УДК 510.635:004.891(045)

І.І. Чернега
Національна академія Служби безпеки України, Київ

КРИПТОГРАФІЧНИЙ ЗАХИСТ ДЕРЖАВНОЇ ІНФОРМАЦІЇ

Криптографічний захист державної інформації є важливим. Існують багато методів, таких як симетричне та асиметричне шифрування, хешування та цифровий підпис. Вони можуть використовуватися окремо або в комбінації. Криптографічний захист допомагає забезпечити безпеку та конфіденційність даних в електронному вигляді. Відповідні методи шифрування та протоколи обміну ключами запобігають несанкціонованому доступу та забезпечують цілісність даних.

Криптографічний захист інформації може комбінуватися з фізичним захистом для забезпечення безпеки та конфіденційності даних у державних установах. У асиметричному шифруванні використовується два ключі - публічний та приватний. Публічний ключ використовується для зашифрування даних, а приватний - для їх розшифрування.

Хеш-функції використовуються для створення унікального "відбитка" даних, який може бути використаний для перевірки їх цілісності. Криптографічний захист інформації є важливим для захисту даних в електронному вигляді. Комбінація криптографічного захисту та фізичного захисту пристроїв та мереж може допомогти забезпечити безпеку та конфіденційність даних. Наприклад, шифрування даних за допомогою AES з використанням ключа довжиною 256 бітів є дуже надійним методом захисту.

Цифрові підписи, такі як RSA та DSA, можуть використовуватися для підтвердження автентичності та цілісності документів. Асиметричне шифрування використовує два ключі - публічний та приватний, і використовується для безпеки передачі даних в мережі Інтернет. Для симетричного шифрування використовуються AES, DES та 3DES. Хешування застосовується для захисту від несанкціонованого доступу та вторгнень, включає в собі захист паролів та перевірку цілісності даних.

Цифровий підпис - це криптографічний механізм, що дозволяє забезпечити автентифікацію та цілісність даних, Криптографічний підпис дозволяє зберігати конфіденційність, цілісність та доступність даних у державних органах. Крім того, цифровий

підпис може бути використаний для підтвердження автентичності документів та повідомлень. Державні органи можуть використовувати алгоритми, такі як RSA та DSA, для створення цифрових підписів.

Протоколи обміну ключами - це методи забезпечення безпеки при обміні даними між сторонами за допомогою обміну криптографічними ключами. Основні протоколи цього типу включають: Діффі-Геллмана, RSA та ECDH. Вони використовуються в інтернет-безпеці, банківських транзакціях та інших сферах. Наприклад, TLS використовує протокол Діффі-Геллмана. Ці протоколи допомагають захистити конфіденційну інформацію та запобігти злому системи через перехоплення ключів під час їх передачі.

Основні методи захисту - симетричне та асиметричне шифрування, хешування, криптографічний цифровий підпис та протоколи обміну ключами. Для криптографічного захисту використовуються різні технології, такі як блочне шифрування, RSA, ECC, AES, SHA, MD5 та інші.Криптографічний захист повинен використовуватись разом з іншими методами захисту та дотримуватись стандартів та рекомендацій, надійності та безпеки системи. Наприклад, важливо забезпечити фізичну безпеку пристроїв, які зберігають чутливу інформацію, а також регулярно оновлювати криптографічні ключі та протоколи, щоб запобігти їх компрометації. Потрібно дотримуватись стандартів та рекомендацій щодо криптографічного захисту, оскільки неправильне застосування може привести до порушення безпеки даних.

Загалом, криптографічні методи та технології є невід'ємною частиною захисту інформації у державних органах та дозволяють зберігати конфіденційність, цілісність та доступність данихКрім того, важливо дотримуватись стандартів та рекомендацій щодо криптографічного захисту, оскільки неправильне застосування може привести до порушення безпеки даних.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Stallings, W. (2017). Криптографія та мережева безпека: принципи та практика.

2. Paar, C., & Pelzl, J. (2010). Розумна криптографія: підручник для студентів та фахівців.