МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
КОРАБЛЕБУДУВАННЯ ІМЕНІ АДМІРАЛА МАКАРОВА
МИКОЛАЇВСЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ
ДЕПАРТАМЕНТ ОСВІТИ І НАУКИ
МИКОЛАЇВСЬКОЇ ОБЛАСНОЇ ДЕРЖАВНОЇ АДМІНІСТРАЦІЇ

ІННОВАЦІЇ В СУДНОБУДУВАННІ ТА ОКЕАНОТЕХНІЦІ

XVI Міжнародна науково-технічна конференція

МАТЕРІАЛИ

25–26 вересня 2025 рік

Національний університет кораблебудування
імені адмірала Макарова
просп. Героїв України, 9

ВИДАВНИЦТВО
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
КОРАБЛЕБУДУВАННЯ
ІМ. АДМІРАЛА МАКАРОВА
2025

Admiral Makarov National University of Shipbuilding, Mykolayiv, Ukraine.

Abstract. The development and implementation of an information subsystem for a bus station are considered, aimed at automating core processes from route planning to ticket sales. The system's conceptual, logical, and physical models are presented, along with a mathematical model for tracking the number of passengers and routes. The use of modern IT solutions increases the efficiency of passenger service, reduces time expenditures, and improves the overall service quality.

Keywords: information system, bus station, web application, mathematical model, ticket booking.

УДК 004.421:004.412.4

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ЗАХИСТУ КОРПОРАТИВНИХ ДАНИХ У ВІДКРИТИХ СИСТЕМАХ

Гайдаєнко О.В.
кандидат технічних наук,
доцент кафедри інформаційних управляючих систем та технологій
Національний університет кораблебудування імені адмірала Макарова,
м. Миколаїв, Україна, oksana.gaidaienko@nuos.edu.ua
Гайдучок У.Т.
студент групи 5141МЗ
Національний університет кораблебудування імені адмірала Макарова,
м. Миколаїв, Україна, ulyanag8008@gmail.com

Анотація. Робота присвячена дослідженню методів захисту корпоративних даних у відкритих системах та розробці інформаційної підсистеми, що забезпечує конфіденційність, цілісність та безпеку інформації.

Ключові слова: захист корпоративних даних, інформаційна система, шифрування, конфіденційність, цілісність, доступність, користувач.

Вступна частина. Технології захисту корпоративних даних стають важливими елементами стратегій безпеки підприємств, тому дослідження сучасних методів і підходів до захисту даних у відкритих системах є актуальним і необхідним для забезпечення стабільності та безпеки інформаційних ресурсів.

Мета роботи. Дослідження сучасних технологій захисту корпоративних даних у відкритих системах, а також розробка рекомендацій щодо їх ефективного впровадження для забезпечення безпеки інформаційних ресурсів організацій.

Основна частина. Інформаційна підсистема захисту корпоративних даних реалізована на основі технологій Flask (Python) для серверної частини та JavaScript (Axios) – для клієнтської частини. Взаємодія відбувається через REST API із використанням JWT (JSON

Web Token) для аутентифікації. Система побудована відповідно до принципів безпеки: конфіденційність, цілісність, доступність.

Модулі системи.

- ✓ Аутентифікація користувачів: користувач проходить перевірку особи за допомогою JWT.
- ✓ Шифрування/дешифрування: реалізовано за допомогою AES у режимі Fernet.
- ✓ Зберігання паролів: хешуються алгоритмом Scrypt із додаванням salt.
- ✓ Контроль доступу: кожен користувач має рівень доступу; усі дії логуються.

Засоби реалізації.

- ✓ Мова програмування: Python 3.13.
- ✓ Фреймворк: Flask.
- ✓ База даних: SQLite (можлива заміна на PostgreSQL).
- ✓ Клієнтська частина: HTML/JS + Axios.
- ✓ Криптобібліотеки: cryptography, hashlib, scrypt, jwt.

Механізми захисту даних.

- ✓ Шифрування (AES-Fernet):

Формула шифрування:

$C = E_к(P)$ – шифрування відкритого тексту P ключем K, $P = D_к(C)$ – розшифрування.

- ✓ Хешування

(Scrypt):

H = Scrypt(password, salt, N, r, p) – створення хешу з врахуванням унікального salt і складних параметрів (N, r, p).

Аудит та логування: Лог-функція L = (U, A, T) де U – користувач, A – дія, T – час.

Математичне забезпечення.

- ✓ В основі розробки – сучасні криптографічні методи:
- ✓ AES – симетричне блочне шифрування.
- ✓ Scrypt – стійке до перебору хешування.
- ✓ JWT – безпечна передача токенів.
- ✓ Timestamp логування – забезпечує повний аудит користувацьких дій.

Запропоновані рішення дозволяють гарантувати стійкість до атак типу brute force, захист від компрометації паролів, а також контроль доступу на основі ролей.

Висновок. У результаті дослідження сучасних технологій захисту корпоративних даних у відкритих системах було проаналізовано ключові методи забезпечення інформаційної безпеки, такі як шифрування, багатофакторна автентифікація, засоби контролю доступу, системи виявлення вторгнень, а також засоби резервного копіювання та моніторингу.

На основі аналізу надано практичні рекомендації щодо ефективного впровадження зазначених технологій з урахуванням потреб та інфраструктури конкретної організації. Реалізація таких заходів дозволяє значно знизити ризики несанкціонованого доступу, втрати чи компрометації даних та забезпечити належний рівень захисту корпоративної інформації у відкритих системах.

Література

[1] Офіційна документація Flask: https://flask.palletsprojects.com/en/latest/

[2] Офіційна документація Flask-SQLAlchemy: https://flask-sqlalchemy.palletsprojects.com/

[3] Офіційна документація Flask-Login: https://flask-login.readthedocs.io/en/latest/

[4] Офіційна документація SQLite: https://www.sqlite.org/docs.html

Офіційна документація бібліотеки Cryptography (AES, Fernet): https://cryptography.io/en/latest/

[5] M. Grinberg. *Flask Web Development: Developing Web Applications with Python.* – O'Reilly Media, 2018.

[6] A. Sweigart. *Beyond the Basic Stuff with Python: Best Practices for Writing Clean Code.* – No Starch Press, 2020.

[7] C. Althoff. *The Self-Taught Programmer: The Definitive Guide to Programming Professionally.* – self-published, 2017.

[8] M. Lutz. *Learning Python.* – O'Reilly Media, 2013.

[9] N. Ferguson, B. Schneier, T. Kohno. *Cryptography Engineering: Design Principles and Practical Applications.* – Wiley Publishing, 2010.

[10] Flask Tutorials: https://realpython.com/tutorials/flask/

[11] Python Cryptography Guide: https://realpython.com/python-encryption/

RESEARCH IN CORPORATE DATA PROTECTION TECHNOLOGIES IN OPEN SYSTEMS

Haidaienko Oksana, Haiduchok Uliana

Admiral Makarov National University of Shipbuilding, Mykolayiv, Ukraine.

Abstract. The work is devoted to the study of methods for protecting corporate data in open systems and the development of an information subsystem that ensures confidentiality, integrity and security of information.

Keywords: corporate data protection, information system, encryption, confidentiality, integrity, availability, user.

СЕКЦІЯ 7. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА УПРАВЛІННЯ ПРОЕКТАМИ