ЗАСТОСУВАННЯ КРИПТОГРАФІЧНОГО АЛГОРИТМУ AES ДЛЯ ЗАХИСТУ ФАЙЛОВИХ ДАНИХ НА ПЕРСОНАЛЬНИХ КОМП'ЮТЕРАХ

Кононенко К.О., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Зростання обсягів цифрової інформації, що зберігається на персональних комп'ютерах, підвищує актуальність захисту файлових даних від несанкціонованого доступу, модифікації та розголошення. Особливу увагу доцільно приділяти локальним файлам, які можуть містити персональні відомості, службові документи та іншу конфіденційну інформацію. Навіть за наявності стандартних механізмів операційної системи питання захисту вмісту файлів залишається важливим у разі втрати пристрою, копіювання носія або отримання сторонньою особою доступу до файлової системи.

Метою доповіді є узагальнення підходів до криптографічного захисту файлових даних на персональних комп'ютерах та визначення особливостей використання алгоритму AES як основи локального захищеного файлового середовища.

Одним із поширених способів забезпечення конфіденційності даних є симетричне шифрування. На відміну від організаційних обмежень доступу, криптографічний захист спрямований на унеможливлення прочитання вмісту зашифрованого файлу без відповідного ключа. Стандарт AES передбачає використання ключів довжиною 128, 192 або 256 біт і застосовується для захисту інформації в різних програмних системах [1]. Водночас безпека конкретного рішення залежить не лише від обраного алгоритму, а й від режиму його роботи та правил поводження з ключами.

Для захисту файлових даних важливими є дві властивості: конфіденційність і цілісність. Перша обмежує можливість ознайомлення зі змістом інформації, друга дозволяє виявляти її несанкціоновані зміни. Режим GCM поєднує шифрування з автентифікацією даних, що дає змогу перевіряти коректність зашифрованого повідомлення під час розшифрування [2]. Застосування AES-256-GCM є доцільним для файлового середовища, у якому необхідно забезпечити обидві зазначені властивості.

Використання автентифікованого шифрування потребує дотримання низки умов. Зокрема, для операцій із тим самим ключем необхідно забезпечувати унікальність значень nonce; повторне використання таких значень може суттєво послабити захист. Крім того, слід перевіряти тег автентифікації до надання доступу до розшифрованих даних. Тому криптографічні параметри та формат зберігання зашифрованого файлу мають визначатися на етапі проєктування, а не лише під час програмної реалізації [2].

Окрему проблему становить керування криптографічними ключами. Зберігання ключа поряд із зашифрованими файлами без додаткових заходів захисту може нівелювати переваги шифрування. Для зменшення цього ризику

можуть застосовуватися похідні ключі, механізми обгортання ключів та розмежування ключів для шифрування даних і захисту ключового матеріалу. Загальні принципи життєвого циклу криптографічних ключів, включно з їх створенням, зберіганням і знищенням, розглянуто в рекомендаціях NIST [3].

Для систем, у яких доступ до файлів пов'язаний із паролем користувача, важливим є стійке формування ключового матеріалу. Застосування функцій виведення ключів із параметрами обчислювальної та пам'яттєвої складності ускладнює масовий перебір паролів. Одним із відомих підходів є Argon2, описаний у RFC 9106 [4]. Проте навіть використання стійкої функції не компенсує слабкого пароля та не усуває потреби в продуманій процедурі відновлення доступу.

Під час побудови локального файлового середовища необхідно враховувати не лише криптографічні операції, а й особливості зберігання метаданих, тимчасових розшифрованих копій та резервних даних. Метадані можуть розкривати відомості про структуру сховища навіть тоді, коли вміст файлів зашифрований. Тимчасові файли, створені для перегляду або редагування документів, також потребують окремих правил оброблення й видалення. Отже, захист файлових даних доцільно розглядати як сукупність взаємопов'язаних технічних і організаційних механізмів.

Межі захисту слід визначати за моделлю загроз: шифрування зменшує ризик розкриття вмісту скопійованих файлів, але не гарантує протидії шкідливим програмам під час роботи авторизованого користувача.

Таким чином, застосування AES-256-GCM створює криптографічну основу для забезпечення конфіденційності та контролю цілісності локальних файлових даних. Ефективність такого підходу визначається комплексністю реалізації: коректним використанням режиму шифрування, належним керуванням ключами, захистом супровідної інформації та обґрунтованим розмежуванням доступу. Подальше дослідження доцільно спрямувати на експериментальну перевірку коректності криптографічних операцій, продуктивності оброблення файлів і стійкості реалізованих механізмів у межах визначеної моделі загроз.

Список літератури

1. Advanced Encryption Standard (AES) : FIPS PUB 197 / National Institute of Standards and Technology. Gaithersburg : NIST, 2023. DOI: https://doi.org/10.6028/NIST.FIPS.197.

2. Dworkin M. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC : NIST Special Publication 800-38D. Gaithersburg : NIST, 2007. DOI: https://doi.org/10.6028/NIST.SP.800-38D.

3. Barker E. Recommendation for Key Management: Part 1 – General : NIST Special Publication 800-57 Part 1 Revision 5. Gaithersburg : NIST, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-57pt1r5.

4. Biryukov A., Dinu D., Khovratovich D., Josefsson S. Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications : RFC 9106. RFC Editor, 2021. DOI: https://doi.org/10.17487/RFC9106.