УДК 681.518.3
В.О. Семенюк, д.т.н., проф.; Я.В. Литвиненко
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОГЛЯД МЕТОДІВ ЗАХИСТУ ТЕКСТОВОЇ ІНФОРМАЦІЇ

V.O. Semenyuk, Dr., Prof.; Ia.V. Lytvynenko

OVERVIEW OF TEXT INFORMATION PROTECTION METHODS

Захист текстової інформації є важливою задачею, особливо в сучасному цифровому середовищі. На даний час існує велика кількість розроблених методів захисту інформації. Щоб зорієнтуватись які найкраще застосувати для нашої задачі проведемо огляд існуючих на практиці методів.

Дана доповідь стосується огляду відомих методів, які можна застосувати для захисту текстової інформації.

Існує кілька методів та стратегій для захисту текстової інформації від несанкціонованого доступу та збереження конфіденційності. Розглянемо деякі з них:

- Шифрування: Симетричне шифрування: Використовує один ключ для як шифрування, так і розшифрування тексту. Приклади - AES, DES.
- Асиметричне (або публічне) шифрування: Використовує пару ключів (приватний і публічний) для шифрування та розшифрування. Приклади - RSA, ECC.
- Хешування: Використання хеш-функцій: Дозволяє перетворити вхідні дані в унікальний хеш-код фіксованої довжини. Використовується для перевірки цілісності даних.
- Цифровий підпис: RSA, DSA, ECDSA: Дозволяє встановити автентичність та цілісність даних за допомогою підпису, який генерується приватним ключем.

До інших методів і стратегій захисту інформації можна віднести:

- Використання VPN: Віртуальні приватні мережі: Забезпечують безпечний тунель для передачі даних через незахищені мережі, що дозволяє шифрувати текстову інформацію.
- Керування доступом: Ролева модель: Визначення різних рівнів доступу до інформації на основі ролей користувачів.
- Механізми аутентифікації: Використання паролів, біометричних даних чи двофакторної аутентифікації.
- Фільтрація та моніторинг: Системи виявлення вторгнень (IDS) та системи захисту від вторгнень (IPS): Сприймають та реагують на аномалії або несподівані події в мережі.
- Зберігання та обробка: Шифрування на рівні файлів або дисків: Захищає дані, коли вони зберігаються або обробляються на пристроях.
- Оновлення та патчі: Регулярні оновлення програмного забезпечення: Забезпечують виправлення виявлених уразливостей.

Ці методи та стратегії захисту часто використовуються в поєднанні для створення комплексних систем безпеки, оскільки один захисний захід не завжди достатньо ефективний.

Література

1. Писарчук О.О. Основи захисту інформації : навчальний посібник / О.О. Писарчук, Ю. Г. Даник, С. Г. Вдовенко та ін. – Житомир : ЖВІ ДУТ, 2015. 226 с.
2. Хорошко В.А. Методи й засоби захисту інформації / ВА Хорошко, АА Чекатков К.: ЮНІОР, 2003.