**ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**
**ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ**
**КАФЕДРА ПРОГРАМНИХ ЗАСОБІВ І ТЕХНОЛОГІЙ**

**Пояснювальна записка**

до кваліфікаційної роботи магістра

на тему:

# «ДОСЛІДЖЕННЯ ЗАСОБІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ФАЙЛІВ»

Виконав: студент *2* курсу, групи *6ПР3*
спеціальності 121 «Інженерія програмного забезпечення»
*Созанський С.В.*
(прізвище та ініціали)
Керівник: *Хохлов В.А.*
(прізвище та ініціали)
Рецензент *М.О.Вороненко*
(прізвище та ініціали)

Херсон – 2024 р.

Факультет *Інформаційних технологій та дизайну*
Кафедра *Програмних засобів і технологій*
Освітньо-кваліфікаційний рівень *магістр*
Галузі знань *12 «Інформаційні технології»*
Спеціальність *121 «Інженерія програмного забезпечення»*
Освітньо-професійної програми *«Програмна інженерія»/«Програмне забезпечення систем»*

**ЗАТВЕРДЖУЮ**
Завідувач кафедри ПЗіТ,
доцент
_____О.Є.Огнєва
«____» _____ 2024 року

**ЗАВДАННЯ**
**НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ**
*Созанського Сергія Вікторовича*
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження засобів криптографічного захисту файлів*

керівник роботи *Хохлов Вадим Анатолійович, к.т.н., доцент*,
( прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом ХНТУ від «*23*» *вересня* 20*24* року № *484-с*.
2. Строк подання студентом роботи *05.12.2024*
3. Вихідні дані до роботи *літературні та періодичні джерела, матеріали передипломної практики*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) *аналіз предметної галузі, аналіз аналогічних проектів; розробка технічного завдання; розробка архітектури додатку; розробка додатку, оптимізація та тестування.*

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
*20 рисунків*

6. Консультанти розділів роботи

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

7. Дата видачі завдання *25.09.2024*

## КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів дипломного роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Аналіз предметної галузі | 25.09.2024-09.10.2024 | |
| 2 | Розробка технічного завдання | 10.10.2024-22.10.2024 | |
| 3 | Розробка архітектури додатку | 23.10.2024-03.11.2024 | |
| 4 | Розробка, оптимізація та тестування додатку | 04.11.2024-18.11.2024 | |
| 5 | Написання пояснювальної записки до дипломного проекту | 19.11.2024-05.12.2024 | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Студент** _____ *Созанський С.В*
( підпис ) (прізвище та ініціали)

**Керівник роботи** _____ *Хохлов В.А.*
( підпис ) (прізвище та ініціали)

# АНОТАЦІЯ

Кваліфікаційна робота магістра містить такі структурні частини: вступ, три розділи, висновок та список посилань.

Перший розділ «Дослідження та аналіз предметної області» складається з чотирьох частин: «Аналітичний огляд джерел», «Аналіз поточної ситуації», «Порівняння існуючих рішень» та «Недоліки і можливості для вдосконалення в криптографії». У цьому розділі аналізується предметна область дослідження. Досліджуються існуючі рішення, приводяться приклади існуючих методів і здійснюється огляд прогалин і можливостей для вдосконалення.

У другому розділі «Основи методології розробки додатку» розміщено наступні підрозділи: «Архітектура і дизайн додатку», «Використані інструменти і технології», «Опис структури проекту», «Декомпозиція програмного додатку» та «Процес тестування та налагодження». У цьому розділі розглянуто технології, методи, моделі, алгоритми криптографічного захисту даних, описано процес тестування та налагодження додатку.

У третьому розділі «Розробка та застосування продукту» розміщено наступні підрозділи: «Результати розробки програмного продукту», «Послідовність роботи користувача з додатком», «Аналіз результатів застосування продукту» та «Перспективи подальшого розвитку додатку». У цьому розділі наведено реалізацію програмного продукту. Приведено роботу кожного модуля та викладені перспективи подальшого розвитку додатку.

# ABSTRACT

The master's thesis contains the following structural parts: introduction, three chapters, conclusion, and a list of references.

The first chapter “Research and analysis of the subject area” consists of four parts: “Analytical Review of Sources”, ‘Analysis of the Current Situation’, ‘Comparison of Existing Solutions’, and ‘Shortcomings and Opportunities for Improvement in Cryptography’. This section analyzes the subject area of the study. Existing solutions are studied, examples of existing methods are given, and gaps and opportunities for improvement are reviewed.

The second section, “Fundamentals of Application Development Methodology,” contains the following subsections: “Application Architecture and Design”, ‘Tools and Technologies Used’, ‘Project Structure Description’, ‘Application Decomposition’, and ‘Testing and Debugging Process’. This section describes technologies, methods, models, and algorithms for cryptographic data protection, and describes the process of testing and debugging the application.

The third section “Product Development and Application” contains the following subsections: “Results of the software product development”, ‘Sequence of user work with the application’, ‘Analysis of the results of the product application’ and ‘Prospects for further development of the application’. This section describes the implementation of the software product. The work of each module is described and the prospects for further development of the application are outlined.

# РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи на тему «Дослідження засобів криптографічного захисту файлів» містить: 90 сторінок, 20 рисунків, 2 додатки, 17 літературних джерел.

**Об'єкт дослідження** – процеси шифрування та дешифрування інформації, що використовують криптографічні методи для забезпечення безпеки даних.

**Предмет дослідження** – методи та програмні засоби для захисту даних, їх ефективність і швидкість при обробці файлів різного обсягу, а також параметри, що впливають на продуктивність та безпеку під час шифрування.

**Мета кваліфікаційної роботи** – створення програмного додатку для шифрування та дешифрування файлів і папок за допомогою алгоритмів AES і Blowfish.

**Методи дослідження** – теоретичний аналіз наукових праць та існуючих криптографічних алгоритмів, розробка додатку мовою Python з використанням бібліотеки PyCryptodome, порівняльний аналіз для оцінки результатів експериментів.

**Наукова новизна роботи** полягає в розробці оптимізованого програмного рішення для шифрування/дешифрування папок і файлів з використання мови програмування Python.

**Об’єктом розробки** є програмне рішення для захисту файлів і папок за допомогою сучасних криптографічних алгоритмів шифрування, реалізоване на Python з використанням PySide6 для інтерфейсу та модулів криптографії для захисту даних. Методи розробки включають аналіз вимог до системи, проектування, реалізацію алгоритмів шифрування, розробку графічного інтерфейсу користувача, тестування та налагодження. Архітектура програми побудована з урахуванням безпеки, модульності та розширюваності, а

інтерфейс орієнтований на зручність та простоту використання для кінцевого користувача.

Результатом кваліфікаційної роботи є повнофункціональне програмне забезпечення для шифрування файлів та папок, яке надає користувачам можливість вибору алгоритмів AES і Blowfish, встановлення пароля для захисту даних та автоматичне видалення оригінальних файлів після шифрування. Новизна цієї роботи полягає в інтеграції надійних алгоритмів шифрування та орієнтованого на користувача інтерфейсу для забезпечення простоти і доступності процесу шифрування.

**Ключові слова:** ПРОГРАМНИЙ ДОДАТОК, КРИПТОЗАХИСТ, АЛГОРИТМИ ШИФРУВАННЯ, PYTHON, PYCRYPTODOME, PYSIDE, AES, BLOWFISH.

ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IT - інформаційні технології

ПЗ – програмне забезпечення

ПП - програмний продукт

AES - Advanced Encryption Standard

GUI – Graphical User Interface

DRY - Don't Repeat Yourself

KISS - Keep It Simple, Stupid

YAGNI - You Aren’t Gonna Need It

# ВСТУП

Сучасне інформаційне суспільство все більше покладається на цифрові дані, що зумовлює актуальність питання забезпечення безпеки інформації. З розвитком IT і зростанням обсягу персональних та комерційних даних питання конфіденційності, цілісності та доступності інформації набувають першочергового значення. У випадку витоку чи несанкціонованого доступу до конфіденційних даних існує ризик суттєвих фінансових та репутаційних втрат. Тому особливо важливо впроваджувати ефективні інструменти для захисту інформації, одним із яких є криптографія, що дозволяє шифрувати дані, забезпечуючи їх недоступність для сторонніх осіб.

Метою даної кваліфікаційної роботи є розробка програмного рішення для надійного шифрування файлів та папок із використанням сучасних алгоритмів шифрування, таких як AES і Blowfish. Це рішення, реалізоване на Python з використанням PySide6 для зручного та інтуїтивного графічного інтерфейсу, надасть користувачам можливість захищати власні дані за допомогою потужного інструменту з вибором методів шифрування, встановленням пароля та можливістю видалення оригінальних файлів після шифрування.

Актуальність даної кваліфікаційної роботи полягає в необхідності розробки програмного забезпечення, яке дозволить користувачам легко захищати свої файли без глибоких технічних знань. Сучасні загрози кібербезпеки вимагають інноваційних підходів до захисту даних, особливо в умовах зростаючих кібератак, які все частіше спрямовані на особисту інформацію та комерційні дані. Таким чином, автоматизоване рішення для шифрування файлів є важливим інструментом для будь-якого користувача, який хоче захистити свої дані в сучасному цифровому світі.

Для досягнення цілей цієї кваліфікаційної роботи буде використано

системний підхід, який охоплює різні етапи розробки ПЗ. Процес розпочнеться з ретельного аналізу потреб користувачів у надійних засобах шифрування, існуючих рішень у галузі криптографічного захисту та вивчення сучасних алгоритмів шифрування для формування вимог до функціональних можливостей програми.

Наступним етапом буде проектування архітектури програмного забезпечення з урахуванням вимог масштабованості та розширюваності, щоб забезпечити зручність і легкість у використанні, а також з можливістю інтеграції нових алгоритмів шифрування в майбутньому. Етап реалізації включатиме безпосереднє програмування додатку на Python, розробку графічного інтерфейсу з PySide6 для максимальної зручності взаємодії з користувачем, а також створення і тестування алгоритмів шифрування.

Успішне завершення цієї кваліфікаційної роботи продемонструє ефективність застосування сучасних криптографічних технологій та орієнтованого на користувача дизайну для розробки інструменту захисту даних, який надасть користувачам можливість легко й надійно зберігати конфіденційність власної інформації у світі, що стає все більш цифровим.