ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської
науково-практичної конференції

27 листопада 2025 року

м. Львів

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ

ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

ПРИВАТНИЙ ЗАКЛАД ВИЩОЇ ОСВІТИ «ІТ СТЕП УНІВЕРСИТЕТ»

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської науково-практичної конференції

27 листопада 2025 року

Львів – 2025

ББК 32.81+78.362

Інформаційна безпека та інформаційні технології: збірник тез доповідей VII Всеукраїнської науково-практичної конференції, м. Львів, 27 листопада 2025 року. Львів, ЛДУ БЖД, 2025, 493 с.

За точність наведених фактів, самостійність наукового аналізу та нормативність стилістики викладу, а також за використання відомостей, що не рекомендовані до відкритої публікації відповідальність несуть автори опублікованих матеріалів.

УДК 004.056:004.415

АВТОНОМНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ БЕЗПЕЧНОГО ЗБЕРІГАННЯ КОНФІДЕНЦІЙНИХ ДАНИХ

Віктор БОНК[1] Ростислав ТКАЧУК[1,2], Валентина ЯЩУК[1]
1. Львівський державний університет безпеки життєдіяльності
2. Національний університет «Львівська політехніка»

Анотація. *У роботі розглянуто програмне забезпечення для безпечного локального зберігання конфіденційної інформації. Наведено обґрунтування вибору мови програмування Python та середовища розробки PyCharm. Для захисту інформації запропоновано використання симетричне шифрування ChaCha20-Poly1305 із генерацією ключа за допомогою PBKDF2-HMAC-SHA256 і випадкової солі, що гарантує конфіденційність та автентифікацію даних. Запропоноване рішення забезпечує надійне, зручне та автономне зберігання персональних даних, сумісне з сучасними стандартами безпеки та нормативними вимогами.*

Ключові слова: *кіберзахист, конфіденційна інформація, локальне сховище, шифрування, Python, модульна архітектура.*

Abstract*. The paper considers software for secure local storage of confidential information. The rationale for choosing the Python programming language and the PyCharm development environment is presented. To protect information, it is proposed to use symmetric encryption ChaCha20-Poly1305 with key generation using PBKDF2-HMAC-SHA256 and a random salt, which guarantees data confidentiality and authentication. The proposed solution provides reliable, convenient and autonomous storage of personal data, compatible with modern security standards and regulatory requirements.*

Keywords: *cyber security, confidential information, local storage, encryption, Python, modular architecture.*

У сучасному цифровому середовищі стрімке зростання обсягів персональних даних і численних онлайн-сервісів підсилює ризики витоку, підробки та несанкціонованого доступу до інформації, що підтверджується численними масштабними інцидентами в державному та корпоративному секторі. Більшість користувачів не мають достатніх технічних знань для самостійного захисту даних, а стандартні інструменти часто зберігають інформацію у відкритому або слабко зашифрованому вигляді та не враховують захист вкладень. У цьому контексті особливо актуальною стає потреба в автономному програмному забезпеченні для локального зберігання конфіденційних відомостей без використання хмарних сервісів, яке забезпечує повноцінне шифрування, простоту використання та відповідність вимогам GDPR, українського законодавства та міжнародних стандартів NIST. Такий підхід дозволяє мінімізувати ризики втрати чи компрометації даних і підвищує рівень довіри користувачів до цифрових технологій [1].

Для створення програмного забезпечення безпечного зберігання конфіденційної інформації необхідне середовище, що забезпечує зручне написання коду, налагодження, керування залежностями та підтримку су-

часних бібліотек. Проведений аналіз засвідчив, що PyCharm є оптимальним інструментом для розробки Python-застосунків завдяки інтелектуальному автозавершенню, потужному налагоджувачу, інтеграції з Git, зручному управлінню віртуальними середовищами та повній сумісності з криптографічними бібліотеками й фреймворками для створення GUI [2].

Альтернативні рішення — Visual Studio Code, Visual Studio, Sublime Text і Jupyter Notebook — мають окремі переваги, однак або потребують значного додаткового налаштування, або не підтримують повноцінний цикл розробки десктопних застосунків. З огляду на комплексність інструментів, офіційну підтримку та зручність роботи з екосистемою Python, PyCharm було обрано як основне середовище розробки.

Python було обрано як оптимальне рішення завдяки поєднанню високої гнучкості, швидкості розробки, широкої підтримки GUI-фреймворків і наявності надійних криптографічних бібліотек. Використані інструменти Python забезпечили реалізацію всіх необхідних компонентів системи: криптографічного захисту, обробки файлів, зберігання структурованих даних і побудови графічного інтерфейсу [3].

Таким чином, екосистема Python надала збалансоване середовище для створення сучасного, захищеного та кросплатформного застосунку, забезпечивши оптимальне співвідношення продуктивності, функціональності та рівня безпеки.

Розроблене програмне забезпечення побудоване за модульною архітектурою, що забезпечує чіткий розподіл функціональних обов'язків, підвищує масштабованість та спрощує супровід системи. Структура складається з чотирьох основних підсистем: ядра, моделей даних, сервісних компонентів і графічного інтерфейсу.

Ядро (core) реалізує основні операції зі сховищем, включно з генерацією криптографічних ключів на основі PBKDF2-HMAC-SHA256 та шифруванням даних за алгоритмом ChaCha20-Poly1305. Сховище представлено єдиним зашифрованим файлом, що містить параметри криптографічної сесії та зашифрований вміст.

Моделі даних (models) описують типи записів (акаунти, картки, документи, нотатки), які уніфіковано представлені через базовий клас та можуть містити вкладені файли у форматі base64.

Сервісні модулі (services) забезпечують керування записами, обробку вкладень, тимчасове копіювання конфіденційних даних у буфер обміну та контроль неактивності користувача.

Графічний інтерфейс (gui) включає вікна аутентифікації, основне робоче середовище, панелі перегляду та діалоги налаштувань, забезпечуючи доступність функцій у зрозумілому інтерактивному форматі.

Розроблена система використовує повне симетричне шифрування всього сховища, зберігаючи всі конфіденційні дані в одному файлі без жодної інформації у відкритому вигляді. Для шифрування застосовано алго-

ритм ChaCha20-Poly1305, який забезпечує як конфіденційність, так і автентифікацію даних.

Ключ генерується шляхом перетворення майстер-пароля через PBKDF2-HMAC-SHA256 із використанням випадкової солі. Структура файлу включає salt, nonce та ciphertext, що гарантує коректність і безпеку відновлення даних.

Процедури шифрування й розшифрування складаються з послідовних етапів: серіалізації та десеріалізації структури сховища, генерації криптографічних параметрів, шифрування/дешифрування та формування підсумкового файлу. Усі помилки автентифікації блокують доступ до даних, унеможливлюючи їх читання при спотворенні вмісту або введенні неправильного пароля.

Система підтримує додавання вкладених файлів до будь-якого запису. Вкладення зберігається у вигляді текстового представлення (base64), що забезпечує сумісність із JSON-структурою та коректність подальшого шифрування.

Процес включає вибір користувачем файлу, перевірку його параметрів, кодування в base64, включення вкладення до моделі запису та повторне шифрування всього сховища. Тимчасові файли створюються лише на час перегляду та видаляються по завершенні сеансу. Обмеження на розмір вкладення забезпечують ефективність шифрування та швидкість роботи системи.

Запропоноване рішення забезпечує захищене збереження особистих записів і вкладень на основі сучасних криптографічних алгоритмів, поєднуючи зручність використання, гнучкість налаштувань і високий рівень надійності, що робить його придатним для особистих і професійних потреб.

Література

1. Моравський В., Ткачук Р. Л., Колос Н. М. Криптологія: сучасні тенденції та перспективи. Інформаційна безпека та інформаційні технології : зб. тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів. (Львів, 30 листопада 2023 р.). Львів : ЛДУБЖД, 2023. С. 130–133.

2. Балацька В.С., Ткачук Р.Л., Маслова Н.О. Еволюція КСЗІ та інтеграція блокчейн-технологій у кіберзахисті державних інформаційних систем України. Кібербезпека: освіта, наука, техніка. Спеціальний випуск : електронне фахове наукове видання Київ, 2025. № 2 (30). С. 316–332. DOI: https://doi.org/10.28925/2663-4023.2025.30.975

3. Казмірчук Є. Ткачук Р. Л. Тестування безпеки програмного коду. Інформаційна безпека та інформаційні технології : зб. тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів. (Львів, 26 листопада 2021 р.). Львів : ЛДУБЖД, 2021. С. 43–45.

Секція 2

КІБЕРБЕЗПЕКА

Наукове видання

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської науково-практичної конференції

Відповідальні за випуск **Назарій БУРАК**
Олександр ХЛЕВНОЙ

Оригінал-макет **Юлія НАЗАР, Ольга СМОТР, Роман ГОЛОВАТИЙ, Діана РАЙТА, Віра ДОВБНЯК, Іван РОВЕЦЬКИЙ, Наталія ЖЕЗЛО-ХЛЕВНА**

Підписано до друку 12.11.2025 р.
Формат 60×84/16. Гарнітура Times New Roman.
Друк на різографі. Папір офсетний.
Ум. друк. арк. 30.

Друк ЛДУ БЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
тел./факс: (032) 233-32-40, 233-24-79.