АНОТАЦІЯ

Ольга КОБИЛКІНА. «Використання сучасних криптографічних методів для захисту персональних даних в умовах воєнного стану». Кваліфікаційна робота за спеціальністю 122 “Комп’ютерні науки” складається з текстової частини, що містить 3 розділи, 78 сторінок, 47 рисунки, 3 таблиці, 33 джерела і 3 додатки.

Дана кваліфікаційна робота присвячена дослідженню використання сучасних криптографічних методів в умовах воєнного стану та їхню ефективність у забезпеченні конфіденційності інформації. Метою роботи є аналіз сучасних криптографічних алгоритмів, оцінка їх ефективності та розробка безпечного менеджера паролів, що забезпечує надійне зберігання та управління аутентифікаційними даними.

Об’єктом дослідження є методи та технології захисту персональних даних у цифровому середовищі.

Предметом дослідження є програмні засоби та алгоритми, що використовуються для безпечного зберігання та управління паролями.

Методи дослідження включають аналіз наукових джерел, порівняння існуючих менеджерів паролів (Bitwarden, LastPass, 1Password, KeePass, NordPass), а також моделювання архітектури системи захисту персональних даних з використанням UML-діаграм. У практичній частині реалізовано механізми генерації та шифрування паролів із застосуванням алгоритму AES-256.

Основні результати роботи включають розробку програмного прототипу менеджера паролів, що забезпечує захищене зберігання даних і може бути інтегрований у корпоративні та особисті інформаційні системи. Отримані результати можуть бути використані для створення безпечних рішень з управління аутентифікаційними даними.

КЛЮЧОВІ СЛОВА: КРИПТОГРАФІЯ, МЕНЕДЖЕР ПАРОЛІВ, ІНФОРМАЦІЙНА БЕЗПЕКА, ШИФРУВАННЯ, АУТЕНТИФІКАЦІЯ, ЗАХИСТ ДАНИХ.

ABSTRACT

Olha KOBYLKINA. “The use of modern cryptographic methods for protecting personal data under martial law.” The thesis in specialty 122 “Computer Science” consists of a text part containing 3 sections, 78 pages, 47 figures, 3 tables, 33 sources and 3 appendices.

This qualification work is devoted to the study of the use of modern cryptographic methods in martial law and their effectiveness in ensuring the confidentiality of information. The purpose of the work is to analyze modern cryptographic algorithms, assess their effectiveness and develop a secure password manager that provides reliable storage and management of authentication data.

The object of the research is methods and technologies for protecting personal data in the digital environment.

The subject of the research is software tools and algorithms used for secure storage and management of passwords.

The research methods include analysis of scientific sources, comparison of existing password managers (Bitwarden, LastPass, 1Password, KeePass, NordPass), as well as modeling of the architecture of the personal data protection system using UML diagrams. In the practical part, mechanisms for generating and encrypting passwords using the AES-256 algorithm are implemented.

The main results of the work include the development of a software prototype of a password manager that provides secure data storage and can be integrated into corporate and personal information systems. The results obtained can be used to create secure solutions for managing authentication data.

KEYWORDS: CRYPTOGRAPHY, PASSWORD MANAGER, INFORMATION SECURITY, ENCRYPTION, AUTHENTICATION, DATA PROTECTION.

ЗМІСТ

ВИСНОВКИ

У ході дослідження було розглянуто актуальні питання використання сучасних криптографічних методів для захисту персональних даних в умовах воєнного стану. Проведений аналіз підтвердив необхідність посилення інформаційної безпеки та підвищення надійності систем зберігання і управління паролями.

В першому розділі роботи здійснено аналіз сучасних криптографічних методів захисту даних, зокрема розглянуто основи криптографії, методи шифрування, алгоритми хешування та механізми генерації ключів. Визначено, що симетричні та асиметричні методи шифрування відіграють ключову роль у захисті інформації, а алгоритми хешування забезпечують цілісність та автентичність даних.

Другий розділ було присвячено особливостям забезпечення захисту персональних даних у кризових умовах, зокрема в умовах воєнного стану. Проаналізовано загрози, які виникають у період військових конфліктів, зокрема кібератаки, соціальну інженерію, а також ризики, пов’язані з використанням мобільних пристроїв та відкритих мереж. Окремо було розглянуто основні вектори атак на системи зберігання паролів та їх вплив на вимоги до інформаційної безпеки.

У третьому розділі було розглянуто процес створення менеджера паролів із використанням сучасних криптографічних методів. Проведено аналіз існуючих рішень на ринку, таких як Bitwarden, LastPass, 1Password, KeePass і NordPass. Визначено функціональні та нефункціональні вимоги до системи, змодельовано систему захисту персональних даних та реалізовано механізми генерації та шифрування паролів із використанням алгоритму AES-256. Також було розроблено UML-діаграми, що відображають архітектуру та функціональність запропонованої системи і прототип дизайну

Практичне значення отриманих результатів полягає в можливості використання запропонованої моделі для створення надійних систем

управління паролями, що відповідають сучасним вимогам безпеки. Запропоновані механізми можуть бути інтегровані в корпоративні системи для підвищення рівня захисту персональних даних, що є особливо актуальним у сучасних умовах.

Таким чином, у роботі досягнуто поставленої мети – досліджено сучасні криптографічні методи захисту даних, визначено ключові загрози в умовах воєнного стану, розроблено та реалізовано механізм управління паролями з високим рівнем безпеки. Отримані результати можуть бути використані для подальших досліджень у сфері інформаційної безпеки та криптографічного захисту персональних даних.