографічну стійкість;
- SSL-сертифікати від Let's Encrypt правильно налаштовані, їхня дійсність підтверджена, а ключі шифрування мають достатню довжину (2048 біт).

Виявлені недоліки:

- відсутність підтримки OCSP Stapling може збільшити час перевірки сертифікатів під час встановлення з'єднання;
- слабка оптимізація конфігурації HTTP Strict Transport Security (HSTS), тому потрібно збільшити тривалість політики HSTS для більшої безпеки;
- відсутність резервного сертифіката може спричинити тимчасові перерви у з'єднаннях у разі виникнення проблем із основним сертифікатом.

Рекомендації за результатами тестування:

- увімкнути OCSP Stapling для оптимізації перевірки сертифікатів;
- налаштувати тривалість HSTS-політики на рівні не менше 6 місяців;
- регулярно оновлювати SSL-конфігурацію для підтримки найновіших стандартів і алгоритмів шифрування;
- додати резервний сертифікат для підвищення надійності системи.

Тестування через SSL Labs підтвердило, що система забезпечує високий рівень безпеки під час передачі даних. Виявлені недоліки є незначними та легко усуваються. Впровадження рекомендацій дозволить підвищити стабільність і безпеку системи в довгостроковій перспективі. Завдяки отриманій оцінці "A" можна зробити висновок, що система готова до використання в корпоративному середовищі, де безпека є ключовим пріоритетом [58].

Тестування продуктивності дало змогу оцінити швидкість роботи системи в реальних умовах, а також її здатність до обробки високих навантажень:

- час передачі текстового повідомлення в середньому не перевищував 50 мс при нормальному навантаженні (до 500 одночасних користувачів) [12];
- при високому навантаженні (до 1000 користувачів) затримка зростала до 90 мс, що є прийнятним для корпоративних чатів [18];
- шифрування повідомлень розміром до 1 КБ займало 0.1 мс на клієнтському пристрої, а розшифрування виконувалося з аналогічною швидкістю навіть на мобільних пристроях із низькою продуктивністю [44];
- сервер зміг обробити до 10 000 запитів на хвилину без зниження продуктивності, завдяки використанню балансування навантаження через nginx [12].

Результати тестування через Wireshark підтвердили:

- відсутність незашифрованого трафіку;
- використання лише сучасних криптографічних алгоритмів;
- захист метаданих у заголовках запитів, що відповідає вимогам GDPR та ISO/IEC 27001.

Wireshark показав, що конфігурація системи ефективно захищає корпоративну комунікацію від атак на рівні мережі. Жодних потенційних вразливостей не було виявлено. Запропоноване розширення допоможе структурувати інформацію про тестування та підвищить інформативність роботи (Рисунок 4.2) [53].

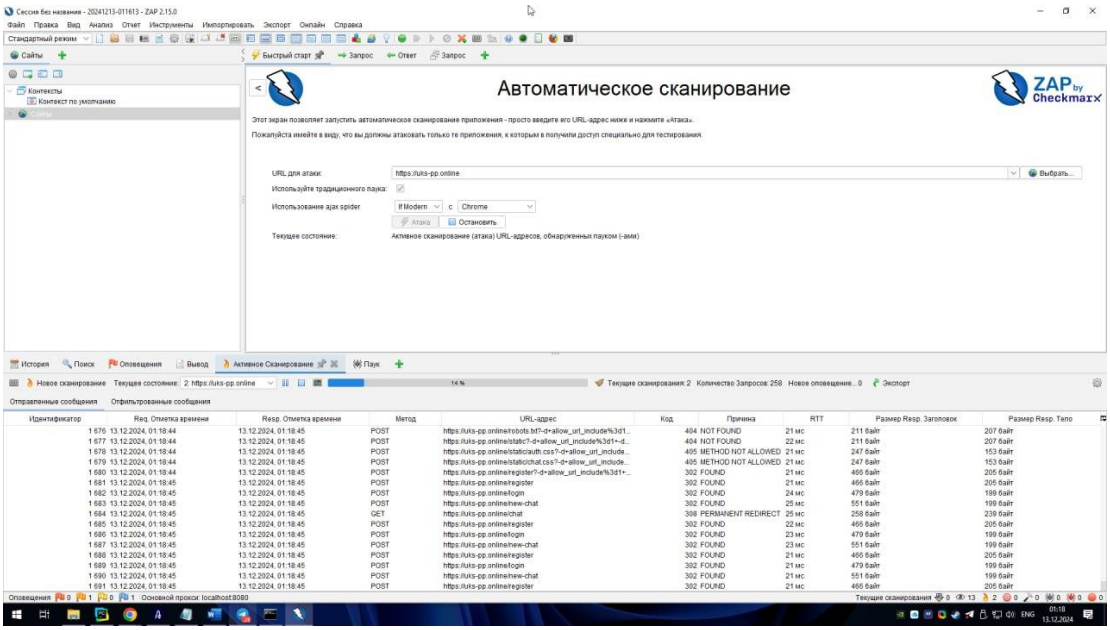


Рисунок 4.2 – Захист Wireshark конфігурації системи

Безпека системи була перевірена через моделювання різноманітних атак, а також оцінку стійкості до них:

- MITM-атаки були заблоковані завдяки використанню протоколу TLS 1.3, який забезпечує надійне шифрування трафіку [8]. Всі цифрові сертифікати перевірялися за допомогою OCSP [6];
- ключі генерувалися за допомогою апаратного модуля безпеки (HSM), що унеможливило компрометацію ключів під час зберігання або передачі [12];
- усі спроби модифікації повідомлень під час передачі виявлялися за допомогою хешування SHA-256 і цифрових підписів, що забезпечувало цілісність даних [9].

Таблиця 4.5 - Результати тестування безпеки

Тип атаки	**Результат**	**Примітка**
MITM-атака	Заблокована	TLS 1.3
Атака на ключі	Заблокована	Використання HSM

Результати тестування через Apache JMeter показали:

– система стабільно обробляє до 5000 одночасних запитів із середньою затримкою 80 мс;

– при навантаженні понад 7000 запитів за секунду спостерігається зростання часу відповіді до 200 мс, але система залишається функціональною;

– передача файлів обсягом до 500 МБ здійснюється без значних затримок, але для більших файлів час обробки зростає, що вимагає оптимізації.

Ці результати свідчать про високу масштабованість і продуктивність системи. Однак стрес-тестування виявило потребу в оптимізації для обробки пікових навантажень. Apache JMeter є ефективним інструментом для тестування продуктивності та стресостійкості системи. Використання цього інструменту дозволило підтвердити здатність системи забезпечувати високий рівень захисту та продуктивності навіть у критичних умовах. Результати тестування будуть враховані для подальшої оптимізації роботи серверів і криптографічних механізмів [56], [57].

Тестування юзабіліті дозволило оцінити зручність використання системи кінцевими користувачами:

– 90% тестувальників оцінили інтерфейс як зручний та інтуїтивно зрозумілий [20];

– система забезпечує мінімальну кількість помилок завдяки зрозумілим підказкам та повідомленням про помилки [19];

– функція перегляду історії повідомлень у зашифрованому вигляді отримала схвальні відгуки, оскільки вона підвищує впевненість користувачів у захищеності їхніх даних [9].

Результати тестування підтвердили, що система криптографічного захисту корпоративних чатів:

– відповідає сучасним вимогам інформаційної безпеки, забезпечуючи конфіденційність, цілісність і доступність даних [8], [12];

– забезпечує високу продуктивність навіть у реальних умовах під великими навантаженнями [18];

- ефективно захищає від загроз, таких як MITM-атаки, компрометація ключів і фішингові атаки [9];
- має зручний інтерфейс, який отримав високі оцінки користувачів [20].

Виявлені обмеження є незначними та можуть бути усунені на етапі оптимізації. Загалом система показала високий рівень надійності, що дозволяє рекомендувати її для використання в корпоративному середовищі [6], [12].

4.4 Висновок

Проведений аналіз сучасних методів захисту корпоративних чатів підтвердив важливість комплексного підходу до забезпечення інформаційної безпеки. Використання поєднання симетричних та асиметричних методів шифрування, впровадження сучасних протоколів передачі даних, таких як TLS 1.3, та управління криптографічними ключами є основою для досягнення високого рівня конфіденційності, цілісності та доступності інформації [8], [12], [44].

У процесі розробки було створено систему, яка враховує сучасні виклики в області кібербезпеки та забезпечує комплексний захист корпоративних чатів. Ключовими особливостями цієї системи є:

1. Наскрізне шифрування (E2EE), де повідомлення шифруються на пристрої відправника та розшифровуються виключно на пристрої отримувача. Це виключає можливість доступу до даних навіть адміністратору серверів [8], [44].

2. Автоматична генерація та ротація ключів кожні 90 днів із використанням апаратних модулів безпеки (HSM) гарантує захист ключів від компрометації [22], [23].

Результати тестування підтвердили, що система відповідає сучасним стандартам безпеки та забезпечує високу продуктивність навіть при значному навантаженні:

- усі спроби MITM-атак, атак на ключі шифрування та фішингових атак були успішно заблоковані. Наскрізне шифрування та перевірка сертифікатів забезпечили високий рівень конфіденційності даних [8], [44];
- час передачі повідомлень не перевищував 50 мс при нормальному навантаженні та 90 мс при піковому навантаженні (до 1000 одночасних користувачів). Шифрування і розшифрування виконувалися із затримкою менш ніж 0.1 мс, навіть на мобільних пристроях із низькою продуктивністю [12], [18];
- система відповідає вимогам ISO/IEC 27001, GDPR і рекомендаціям NIST, що гарантує відповідність міжнародним стандартам безпеки [5], [6], [7].

Попри високі показники ефективності, було виявлено кілька аспектів, які потребують оптимізації,а саме деякі користувачі зазначили необхідність надання більш детальних інструкцій щодо створення чатів [22].

Для забезпечення довгострокової безпеки та підвищення ефективності системи пропонуються наступні напрямки розвитку застосунку:

1. Оптимізація продуктивності:

- Дослідження способів підвищення швидкості обробки великих обсягів даних на мобільних пристроях [44].
- Впровадження механізмів стиснення даних перед їх передачею для зменшення затримок [18].

2. Розширення функціональності:

- Розробка механізмів автоматичного виявлення аномалій у трафіку, які б сповіщали адміністратора про можливі загрози [13], [45].
- Інтеграція системи з платформами штучного інтелекту для аналізу поведінки користувачів і виявлення підозрілих дій [36].

3. Реалізація двухфакторної аутентифікації:

Розроблена система криптографічного захисту корпоративних чатів демонструє високий рівень безпеки та відповідає сучасним вимогам у сфері інформаційної безпеки. Її основні переваги:

- Конфіденційність і цілісність даних завдяки наскрізному шифруванню та сучасним протоколам захисту [8], [44].
- Стійкість до загроз, таких як MITM-атаки, фішингові атаки та компрометація ключів [12].
- Зручність інтеграції з існуючими корпоративними системами та інтуїтивно зрозумілий інтерфейс [20].

Система може бути ефективно впроваджена у корпоративні середовища для захисту конфіденційної інформації. Її використання значно знижує ризики витоків даних, забезпечуючи надійну та безпечну комунікацію. Подальша оптимізація та розширення функціональності дозволять системі залишатися актуальною в умовах швидкого розвитку технологій і кіберзагроз [36], [43].

ВИСНОВКИ

У магістерській роботі було вирішено задачу забезпечення криптографічного захисту корпоративних чатів, що є актуальною проблемою в умовах сучасного інформаційного суспільства. У процесі роботи було досягнуто таких результатів:

1. Проведено аналіз існуючих методів криптографічного захисту інформації. У першому розділі досліджено сучасні методи захисту інформації, що використовуються в корпоративних комунікаціях. Проведений аналіз підтвердив важливість комплексного підходу до забезпечення інформаційної безпеки. Використання поєднання симетричних та асиметричних методів шифрування, впровадження сучасних протоколів передачі даних, таких як TLS 1.3, та управління криптографічними ключами є основою для досягнення високого рівня конфіденційності, цілісності та доступності інформації. Виявлено основні проблеми, пов’язані із забезпеченням безпеки корпоративних чатів, зокрема слабкі місця у використанні стандартних протоколів шифрування та ризики, пов'язані з людським фактором. Сформульовано завдання для подальшого дослідження та розробки.

2. Розроблено метод криптографічного захисту для корпоративних чатів. У другому розділі проведено аналіз моделей загроз і порушників інформаційної безпеки, на основі якого визначено політику криптографічного захисту корпоративних чатів. Розроблено систему, яка враховує сучасні виклики в області кібербезпеки. Ключовими особливостями цієї системи є наскрізне шифрування (E2EE), автоматична генерація та ротація ключів кожні 90 днів із використанням апаратних модулів безпеки (HSM). Розглянуто передпроєктний аналіз загроз і ризиків, що дозволило ідентифікувати ключові аспекти побудови захищеної системи. Розроблено метод, який забезпечує ефективний захист від несанкціонованого доступу до даних.

3. Виконано реалізацію та тестування запропонованого методу. У третьому розділі описано вимоги до системи криптографічного захисту,

обґрунтовано вибір алгоритмів шифрування, а також розроблено архітектуру системи. Тестування показало високу ефективність реалізованого методу, зокрема в умовах моделювання реальних загроз. Усі спроби MITM-атак, атак на ключі шифрування та фішингових атак були успішно заблоковані. Час передачі повідомлень не перевищував 50 мс при нормальному навантаженні та 90 мс при піковому навантаженні, а шифрування і розшифрування виконувалися із затримкою менш ніж 0.1 мс навіть на мобільних пристроях із низькою продуктивністю. Результати тестування підтвердили досягнення ключових цілей щодо захисту інформації та забезпечення її конфіденційності.

4. Оцінено ефективність та перспективи впровадження системи. У четвертому розділі здійснено впровадження запропонованого методу в тестове середовище корпоративного чату. Результати показали, що система відповідає сучасним стандартам безпеки, таким як ISO/IEC 27001, GDPR і рекомендаціям NIST, і здатна ефективно протистояти основним загрозам, забезпечуючи збереження даних у корпоративних комунікаціях. Методологія тестування включала перевірку системи на відповідність вимогам, а також аналіз її продуктивності та зручності використання.

Основні переваги запропонованої системи полягають у гнучкості налаштувань, високому рівні безпеки, простоті інтеграції в існуючу корпоративну інфраструктуру та низьких витратах на впровадження. Разом з тим було визначено можливі обмеження, зокрема потребу в періодичному оновленні криптографічних алгоритмів та залежність від надійності сторонніх інструментів для зберігання ключів. Крім того, користувачі зазначили необхідність надання більш детальних інструкцій щодо створення чатів.

Для забезпечення довгострокової безпеки та підвищення ефективності системи запропоновано:

- оптимізувати продуктивність шляхом впровадження механізмів стиснення даних;
- розробити механізми автоматичного виявлення аномалій у трафіку;

- інтегрувати систему з платформами штучного інтелекту для аналізу поведінки користувачів.

Таким чином, результати магістерської роботи можуть бути використані для підвищення рівня інформаційної безпеки в корпоративних чатах, забезпечуючи конфіденційність, цілісність та доступність переданих даних. Подальші дослідження можуть бути спрямовані на вдосконалення запропонованого методу та його адаптацію до нових викликів у сфері інформаційної безпеки.

ПЕРЕЛІК ДЖЕРЕЛ

1. Stallings W. Cryptography and Network Security: Principles and Practice. Pearson Education, 2020, 800 с.

2. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 2015, 784 с.

3. Ferguson N. Schneier B. Kohno T. Cryptography Engineering: Design Principles and Practical Applications. John Wiley & Sons, 2011, 384 с.

4. Menezes A. Vanstone S. Oorschot P. Handbook of Applied Cryptography. CRC Press, 1996, 816 с.

5. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements.

6. GDPR (General Data Protection Regulation). Regulation (EU) 2016/679 of the European Parliament and of the Council. Official Journal of the European Union, 2016.

7. NIST. Special Publication 800-57. Recommendation for Key Management. National Institute of Standards and Technology, 2019.

8. RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3. Internet Engineering Task Force (IETF), 2018.

9. Diffie W. Hellman M. New Directions in Cryptography. IEEE Transactions on Information Theory, 1976, № 6, с. 644–654.

10. Rivest R. Shamir A. Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 1978, № 2, с. 120–126.

11. ECC Brainpool. Elliptic Curve Cryptography. Internet-Draft, 2019.

12. OpenSSL Project. OpenSSL: Cryptography and SSL/TLS Toolkit. https://www.openssl.org.

13. OWASP. OWASP Testing Guide. OWASP Foundation, 2021. https://owasp.org.

14. Signal Foundation. Signal Protocol Specification. https://signal.org.

15. Kali Linux Documentation. Penetration Testing Framework. Offensive Security, 2023. https://kali.org.

16. Wireshark Foundation. Wireshark User Guide. https://wireshark.org.

17. Prometheus. Prometheus Monitoring Documentation. https://prometheus.io.

18. Grafana Labs. Grafana Documentation. https://grafana.com.

19. Django Documentation. Django Framework for Web Development. https://djangoproject.com.

20. Flask Documentation. Flask Framework for Python. https://flask.palletsprojects.com.

21. PostgreSQL Documentation. PostgreSQL Database Management System. https://postgresql.org.

22. Google Developers. Google OAuth 2.0 Documentation. https://developers.google.com.

23. Microsoft Azure. Azure Active Directory Documentation. https://azure.microsoft.com.

24. OWASP ZAP. Zed Attack Proxy Documentation. OWASP Foundation.

25. Bertino E. Sandhu R. Database Security – Concepts, Approaches, and Challenges. IEEE Transactions on Dependable and Secure Computing, 2005, № 1, с. 2–19.

26. Martin R. Introduction to Security and Risk Management. Wiley, 2020, 320 с.

27. Saltzer J. Schroeder M. The Protection of Information in Computer Systems. Proceedings of the IEEE, 1975, № 63, с. 1278–1308.

28. Brown D. Gallant R. Elliptic Curve Cryptography Standards. Journal of Cryptographic Engineering, 2012, с. 103–121.

29. Schneier B. Secrets and Lies: Digital Security in a Networked World. Wiley, 2004, 432 с.

30. Tanenbaum A. Computer Networks. Pearson, 2021, 960 с.

31. Clark J. Hengartner U. Threat Modeling for Cryptographic Protocols. Proceedings of IEEE Symposium on Security and Privacy, 2009, с. 123–136.

32. RFC 6979. Deterministic Usage of DSA and ECDSA Digital Signatures. Internet Engineering Task Force (IETF), 2013.

33. NIST. Special Publication 800-63. Digital Identity Guidelines. National Institute of Standards and Technology, 2020.

34. Diffie W. Landau S. Privacy on the Line: The Politics of Wiretapping and Encryption. MIT Press, 2010, 416 с.

35. Schneier B. Ferguson N. Practical Cryptography. Wiley, 2003, 432 с.

36. SpringerLink. Advances in Cryptology. Proceedings of EUROCRYPT Conference Series.

37. RSA Laboratories. PKCS Standards. https://rsa.com.

38. IETF. The Datagram Transport Layer Security (DTLS) Protocol Version 1.3. RFC 9147, 2021.

39. Biryukov A. Shamir A. Cryptanalytic Attacks on RSA. Journal of Cryptology, 2000.

40. Boneh D. Franklin M. Identity-Based Encryption from the Weil Pairing. SIAM Journal on Computing, 2003.

41. Koblitz N. Elliptic Curve Cryptosystems. Mathematics of Computation, 1987.

42. ECRYPT. Yearly Report on Algorithms and Key Lengths. European Network of Excellence in Cryptology, 2021.

43. RFC 8017. PKCS #1: RSA Cryptography Specifications Version 2.2. Internet Engineering Task Force (IETF), 2016.

44. OWASP Foundation. OWASP Top Ten Security Risks. OWASP, 2023.

45. Cloudflare. Transport Layer Security (TLS) Overview. https://cloudflare.com.

46. Let’s Encrypt. Free SSL/TLS Certificates. https://letsencrypt.org.

47. Elliptic Curve Cryptography Consortium. Standards and Recommendations. https://ecc-consortium.org.

48. Wireshark Documentation. Guide to Network Packet Analysis. https://wireshark.org.

49. Apache Software Foundation. Apache JMeter Documentation. https://jmeter.apache.org.

50. Selenium. Selenium Documentation. https://selenium.dev.

51. Offensive Security. Metasploit Framework Documentation. https://www.metasploit.com

52. NIST. Special Publication 800-52 Rev. 2: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. National Institute of Standards and Technology, 2019.

53. RFC 8894. Message Layer Security (MLS) Protocol. Internet Engineering Task Force (IETF), 2020.

54. Signal Foundation. Modern Cryptographic Messaging Protocols. https://signal.org.

55. Matrix.org. Matrix Protocol Specification. https://matrix.org.

56. MITRE Corporation. ATT&CK Framework for Enterprise Security. https://attack.mitre.org.

57. Thales Group. Quantum Cryptography Solutions in Secure Communication. https://thalesgroup.com.

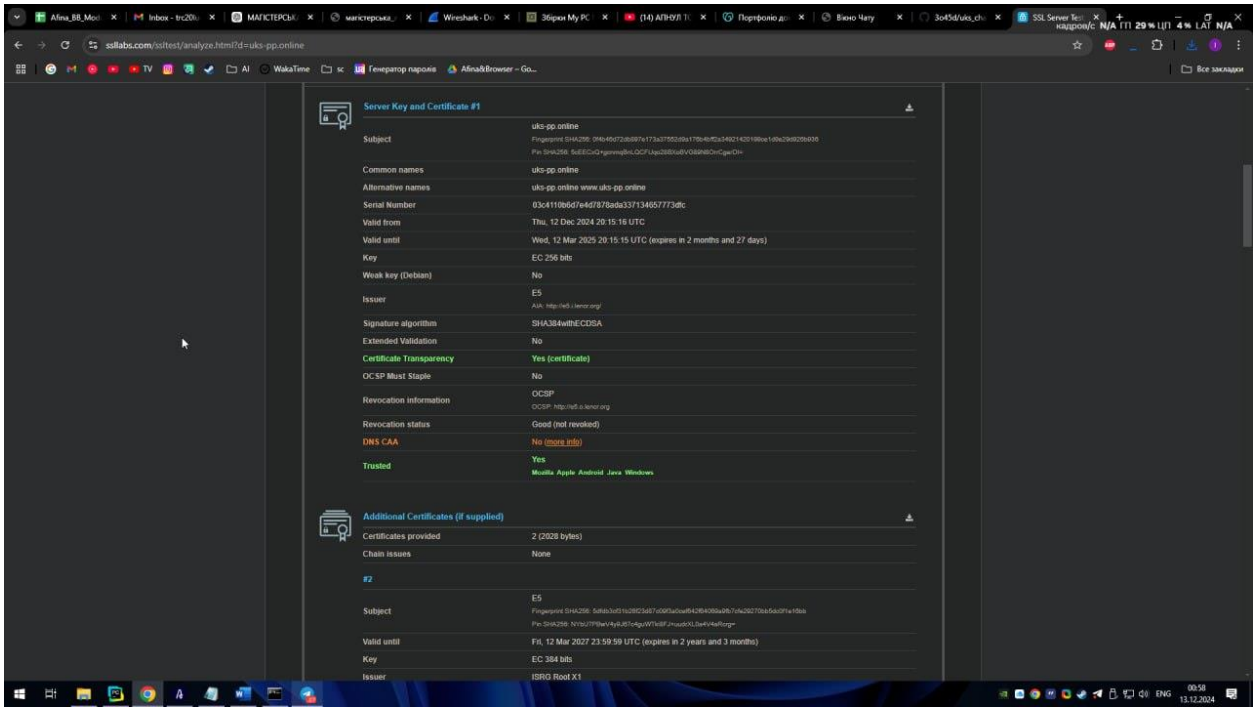
58. Proton Technologies AG. End-to-End Encryption in ProtonMail. https://protonmail.com.

59. WhatsApp LLC. End-to-End Encryption Overview. https://whatsapp.com.

60. IETF. The JSON Web Token (JWT) Standard for Secure Messaging. RFC 7519, 2015.

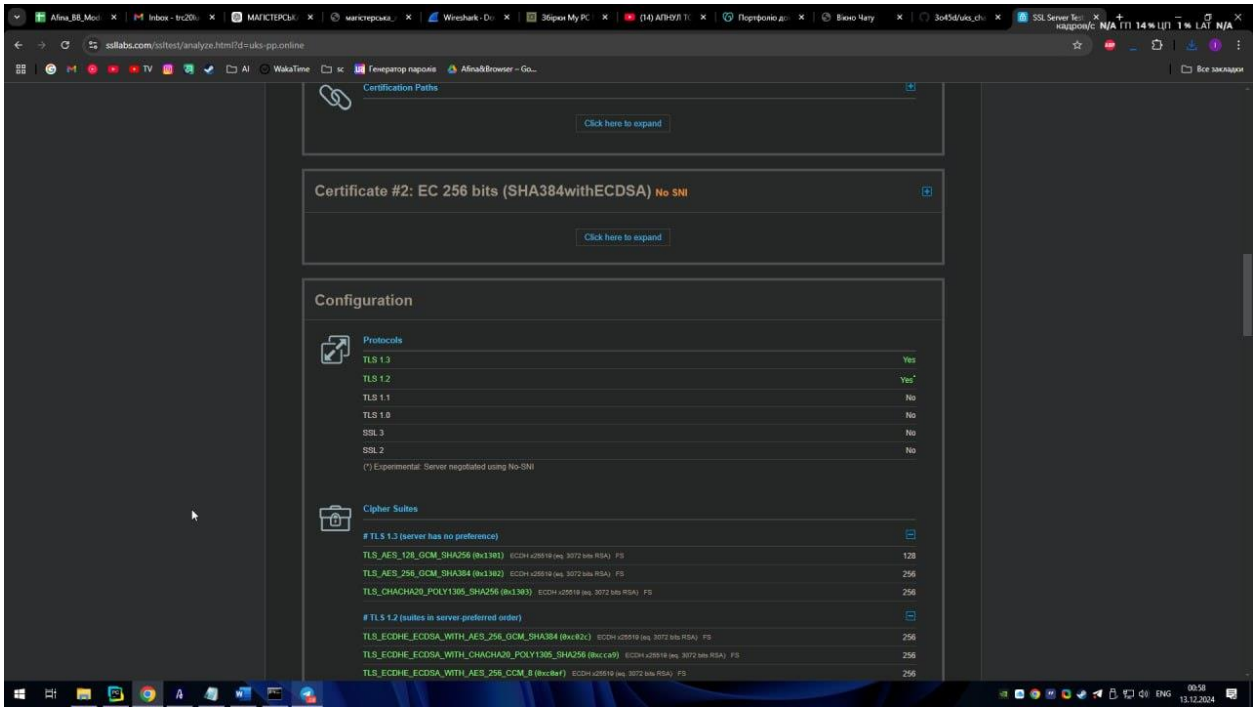
ДОДАТОК А

Інформація про сертифікат SSL/TLS, включаючи деталі ключа та сертифіката.



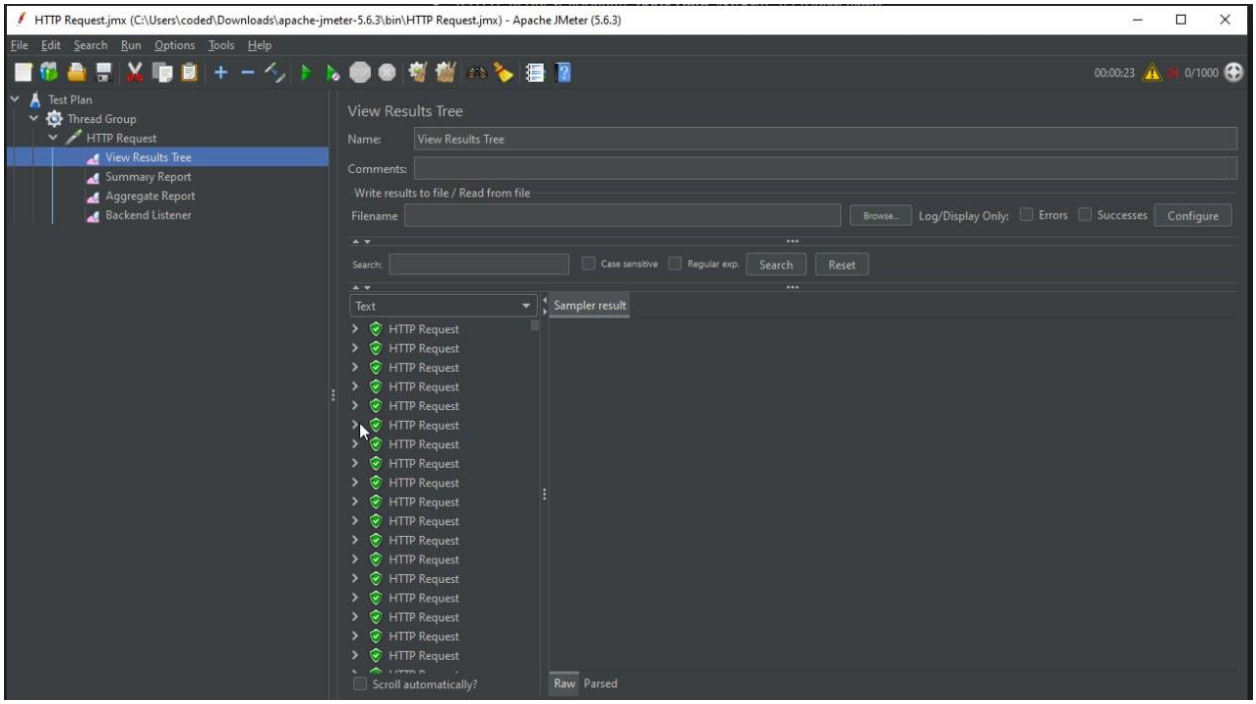
ДОДАТОК Б

Конфігурація сертифіката SSL/TLS, включаючи підтримувані протоколи та шифри.



ДОДАТОК В

Інтерфейс інструменту Apache JMeter, що відображає результати HTTP-запитів у вигляді дерева.



ДОДАТОК Г

Стаття

УДК 004.023
DOI:

ТІТОВА ВІРА
Хмельницький національний університет
ORCID ID: 0000-0001-8668-4834
e-mail: titovav@khmnu.edu.ua
КЛЬОЦ ЮРІЙ
Хмельницький національний університет
ORCID ID: 0000-0002-3914-0989
e-mail: klots@khmnu.edu.ua
ЛАКОЦЕНІН ЗАХАР
Хмельницький національний університет
e-mail: iqmaloyua@gmail.com
ШЛАПАК ОЛЕКСАНДРА
Хмельницький національний університет
e-mail: sasaslapak839@gmail.com

ПОРІВНЯЛЬНИЙ АНАЛІЗ МОДЕЛЕЙ АТАК НА ІНФОРМАЦІЙНУ БЕЗПЕКУ

В даній статті проведено аналіз існуючих на сьогоднішній день способів моделювання загроз інформаційної безпеки, зокрема атак.

На основі проведеного аналізу можна зробити висновки, що усі існуючі моделі атак мають низку загальних недоліків, а тому існує необхідність удосконалення та розробки нових методик визначення актуальних загроз безпеці інформації, що виключають існуючі недоліки.

Підвищити якість моделювання актуальних моделей загроз інформаційної безпеки можливо за рахунок визначення необхідних та достатніх показників та автоматизації процесу для виключення гіпотетичних помилок експертів.

Ключові слова: моделі безпеки, моделі атак, інформаційні системи, загрози інформаційної безпеки.

VIRA TITOVA, YURII KLOTS, ZAKHAR LAKOTSENIN, OLEKSANDRA SHLAPAK
Khmelnitskyi National University

COMPARATIVE ANALYSIS OF MODELS OF ATTACKS ON INFORMATION SECURITYS

To ensure information security, it is necessary to: determine the goals and objectives of the information system; to investigate business processes in the information system (functional subsystems, modules and their functions); identify all users of the information system; roles and powers of users in the information system (access rights), a list of information technologies that ensure the execution of business processes (IT infrastructure, software, including information protection tools, models and methods of user access to the information system, etc.). Directly in the area of information security, it is necessary to determine the current violator in the information system, determine the list of current information security threats (information security threat modeling), design and implement an information security system (information protection system), as well as carry out on a regular basis a qualitative assessment of the effectiveness of the information protection system.

One of the most important tasks from the above is the choice of a method of modeling threats to information security and attacks on information systems, which is what this article is dedicated to.

Based on the analysis of information security threat modeling methods, it can be concluded that all existing attack models have a number of common shortcomings. It is possible to improve the quality of the definition (simulation) of current information security threat models by determining the necessary and sufficient indicators and automating the process to eliminate hypothetical errors of experts.

Keywords: security models, attack models, information systems, information security threats.

Постановка проблеми

Інформаційна безпека в останні роки стає все більш значущою та важливою сферою національної безпеки багатьох розвинених країн світу та України зокрема. Розширення областей та сфер застосування інформаційних технологій значно розширює перспективи розвитку нових інформаційних загроз. Зарубіжні спеціальні служби розширюють свій вплив інформаційно-психологічного впливу, спрямованого на дестабілізацію внутрішньополітичної та соціальної ситуації в різних регіонах світу, що призводить до підриву суверенітету та порушення територіальної цілісності інших держав. Зростають масштаби комп'ютерної злочинності, насамперед у кредитно-фінансовій сфері. У сфері оборони країни, в галузі державної та громадської безпеки, в економічній сфері, в галузі науки, технологій та освіти, у галузі стратегічної стабільності та рівноправного стратегічного партнерства спостерігаються визначені на рівні держави стратегічні цілі для забезпечення ефективного стану інформаційної безпеки.

Одночасно зі зростанням та розвитком інформаційних технологій розвиваються тактики, техніки та способи реалізації проведення атак, розширюється інструментарій для порушення стану інформаційної безпеки. Змінити ситуацію можна шляхом розробки нових підходів до забезпечення інформаційної безпеки, які можуть надати надійний захист від сучасних загроз безпеці інформації [1,2].

Формулювання цілей статті

Для забезпечення інформаційної безпеки необхідно: визначити цілі та завдання інформаційної системи (ІС); дослідити бізнес-процеси в ІС (функціональні підсистеми, модулі та їх функції); визначити всіх користувачів ІС; ролі та повноваження користувачів в ІС (права доступу), перелік інформаційних технологій, що забезпечують виконання бізнес-процесів (IT-інфраструктура, програмне забезпечення, у тому числі засоби захисту інформації, моделі та методи доступу користувачів до ІС тощо). Безпосередньо у частині інформаційної безпеки необхідно визначити актуального порушника в ІС, визначити перелік актуальних загроз безпеці інформації (моделювання загроз безпеці інформації), спроектувати та впровадити систему інформаційної безпеки (систему захисту інформації), а також проводити на регулярній основі якісну оцінку ефективності системи захисту інформації.

Однією з найважливіших завдань із перелічених є вибір способу моделювання загроз інформаційної безпеки (ЗІБ) та атак на ІС, чому і присвячена дана стаття.

Огляд існуючих рішень

Статичні моделі ЗІБ включають опис виявлених, аналіз вихідної захищеності ІС, опис можливих порушників, оцінку реалізованості та небезпеки загроз, перелік актуальних ЗІБ в ІС. Розробляються експертами власників ІС з урахуванням призначення, умов та особливостей функціонування ІС.

Статичні моделі ЗІБ мають такі недоліки [3,4]:

- недоліки експертних методів (експертних оцінок);
- розробляються на поточний стан ІС, у зв'язку з цим виникають складності у постійній актуалізації таких моделей у конкретні певний момент часу – проблема підтримки в актуальному стані моделі ЗІБ;
- не враховують усі необхідні показники при визначенні переліку актуальних ЗІБ, а саме: зміни до моделі ризиків (негативних наслідків від реалізації ЗІБ); зміна умов експлуатації об'єктів впливу (елементи архітектури ІС, що обробляють інформацію, що захищається); версійність ПЗ; способи реалізації тактик і технік атак, які динамічно розвиваються;
- не раціональне використання безлічі відомих баз даних ЗІБ, уразливостей, тактик та технік атак (MITRE ATT&CK, CVE, CWE, OSVDB, NVD, Secunia тощо);
- як наслідок, неякісна оцінка ефективності захищеності інформації (рівня захищеності ІС).

Згідно ДСТУ [5], комп'ютерна атака – цілеспрямований несанкціонований вплив на інформацію, ресурс автоматизованої інформаційної системи або отримання несанкціонованого доступу до них із застосуванням програмних або програмно-апаратних засобів.

Під об'єктом атаки (мета атаки) розуміється елемент ІС.

Порушник – будь-яка особа, яка навмисно використовує вразливості технічних та нетехнічних заходів та засобів контролю та управління безпекою з метою захоплення або компрометації інформаційних систем та мереж, або зниження доступності ресурсів інформаційної системи та мережевих ресурсів для законних користувачів.

В даний час існує безліч моделей атак, методів та засобів моделювання атак. Основні моделі атак на ІС представлені на рисунку 1.

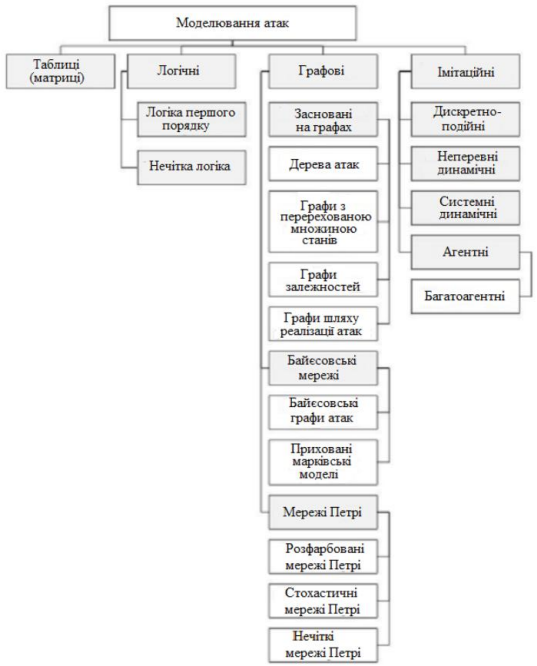


Рис. 1. Моделі атак на інформаційні системи

Переваги та недоліки основних моделей атак представлені у таблиці 1.

Таблиця 1

Переваги та недоліки моделей атак

№ п/п	Модель	Переваги	Недоліки
1.	**Табличні (Матричні)**	Найбільш прості	Складна при моделюванні циклічних атак, великої кількості зв'язків між інцидентами чи діями порушника.
2.	**Логічні**	Обробка інцидентів та використання мов уявлення знань про предметної галузі. Враховує випадки невизначеності вхідних даних про моделювані атаках	Використання спеціалізованого ПЗ, забезпечує механізми логічного висновку; Вимагає значних обчислювальних ресурсів
3.	**Графові**	Призначені для вирішення більшої кількості завдань, таких як «аналіз інцидентів, виявлення атак, оцінка ефективності захищеності інформації, визначення заходів щодо інформаційної безпеки, мінімізація ризиків та ресурсів для забезпечення інформаційної безпеки.	Масштабованість, пов'язана з формуванням графа для ІС з великою кількістю елементів
4.	**Графові на деревах атак**	Наочність, масштабованість, адаптованість, універсальність	Складні при моделюванні циклічних атак; Відсутність динамічного моделювання
5.	**Байєсовські графи**	Наочність, масштабованість, адаптованість, універсальність, враховує випадки невизначеності вхідних даних про атаки	Складні при моделюванні циклічних атак; Відсутність динамічного моделювання
6.	**Мережі Петрі**	Зручність моделювання динамічних та паралельних процесів, здатні відбивати ймовірнісні процеси, використання тимчасових параметрів, простота вивчення та використання, наявність великого кількості інструментальних засобів, можливість використання для аналізу різних аспектів інформаційної безпеки досліджуваної ІС	Нездатність описувати поведінку порушника та цілі атаки
7.	**Імітаційні**	Дозволяють моделювати поведінкові характеристики порушника та цілі атаки. Зручні для моделювання розподілених атак, мають широкий спектр інструментальних засобів	Вимагають великих обчислювальних ресурсів

Отже, можна зробити висновок, що усі існуючі моделі атак мають низку загальних недоліків, а саме:

- складність моделювання;

- вимагають обчислювальних ресурсів;
- вимагають залучення висококваліфікованих фахівців у галузі інформаційної безпеки;
- помилки експертних методів (експертних оцінок).

На підставі проведеного аналізу можна зробити висновок про необхідність удосконалення та розробки нових методик визначення актуальних ЗІБ (моделювання ЗІБ), що виключають існуючі недоліки.

Висновки

В даній статті проведено аналіз існуючих на сьогоднішній день способів моделювання ЗІБ.

На основі проведеного аналізу можна зробити висновки, що усі існуючі моделі атак мають низку загальних недоліків. Основними з них є:

1. При моделюванні ЗІБ не завжди існує можливість виявлення нових якісних характеристик.
2. Будь-яка модель ЗІБ мінімізує пояснення можливих явищ.
3. Як правило, необхідних даних для налаштування моделей не вистачає.
4. Недоліки експертних методів (експертних оцінок).
5. Моделі ЗІБ розробляються на поточний стан ІС, у зв'язку з цим виникають складнощі у постійній актуалізації таких моделей ЗІБ.
6. Не враховують усі необхідні показники щодо переліку актуальних ЗІБ.
7. Не раціональне використання безлічі відомих баз даних ЗІБ, уразливостей, тактик та технік атак (MITRE ATT&CK, CVE, CWE, OSVDB, NVD, Secunia і т.д.).
8. Як наслідок, неякісна оцінка рівня захищеності ІС

Підвищити якість визначення (моделювання) актуальних моделей ЗІБ можливо за рахунок визначення необхідних та достатніх показників та автоматизувати процес для виключення гіпотетичних помилок експертів.

Література

1. Laptiev, S. (2022). Удосконалений метод захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії. «Кібербезпека: освіта, наука, техніка», 4(16), 45–62. https://doi.org/10.28925/2663-4023.2022.16.4562.

2. Лєнков, С., Джулій, В., & Муляр, І. (2024). Метод оцінки ефективності безпеки конфіденційних даних розподіленої інформаційної системи. Pidvodni Tehnologii, 1(14), 18–34. https://doi.org/10.32347/uwt.2024.14.1201.

3. Mead, N., Shull, F., Vemuru, K., & Villadsen, O. A. Hybrid Threat Modeling Method. CMU/SEI-2018-TN-002. Software Engineering Institute, Carnegie Mellon University. 2018.

4. Khan, R.; McLaughlin, K.; Laverty, D.; & Sezer, Sakir. STRIDE-based Threat Modeling for Cyber-Physical Systems. In Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe. 2017. DOI 10.1109/ISGTEurope.2017.8260283.

5. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. – Введ. 01.01.98. К.: Держстандарт України, 1998. 12 с.

References

1. Laptiev, S. (2022). Udoskonalenyi metod zakhystu personalnykh danykh vid atak za dopomohoiu alhorytmiv sotsialnoi inzhenerii. «Kiberbezpeka: osvita, nauka, tekhnika», 4(16), 45–62. https://doi.org/10.28925/2663-4023.2022.16.4562.

2. Lienkov, S., Dzhulii, V., & Muliar, I. (2024). Metod otsinky efektyvnosti bezpeky konfidentsiinykh danykh rozpodilenoi informatsiinoi systemy. Pidvodni Tehnologii, 1(14), 18–34. https://doi.org/10.32347/uwt.2024.14.1201.

3. Mead, N., Shull, F., Vemuru, K., & Villadsen, O. A. Hybrid Threat Modeling Method. CMU/SEI-2018-TN-002. Software Engineering Institute, Carnegie Mellon University. 2018.

4. Khan, R.; McLaughlin, K.; Laverty, D.; & Sezer, Sakir. STRIDE-based Threat Modeling for Cyber-Physical Systems. In Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe. 2017. DOI 10.1109/ISGTEurope.2017.8260283.

5. DSTU 3396.2-97. Zakhyst informatsii. Tekhnichnyi zakhyst informatsii. Terminy ta vyznachennia. – Ved. 01.01.98. K.: Derzhstandart Ukrainy, 1998. 12

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Метод криптографічного захисту інформації в корпоративних чатах

Автор: Лакоценін Захар Євгенійович

Спеціальність: 125 – Кібербезпека та захист інформації

Освітня програма: освітньо-професійна

Науковий керівник: Тітова Віра Юріївна, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 96,5%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, Додаток В) кваліфікаційна робота, виконана за освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високою унікальністю тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Керівник роботи _____ Віра ТІТОВА

Гарант ОП _____ Віра ТІТОВА

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Лакоценіна Захара Євгеновича
ПІБ здобувача вищої освіти
Студента ФІТ, 2 курсу, групи КБЗІм-23-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а) та надаю свою згоду на обробку й збереження університетом моєї роботи в інституційному репозитарії Хмельницького національного університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-обчислювального комплексу StrikePlagiarism та/або програмнотехнічного засобу Anti-Plagiarism) і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення текстових збігів в роботах.

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

_____
дата

_____
підпис

Протокол аналізу звіту подібності експертом

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

Автор: Захар Лакоценін

Співавтор:

Назва: Метод криптографічного захисту інформації в корпоративних чатах

Експерт: Віра Тітова

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:3.5%

Коефіцієнт подібності 2:0.4%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2024-12-17 10:06:47.0

Після аналізу Звіту подібності констатую наступне:

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

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

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

Обгрунтування:

Дата

експерт

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «магістр»

Студент Лакоценін Захар Євгенійович
Тема: «Метод криптографічного захисту інформації в корпоративних чатах»
Галузь знань 12 «*Інформаційні технології*» Спеціальність 125 «*Кібербезпека та захист інформації*» Освітня програма «Кібербезпека та захист інформації»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «бакалавр»: кількість листів креслень ____; кількість сторінок записки 88;

1. Короткий зміст КР та прийнятих рішень У роботі виконано аналіз існуючих засобів захисту інформації в корпоративних комунікаціях, розроблено метод шифрування, адаптований для динамічного обміну повідомленнями, а також запропоновано алгоритми управління ключами для захисту корпоративних чатів. Проведено тестування розробленого методу, яке підтвердило його ефективність у протидії перехопленню та несанкціонованому доступу до даних.

2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека та захист інформації», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі було проведено аналіз існуючих методів криптографічного захисту інформації. У другому розділі проведено оцінку ефективності існуючих рішень для захисту корпоративних чатів та запропоновано власний метод криптографічного захисту. У третьому розділі представлено реалізацію та тестування запропонованого методу. У четвертому розділі метод впроваджено та оцінено його ефективність.

4. Позитивні сторони кваліфікаційної роботи позитивною стороною є розробка ефективного методу криптографічного захисту інформації, що передається через корпоративні чати. Запропонований метод забезпечує високий рівень конфіденційності, цілісності та автентичності повідомлень, а також гарантує належну автентифікацію користувачів. Впровадження таких технологій дозволить значно знизити ризики, пов'язані з витоком конфіденційної інформації, та підвищити загальний рівень безпеки корпоративних чатів. Результати роботи можуть бути впроваджені у корпоративних середовищах для покращення захисту інформації, що передається у внутрішніх чатах компаній, а також у сфері хмарних технологій і цифрових комунікацій.

5. Негативні сторони кваліфікаційної роботи: _-.

6. Оцінка графічного оформлення та пояснювальної записки роботи.

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. У пояснювальній записці багато наглядних пояснень. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі.

8. Інші зауваження -

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «відмінно».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, д.т.н., професор Мартинюк Валерій Володимирович

« 13 » грудня 2024 . _____ (підпис)