

Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра інформаційних технологій та систем електронних комунікацій

«Допущено до захисту»
Начальник кафедри інформаційних
технологій та систем електронних
комунікацій

Олександр ПРИДАТКО
“ ___ ” _____ 20__ року

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему: «Розроблення Full-stack рішень для системи зберігання та кодування
конфіденційних даних»

Виконав:

здобувач VI курсу, групи КН-61м
спеціальності 122 «Комп'ютерні науки»
(шифр і назва спеціальності)

Роман МИСЬКО

(ім'я та прізвище)

Керівник Юрій БОРЗОВ

(ім'я та прізвище)

Рецензент _____

(ім'я та прізвище)

Львів 2024 рік

Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту

Кафедра інформаційних технологій та систем електронних комунікацій

Освітній ступінь магістр

Спеціальність 122 “Комп’ютерні науки”

Освітня програма Комп’ютерні науки

ЗАТВЕРДЖУЮ

Начальник кафедри інформаційних
технологій та систем електронних
комунікацій

Олександр ПРИДАТКО

“ ___ ” _____ 20__ року

ЗАВДАННЯ

на кваліфікаційну роботу

Здобувач Роман МИСЬКО

(ім'я, прізвище)

1. Тема “Розроблення Full-stack рішень для системи зберігання та кодування
конфіденційних даних”

керівник роботи Юрій БОРЗОВ, к.т.н., доцент

(ім'я, прізвище, науковий ступінь, вчене звання)

затверджені наказом ЛДУ БЖД від “ ___ ” _____ 20__ року № _____

2. Термін подання здобувачем роботи _____

3. Початкові дані до роботи

1. Full Stack Web Development: The Comprehensive Guide. -2023 - Philip Ackermann
2. Web Development with Django: Learn to build modern web applications with a Python-based framework. - 2021 – Ben Shaw, Saurabh Badhwar, Andrew Bird, Bharath Chandra K. S., Chris Guest
3. Learning Web App Development: Build Quickly with Proven JavaScript Techniques 1st Edition. - 2014 - Semmy Purewal
4. A Byte of Python. - 2013 - Swaroop C. H.
5. Build a Website with Django 3. - 2018 - Nigel George

4. Зміст кваліфікаційної роботи/проекту (перелік питань, які потрібно розробити)

Вступ

Розділ 1. Аналіз існуючих рішень

Розділ 2. Технології реалізації системи зберігання та кодування конфіденційних даних

Розділ 3. Розробка системи зберігання та кодування конфіденційних даних

Розділ 4. Реалізація системи зберігання та кодування конфіденційних даних системи

Висновки

Список використаних джерел

Додатки

1. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

2. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз існуючих рішень		
2	Технології реалізації системи зберігання та кодування конфіденційних даних		
3	Розробка системи зберігання та кодування конфіденційних даних		
4	Реалізація системи зберігання та кодування конфіденційних даних системи		

Здобувач

_____ (підпис)

Роман МИСЬКО

(ім'я та прізвище)

Керівник роботи

_____ (підпис)

Юрій БОРЗОВ

(ім'я та прізвище)

АНОТАЦІЯ

Роман МИСЬКО. «Розроблення Full-stack рішень для системи зберігання та кодування конфіденційних даних». Кваліфікаційна робота за спеціальністю 122 «Компютерні науки» складається з текстової частини, що містить 4 розділи, 60 сторінок і містить 20 ілюстрацій та 14 джерел.

Дана кваліфікаційна робота присвячена розробці та реалізації Full-stack системи на базі фреймворку Django, спрямованої на забезпечення безпеки та конфіденційності зберіганої інформації та взаємодії з нею. Основною метою дослідження є застосування алгоритмів шифрування кешування, Advanced Encryption Standard (AES) та Rivest-Shamir-Adleman (RSA), та хешування для ефективного та надійного зберігання конфіденційної інформації.

Розроблена система на платформі Django використовує високопродуктивні алгоритми шифрування для захисту даних під час їхнього зберігання. В рамках роботи реалізовані механізми взаємодії користувача з системою реєстрації та логування в систему.

ABSTRACT

Roman MYSKO. "Development of Full-stack Solutions for Confidential Data Storage and Encryption". Qualification work in specialty 122 "Computer science" consists of a textual part that includes 4 chapters, 60 pages, including 20 illustrations, and 12 sources.

This master's thesis is dedicated to the development and implementation of a Full-stack system based on the Django framework aimed at ensuring the security and confidentiality of stored information and its interaction. The main goal of the research is the application of encryption algorithms for caching, Advanced Encryption Standard (AES), and Rivest-Shamir-Adleman (RSA), as well as hashing for efficient and reliable storage of confidential information.

The developed system on the Django platform utilizes high-performance encryption algorithms to protect data during storage. Mechanisms for user interaction with the registration and login system have been implemented within the work.

ЗМІСТ

Вступ.....	7
Розділ 1. Аналіз існуючих рішень.....	10
1.1 Хешування та SSO.....	10
1.2 Алгоритми шифрування AES (Advanced Encryption Standard) та RSA (Rivest, Shamir, Adleman).....	16
1.3 Full-Stack розробка.....	23
1.4 Постановка завдання.....	31
Розділ 2. Технології реалізації системи зберігання та кодування конфіденційних даних.....	33
2.1 Django.....	33
2.2 Зв'язок Django із базами даних, SQLite.....	35
2.3 Мова програмування Python	42
Розділ 3. Розробка системи зберігання та кодування конфіденційних даних.....	46
3.1 Архітектура системи.....	46
3.2 Розробка та алгоритм системи.....	50
Розділ 4. Реалізація системи зберігання та кодування конфіденційних даних.....	53
4.1 Система реєстрації.....	53
4.2 Система логіну.....	55
4.3 Домашня сторінка.....	55
4.4 Обробка конфіденційних даних.....	56
Висновок.....	58
Список використаних джерел.....	59

ВСТУП

Сучасні технології інформаційної безпеки набувають все більшого значення у світі, де обмін та зберігання конфіденційної інформації стає невід'ємною частиною багатьох аспектів життя. Забезпечення надійності, цілісності та конфіденційності даних вимагає впровадження ефективних систем зберігання та управління інформацією.

Повноцінний розробник - це інженер програмного забезпечення, який володіє як інтерфейсом користувача, так і основною інфраструктурою програми. Вони використовують свої численні таланти для створення інтуїтивно зрозумілого інтерфейсу для користувачів. Вони також добре розуміються на управлінні базами даних, адмініструванні сервера та дизайні інтерфейсу користувача.

Крім того, розробнику повного стеку не обов'язково бути експертом у кожній галузі веб-розробки.

В глобальному розумінні під стеком (Stack) розуміють типовий набір програм та технологій, які дозволяють досягти заданого результату. Наприклад, програмний стек смартфона включає ОС, базові та додаткові застосунки для телефону, браузері. Частіше говорять про веб стек, мобільний стек та стек нативних застосунків (native application stack).

Існує низка мов програмування та фреймворків для створення веб - додатка. Раніше не існувало мов програмування, які могли б виконувати як фронтенд, так і бекенд розробку додатку. LAMP stack: Linux, Apache, MySQL і PHP раніше були стандартом для повностекової веб-розробки. PHP в основному використовувався для бекенду, а HTML, CSS і JavaScript були основними стеками для розробки фронтенду, в той час як MySQL використовувався для баз даних. Apache виступає як веб-сервер в операційній системі Linux у стеку LAMP. Однак для розробки веб - додатку з використанням стека LAMP розробникам потрібно було вивчити кілька мов, всі з яких використовують різний синтаксис і мають різну природу. Крім того, з появою Node.js в якості

серверної платформи JavaScript зміг забезпечити розробку повностекового програмного забезпечення в рамках єдиної мови програмування.

Незважаючи на те, що Node.js є найбільш поширеною технологією для розробки бекенд-систем, існує безліч фреймворків, таких як Angular, React, Vue.js або Knockout.js, а також шаблонні двигуни (шаблонизатор), такі як EJS, Handlebars або Pug.

Дана кваліфікаційна робота присвячена розробці та впровадженню фул-стак системи, побудованої на фреймворку Django, яка має на меті забезпечити безпеку та конфіденційність інформації, а також надати ефективний механізм реєстрації та логування користувачів. Особлива увага приділяється застосуванню передових алгоритмів шифрування, таких як Advanced Encryption Standard (AES) та Rivest-Shamir-Adleman (RSA), а також використанню механізмів кешування та хешування для забезпечення ефективного зберігання конфіденційної інформації.

В роботі буде розглянуто теоретичний аспект застосування алгоритмів шифрування та кешування для забезпечення безпеки даних. Детально буде вивчено механізм роботи алгоритмів AES та RSA, а також надано огляд того, як закодовані дані виглядають у базі даних під час їх зберігання.

Окрім теоретичної частини, у роботі буде представлена розроблена система, що використовує високопродуктивні алгоритми шифрування та забезпечує зручний і безпечний доступ користувачів до системи через механізми реєстрації та логування. Також буде продемонстровано, як виглядає закодована інформація в базі даних, підкреслюючи надійність та ефективність розробленої системи.

Ця робота відкриває нові можливості для впровадження безпечних систем зберігання інформації у різних галузях, де важливо зберігати конфіденційні дані в сучасному цифровому світі.

У контексті даної кваліфікаційної роботи передбачається можливість локального запуску розробленої системи для подальшого тестування та експериментів. Локальний запуск системи передбачає використання

середовища для розробки та випробувань без необхідності встановлення системи на зовнішньому сервері чи хмарному середовищі.

ВИСНОВОК

Під час виконання кваліфікаційної роботи розроблено систему зберігання та кодування конфіденційних даних на базі Python Django. Проаналізовані та імплементовані системи зберігання конфіденційних даних за допомогою систем кодування даних. Серед алгоритмів шифрування було застосовано хешування, AES та RSA. Розроблено сторінки реєстрації, логування та сторінку авторизованого користувача. Для зберігання даних та взаємодія з ними використано базу даних SQL Lite. Наведені результати роботи та алгоритми дій програми після запуску через localhost.

В процесі виконання роботи:

- проведено аналіз алгоритмів шифрування, кешування та основ Full-Stack розробки систем;
- здійснено вибір технологій реалізації та програмних засобів розроблення;
- розроблено систему на платформі Django, яка використовує алгоритми шифрування для забезпечення безпеки даних;
- реалізовано механізми реєстрації та логування користувачів для забезпечення безпечного доступу до системи та взаємодії з базою даних;
- проведено експериментальне тестування розробленої системи для оцінки ефективності та безпеки.

Розроблені засоби запобігання виникнення виключних ситуацій для недопущення втрати працездатності програми при помилкових ситуаціях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- 1) [Електронний ресурс]. -
<https://www.coursera.org/articles/full-stack-developer>
- 2) [Електронний ресурс]. -<https://en.wikipedia.org/wiki/SQLite>
- 3) [Електронний ресурс]. -<https://vidalinternational.in/full-stack-development-relationship-between-frontend-and-backend/#:~:text=The%20backend%20handles%20data%20processing,this%20data%20to%20the%20user.>
- 4) [Електронний ресурс]. -<https://www.stackhawk.com/blog/sql-injection-prevention-django/>
- 5) [Електронний ресурс]. -
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
- 6) [Електронний ресурс]. -[https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))
- 7) [Електронний ресурс]. -
[https://en.wikipedia.org/wiki/Django_\(web_framework\)](https://en.wikipedia.org/wiki/Django_(web_framework))
- 8) Full Stack Web Development: The Comprehensive Guide. -2023 - Philip Ackermann
- 9) Web Development with Django: Learn to build modern web applications with a Python-based framework. -2021 – Ben Shaw, Saurabh Badhwar, Andrew Bird, Bharath Chandra K. S., Chris Guest
- 10) Learning Web App Development: Build Quickly with Proven JavaScript Techniques 1st Edition. -2014 - Semmy Purewal
- 11) A Byte of Python. -2013 - Swaroop C. H.
- 12) Build a Website with Django 3. -2018 - Nigel George
- 13) Ковальчук А., Пелешко Д., Борзов Ю. Модифікація алгоритму RSA: шифрування та дешифрування за одним рядком матриці зображення, Науковий вісник НЛТУ України. Збірник науково-технічних праць. Львів.,– 2012. – Вип. 22.6., с.336-340

14) Рак Т.Є., Борзов Ю.О. Лінійні форми з елементами алгоритму RSA і додаткове зашумлення в захисті півтонових зображень. Науковий вісник НЛТУ України Збірник науково-технічних праць. Львів., – 2015. – Вип. 25.3., с.377-382

15) [Електронний ресурс]. - <https://aws.amazon.com/compare/the-difference-between-soap-rest/#:~:text=SOAP%20and%20REST%20are%20two%20different%20approaches%20to%20API%20design,exchange%20data%20in%20multiple%20formats>.

16) [Електронний ресурс]. - <https://blog.hubspot.com/website/rest-vs-soap>

17) Principles of Web API Design: Delivering Value with APIs and Microservices. – 2021.- James Higginbotham.