УДК 004.056.5

Тимощук В. – ст. гр. КТ-21, Стебельський М. – ст. гр. СБс-33
Тернопільський національний технічний університет імені Івана Пулюя

ШИФРУВАННЯ ДАНИХ В ОПЕРАЦІЙНИХ СИСТЕМАХ

Науковий керівник: Тимощук Д.І.

V. Tymoshchuk, M. Stebelskyi
Ternopil Ivan Puluj National Technical University

DATA ENCRYPTION IN OPERATING SYSTEMS

Supervisor: D. Tymoshchuk

Ключові слова: шифрування, операційні системи, Windows, Linux, Unix, MacOS.
Keywords: encryption, operating systems, Windows, Linux, Unix, MacOS.

Захист конфіденційності та цілісності даних є одним із важливих аспектів сучасного інформаційного світу. Шифрування є ефективним способом захисту даних в операційних системах від несанкціонованого доступу. Операційні системи, такі як Windows, Linux, Unix та MacOS, надають вбудовані рішення для шифрування даних, такі як BitLocker, LUKS, GELI та FileVault відповідно.

Одним з найпоширеніших рішень шифрування даних є BitLocker, який доступний в операційних системах Windows. Він надає можливість шифрувати всі дані на системному розділі, додаткових розділах або на зовнішньому пристрої зберігання. BitLocker - це засіб шифрування даних, який використовує метод шифрування AES (Advanced Encryption Standard) з 128-бітним або 256-бітним ключем для захисту даних. До того ж, BitLocker також може використовувати апаратний модуль шифрування (TPM - Trusted Platform Module) для зберігання ключів шифрування та захисту системи від несанкціонованого доступу до даних, що зберігаються на жорсткому диску. BitLocker може бути керований через централізовані політики (Group Policy) в корпоративному середовищі.

У свою чергу, LUKS (Linux Unified Key Setup) є стандартом для шифрування даних в операційних системах Linux. Він надає можливість шифрувати розділи або пристрої зберігання на рівні блоків даних. LUKS використовує різні типи шифрування, такі як AES, Twofish, Serpent, та інші. Він також підтримує різні режими роботи, такі як режим шифрування всього пристрою, режим шифрування розділу або режим шифрування віртуального тома.

У операційній системі Unix та її похідних, таких як FreeBSD, OpenBSD, NetBSD, використовується GELI (GEOM ELI). Він надає можливість шифрувати розділи або пристрої зберігання на рівні блоків даних. GELI використовує різні типи шифрування, такі як AES, Blowfish, 3DES та інші. Він також має функції, такі як підтримка ключів шифрування на основі паролю, ключів з файлу або ключів на основі апаратного забезпечення.

Операційна система MacOS пропонує власний інструмент для шифрування даних - FileVault. Він надає можливість шифрувати всі дані на внутрішньому диску або на зовнішньому пристрої зберігання. FileVault використовує різні типи шифрування, такі як XTS-AES-128, XTS-AES-256, та інші. Він також має функцію підтримки керування ключами шифрування через iCloud.

Всі розглянуті рішення надають високий рівень захисту даних за допомогою різних типів шифрування та можливості використання різні режимів шифрування, що

відповідає різним вимогам безпеки. Також всі розглянуті рішення є вбудованими в операційні системи, що робить їх зручними для використання. Вони мають графічний інтерфейс або командний рядок, які дозволяють користувачам налаштовувати та керувати процесом шифрування. Деякі рішення, такі як BitLocker та FileVault, також надають можливість керування ключами через центр керування, що робить їх більш зручними для використання в корпоративному середовищі.

Різні рішення мають різний рівень доступності залежно від операційної системи та версії, яку використовує користувач. Наприклад, BitLocker не доступний в базовій версії Windows 10 Home. У той же час, LUKS, GELI та FileVault доступні відразу в відповідних операційних системах без додаткових обмежень.

Кожне рішення має свій рівень безпеки, який може бути відмінним в залежності від використовуваного шифру, режиму шифрування, довжини ключа, керування ключами та інших факторів. Важливо враховувати вимоги безпеки та рівень захисту даних, який необхідний для конкретного випадку використання.

Легкість використання також є важливим фактором при оцінці ефективності рішення шифрування даних. Чим простіше та зрозуміліше рішення для використання, тим менше шансів на помилки або неправильне налаштування, що може вплинути на безпеку даних.

Загалом, рішення шифрування даних в операційних системах Windows (BitLocker), Linux (LUKS), Unix (GELI) та MacOS (FileVault) є ефективними засобами забезпечення безпеки даних. Вони надають різні функції шифрування, типи шифрів та можливості керування ключами, в залежності від операційної системи та версії.

Практичне використання шифрування даних є корисним для захисту конфіденційної інформації, такої як корпоративні дані, фінансові дані, медичні записи та інше. Шифрування застосовується в різних сценаріях, включаючи роботу з особистими комп'ютерами, ноутбуками, серверами, мобільними пристроями та зовнішніми носіями даних.

Важливо правильно налаштувати та управляти рішеннями шифрування, включаючи забезпечення безпеки ключів, використання сильних паролів та періодичну зміну паролів. Також потрібно пам’ятати, що жодне рішення шифрування не є на 100% надійним.