УДК 004.056 https://doi.org/10.30837/IYF.PCEIP.2024.088

ВИКОРИСТАННЯ МЕТОДІВ, МЕХАНІЗМІВ ТА ЗАСОБІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ПРИКЛАДІ ЗАХИСТУ БІОМЕТРИЧНИХ ДАНИХ

Бабаєва К. Г. гизи
Науковий керівник – к.т.н. Мельникова О. А.
Харківський національний університет радіоелектроніки, каф. БІТ, м. Харків, Україна
e-mail: kamila.babaieva@nure.ua

Information plays a key role in our lives nowadays. Methods, mechanisms and ways for cryptographic information protection allow us to safely store, transmit, and verify information transferred to us. Since, for example, confidential or personal information needs to be protected from being obtained by third parties who can use it for their own purposes. And the life and fate of all people may depend on this information. Nowadays, there are a huge number of methods, mechanisms and ways to protect information. Confidential information must be protected from being leaked or published because it can cause great harm to the owner of the information or to those who disclosed it.

Найважливішим елементом сучасного життя є інформація. Інформація буває відкритою або конфіденційною. Важливість інформації підтверджує вислів Н. Ротшильда: “Хто володіє інформацією, той володіє світом!”. Конфіденційну інформацію потрібно захищати від витоку або публікування, тому що це може нанести велику шкоду власнику такої інформації або тим, хто її передав.

З новими стрімкими технічними проривами, ми отримуємо все більше інформації, яку потрібно зберігати та захищати. Зокрема, це біометричні дані людей, які зараз використовуються, починаючи з безкодового доступу до телефону, комп’ютеру, квартири, дому, закінчуючи підтвердженням оплати рахунків. Наприклад, у Китаї використовують біометричні дані (скан обличчя) для оплати у магазинах. Всю цю інформацію потрібно надійно зберігати, для цього використовується криптографічний захист інформації (шифрування).

Біометричні дані, такі як скани обличчя, відбитки пальців, структура рук чи голос, є важливими елементами в сучасних системах ідентифікації та автентифікації [1, 2]. Вони використовуються для забезпечення вищого рівня безпеки в різних сферах, включаючи фінанси, охорону здоров'я, урядові послуги та багато інших. Проте, захист цих біометричних даних є критично важливою задачею з погляду конфіденційності та цілісності особистої інформації.

Існує багато методів, механізмів та засобів криптографічного захисту інформації: апаратні, програмні та апаратно-програмні системи та комплекси, що реалізують криптографічні алгоритми перетворення.

Основна мета КЗІ полягає в тому, щоб забезпечити високий рівень захисту інформації від несанкціонованого доступу та змін, що можуть спричинити порушення конфіденційності, цілісності або доступності даних [3]. Це особливо важливо в сферах, де обробка та передача конфіденційної інформації є критичною, таких як фінанси, медицина, урядові служби та багато інших.

До засобів криптографічного захисту інформації (КЗІ) можна віднести наступне.

1. Засоби, призначені для виготовлення ключових даних або документів (незалежно від виду носія ключової інформації) та управління ключовими даними, що використовуються в засобах криптографічного захисту інформації.

2. Засоби захисту від нав'язування неправдивої інформації або захисту від несанкціонованої модифікації, що реалізують алгоритми криптографічного перетворення інформації (криптоалгоритми), включаючи засоби імітозахисту та електронного цифрового підпису.

3. Засоби захисту інформації від несанкціонованого доступу (у тому числі засоби розмежування доступу до ресурсів електронно-обчислювальної техніки), у яких реалізовані криптоалгоритми.

У засобах КЗІ повинні бути реалізовані різні механізми для контролю та захисту інформації, ось деякі з них:

1) механізми контролю цілісності криптографічних перетворень та захисту ключових даних;

2) механізми захисту від порушення конфіденційності інформації внаслідок помилкових дій оператора, або в разі відхилень у роботі складових елементів засобу КЗІ;

3) механізми розмежування доступу до функцій засобу КЗІ, криптографічної схеми та ключових даних;

4) довірений канал для отримання інформації, що підлягає захисту;

5) механізми знищення ключових даних після закінчення строку їх дії;

6) механізми захисту ключових даних на їх носіях від несанкціонованого зчитування;

7) механізми захисту від порушення конфіденційності та цілісності ключових даних;

Можна вказати наступні криптографічні засоби захисту, які обов’язково використовуються при передачі та зберіганні інформації.

1. Шифрування. Перетворення інформації з використанням ключа для обмеження доступу до неї тільки авторизованим особам, які володіють ключем.

2. Цифровий підпис. Дозволяє визначити, якою саме особою або системою було підписано інформацію, а також підтвердити цілісність інформації.

3. Гешування даних. Використовується для створення унікального геш-коду з вхідних даних за допомогою геш-функцій. Цей геш-код служить для перевірки цілісності даних, оскільки будь-яка зміна вихідних даних призведе до зміни геш-коду.

4. Контроль доступу. Використовується для регулювання доступу до конфіденційної інформації, використовуючи різноманітні механізми, такі як ролі користувачів, політики доступу, аудит доступу та інші.

Для безпечного збереження та передачі конфіденційних, приватних біометричних даних, необхідно використовувати усі механізми, засоби та методи криптографічного захисту інформації (КЗІ). Це означає, що біометричні дані, такі як скан обличчя, повинні бути збережені у зашифрованому вигляді.

Крім того, важливо зберігати геш-коди розшифрованих даних, щоб після розшифрування можна було перевірити цілісність інформації. При передачі навіть зашифрованих біометричних даних важливо використовувати електронний цифровий підпис (ЕЦП), щоб забезпечити їхню автентичність та недоторканість під час передачі через мережу. Це дозволить перевірити, що дані не були змінені або підроблені під час передачі.

Крім застосування криптографічних методів, важливо забезпечити безпеку в процесі збору, зберігання та обробки біометричних даних. Це означає, що пристрої, які збирають біометричні дані, повинні бути захищені від несанкціонованого доступу та фізичної атаки.

У сучасному світі, де біометричні технології широко використовуються в різних сферах, важливо постійно вдосконалювати заходи захисту біометричних даних із урахуванням швидкого розвитку технологій та змін у загрозах кібербезпеки.

Тільки таким чином можна забезпечити високий рівень безпеки та довіру до систем, які використовують біометричні дані.

Список використаних джерел

1. Мироненко Є.В., Сєвєрінов О.В. Біометрична ідентифікація і автентифікація особи за геометрією обличчя. НТУ «ХПІ», 2020.

2. Gvozdov Roman et al. "Method of Biometric Authentication with Digital Watermarks." 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T). IEEE, 2021.

3. Про затвердження Вимог до засобів криптографічного захисту інформації, призначених для захисту таємної інформації, яка не становить державної таємниці, та конфіденційної інформації в державних органах, органах місцевого самоврядування, на підприємствах, в установах та організаціях, які належать до сфери їх управління, військових формуваннях, які створені відповідно до закону : Наказ Адмін. Держ. служби спец. зв'язку та зах. інформації України від 07.05.2021 р. № 278. URL: https://zakon.rada.gov.ua/laws/show/z0696-21#Text (дата звернення: 05.03.2024).