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 004.8:004.42:004.9

ПОЄДНАННЯ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ТА ГІБРИДНОГО ШИФРУВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Роман МАСЛЯК[1], Ростислав ТКАЧУК[1,2], Наталія МАСЛОВА[2]
[1]Львівський державний університет безпеки життєдіяльності
[2]Національний університет «Львівська політехніка»

Анотація. *У роботі розглянуто розробку десктопної системи FaceLock для захисту файлів і папок, що поєднує біометричну автентифікацію на основі розпізнавання облич та гібридне шифрування (AES-256 + RSA-2048). Система реалізована з модульною архітектурою, яка охоплює компоненти відеоаналізу, розпізнавання облич, криптографії та графічного інтерфейсу, забезпечуючи масштабованість і надійність. Запропоноване рішення демонструє ефективне поєднання криптографічних і біометричних технологій, що відповідає сучасним вимогам до безпечного та зручного управління конфіденційною інформацією.*

Ключові слова: *FaceLock, біометрична автентифікація, розпізнавання облич, гібридне шифрування, AES-256, RSA-2048, захист даних, модульна архітектура, інформаційна безпека, десктопна система.*

Abstract*. The paper discusses the development of a desktop FaceLock system for protecting files and folders, combining biometric authentication based on facial recognition and hybrid encryption (AES-256 + RSA-2048). The system is implemented with a modular architecture that includes components of video analysis, facial recognition, cryptography and a graphical interface, ensuring scalability and reliability. The proposed solution demonstrates an effective combination of cryptographic and biometric technologies that meets modern requirements for secure and convenient management of confidential information.*

Keywords: *FaceLock, biometric authentication, facial recognition, hybrid encryption, AES-256, RSA-2048, data protection, modular architecture, information security, desktop system.*

Актуальність дослідження зумовлена стрімким зростанням обсягів цифрових даних та підвищенням ризиків їх несанкціонованого доступу, що робить традиційні паролі дедалі менш надійними через вразливість до підбору, фішингу та компрометації. Біометричні технології, зокрема розпізнавання обличчя, пропонують значно вищий рівень автентифікації. За сучасними даними, понад 60 % користувачів смартфонів застосовують біометричну автентифікацію, а серед молоді цей показник сягає 75 %. У практичних сферах — від банків до прикордонного контролю — біометричні системи показали високу ефективність, зменшуючи час перевірки та ризики шахрайства. Поєднання таких методів з криптографічним шифруванням файлів і папок, як у системі FaceLock, відповідає глобальній тенденції переходу до безпарольних, зручних і водночас стійких механізмів захисту даних [1, 2].

Пропонована система FaceLock, спрямована на підвищення рівня захисту конфіденційної інформації шляхом інтеграції гібридного шифрування

(AES-256 + RSA) та біометричної ідентифікації на основі розпізнавання облич, значно підвищить рівень безпеки даних, зменшить ризики несанкціонованого доступу та компрометації інформації, забезпечить персоналізований доступ для користувачів і дозволить ефективно застосовувати сучасні методи автентифікації у персональних та корпоративних IT-системах. Передбачається, що такий підхід забезпечить доступ до даних лише після успішної автентифікації користувача, що суттєво знизить ймовірність їхньої компрометації. Використання високоточних алгоритмів розпізнавання облич із середньою точністю понад 99 % на стандартних датасетах у поєднанні з надійним криптографічним захистом дозволить сформувати комплексну модель безпеки, ефективну як у персональних, так і в корпоративних сценаріях використання. Крім того, система забезпечить зручність користування, масштабованість і відповідність сучасним вимогам до захисту даних у різних IT-інфраструктурах, що робить її перспективним рішенням для підвищення надійності інформаційної безпеки в умовах зростання кіберзагроз [3].

Система реалізується з використанням сучасних бібліотек та інструментів: OpenCV і face_recognition для обробки зображень, SQLAlchemy і PostgreSQL для роботи з базою даних, PyQt5 для створення графічного інтерфейсу, а також багатопотокового механізму для паралельного виконання операцій розпізнавання та шифрування. Контейнеризація за допомогою Docker Compose забезпечує відтворюваність, ізоляцію та масштабованість середовища. Біометричні шаблони зберігаються у хешованому або зашифрованому вигляді у PostgreSQL, що відповідає сучасним вимогам кібербезпеки.

Порівняння з існуючими рішеннями — VeraCrypt, TrueCrypt та BitLocker — показало, що ці системи не підтримують інтегровану біометричну автентифікацію. FaceLock усуває це обмеження, об’єднуючи шифрування, розпізнавання облич, обробку відеопотоків у реальному часі та багаторівневий контроль доступу, що підкреслює інноваційність підходу та відповідає сучасним вимогам до комплексного захисту даних [4].

Архітектура системи має модульну будову та включає компоненти для захоплення і обробки відеопотоку, генерації й порівняння біометричних ознак, керування користувачами та виконання криптографічних операцій (рис. 1). Модулі працюють незалежно один від одного, що забезпечує масштабованість, можливість модифікації окремих елементів і стійкість системи до навантажень. Взаємодія між ними реалізована через стандартизовані запити, що спрощує інтеграцію нових функцій.

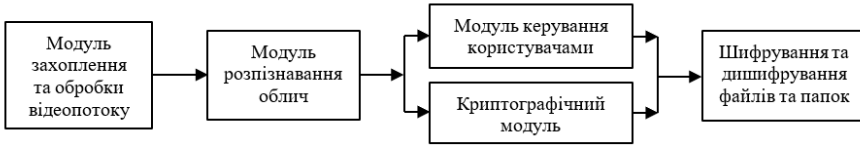

Рисунок 1 – Блок схема алгоритму архітектури системи

Гібридна схема шифрування даних передбачає використання алгоритму AES-256 для симетричного шифрування файлів, а симетричний ключ додатково кодується відкритим ключем RSA-2048 [5, 6]. Така комбінація забезпечує високу швидкодію при обробці великих обсягів даних і надійний захист ключової інформації навіть у разі часткової компрометації системи.

Реалізація системи передбачає графічний інтерфейс FaceLockApp, модуль обробки відеопотоку VideoStreamWorker, систему розпізнавання облич SimpleFaceRec та криптографічний модуль. Процес розпізнавання включає поетапне виявлення обличчя, обчислення дескрипторів і порівняння з базою даних. Реєстрація користувача включає зчитування біометричних ознак, генерацію криптографічних ключів і збереження публічного ключа разом із дескриптором обличчя. Доступ до шифрованих файлів можливий лише після успішної автентифікації користувача.

Отже FaceLock поєднує біометричну автентифікацію та гібридне шифрування, що забезпечує комплексний захист даних, модульну архітектуру для масштабованості та стабільну роботу системи. Інтеграція відеопотоків, розпізнавання облич і багаторівневий контроль доступу робить її інноваційним і практично придатним рішенням для безпечного управління конфіденційною інформацією.

Література

1. Yang, W., Wang, S., Cui, H., Tang, Z., & Li, Y. (2023). *A Review of Homomorphic Encryption for Privacy-Preserving Biometrics. Sensors,* 23(7), 3566. https://doi.org/10.3390/s23073566 MDPI

2. Пановик У. П., Ткачук Р. Л. Кібербезпека через призму системного аналізу. Комп'ютерні технології друкарства : зб. наук. пр. Львів : УАД, 2023. № 1 (49). С. 197–208. URL: https://doi.org/10.32403/2411-9210-2023-1-49-197-208 (index Copernicus International)

3. Боднар О., Лагун А. Е., Ткачук Р. Л. Виявлення небезпечних входжень у комп'ютерну мережу за допомогою систем виявлення вторгнень. 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. 9–12.

4. 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.

5. Singh, S., Igene, L., & Schuckers, S. (2024). *Securing Biometric Data: Fully Homomorphic Encryption in Multimodal Iris and Face Recognition*. arXiv. https://arxiv.org/abs/2408.14609

6. Qin, Y., & Zhang, B. (2023). *Privacy-Preserving Biometrics Image Encryption and Digital Signature Technique Using Arnold and ElGamal*. *Applied Sciences,* 13(14), 8117. https://doi.org/10.3390/app13148117 MDPI

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.