

УНІВЕРСИТЕТ ІМЕНІ АЛЬФРЕДА НОБЕЛЯ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему

*«Застосування стеганографії у хмарній
безпеці»*

Виконала: здобувач 2 курсу, групи КН-22м

Спеціальності 122 Комп'ютерні науки

Войтенко Анастасія Олександрівна

Керівник: Барташевська Ю.М., к.е.н., доцент

м. Дніпро
2024

Тематика кваліфікаційної роботи стосується практики використання програмного забезпечення з алгоритмами стеганографії для додаткової системи захисту. У роботі представлені сучасні методи передачі даних у загальнодоступній системі зв'язку є незахищеною через перехоплення та неналежне маніпулювання з боку перехоплювача. Кваліфікаційна робота складається з вступу, літературного огляду, теоретичної частини, розділу, присвяченого розробці програмного забезпечення, експериментального дослідження та висновків. Використання алгоритмів стеганографії для додаткового захисту в системах зв'язку має на меті забезпечити високий рівень конфіденційності та недоступності для недозволених осіб. Результати досліджень можуть мати важливе значення для розробки та удосконалення методів захисту інформації в умовах високотехнологічного світу.

На основі проведеного дослідження була розроблена програма для стеганографії даних.

Ключові слова: хмарні технології, стеганографія, криптографія, Cover file, Stego file, key.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	8
ВСТУП.....	9
РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ БЕЗПЕКИ ХМАНИХ ОБЧИСЛЕНЬ	11
1.1. Історія хмарних обчислень	11
1.2. Хмарні обчислення сьогодні.....	12
1.3. Хмарна архітектура.....	13
1.4. Моделі хмарного розгортання.....	15
1.5. Хмарна безпека	16
РОЗДІЛ 2 ОСОБЛИВОСТІ СТЕГANOГРАФІЇ	21
2.1. Визначення стеганографії	21
2.2. Різниця між стеганографією та криптографією	22
2.3. Види техніки стеганографії	23
2.4. Вимоги стеганографії	25
2.5. Алгоритми, що використовуються для стеганографії.....	28
РОЗДІЛ 3 ПРАКТИЧНА ЧАСТИНА.....	30
3.1. Домен.....	30
3.2. Створення зашифрованого тексту. Методи шифрування	30
3.3. Алгоритм шифрування.....	31
3.4. Вбудовування.....	32
3.5. Завдання та процедури, що пропонуються.....	32
3.6. Техніко-економічний аналіз	33
3.6.1. Технічна можливість	33
3.6.2. Ризик розвитку	33
3.6.3. Наявність ресурсів	33
3.7. Код алгоритму генерування ключа.....	34
3.8. Шифрування повідомлення.....	35
3.9. Розгортання програмного забезпечення для шифрування.....	36
3.10. Опис коду тіла та інтерфейсу програми.....	42

3.11 Розгортання програмного забезпечення для шифрування.....	44
3.12 Шифрування.....	45
3.13 Розшифровка.....	48
3.14 Експериментальний аналіз	50
3.15 Обмеження.....	51
ВИСНОВКИ.....	53
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	55
ДОДАТКИ.....	58