КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Підготувала:
Кірєєва Софія

Клас: 11-А

ПЛАН

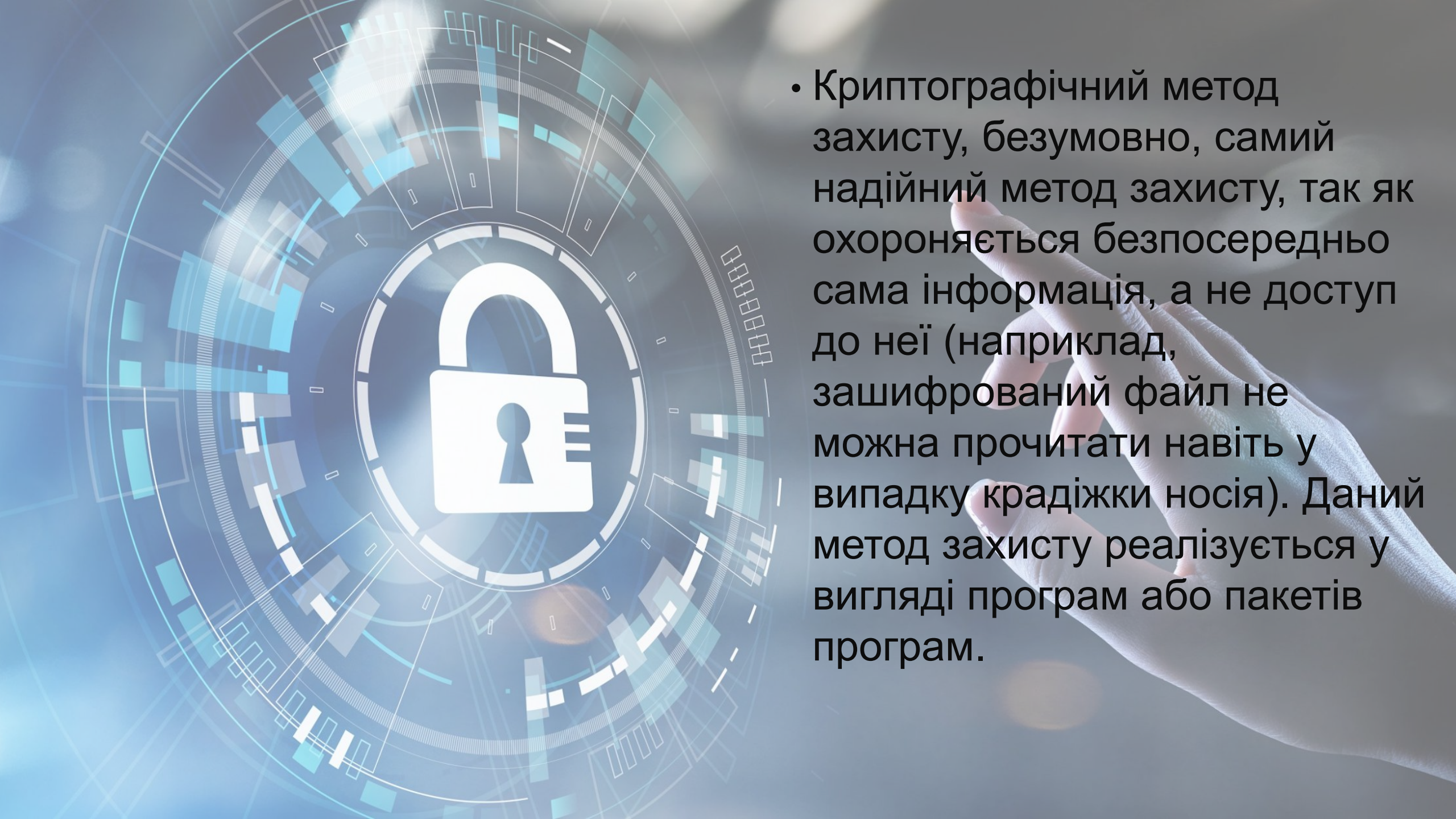
- Вступ
- Що таке криптографічні методи захисту інформації
- Шифрування
- Контроль цілісності
- Аудит

ВСТУП

- Криптографі́чний за́хист інформа́ції — вид захисту інформації, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

ЩО ТАКЕ КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

- Криптографічні методи захисту інформації — це спеціальні методи шифрування, кодування або іншого перетворення інформації, в результаті якого її зміст стає недоступним без пред’явлення ключа криптограми і зворотного перетворення.



- Криптографічний метод захисту, безумовно, самий надійний метод захисту, так як охороняється безпосередньо сама інформація, а не доступ до неї (наприклад, зашифрований файл не можна прочитати навіть у випадку крадіжки носія). Даний метод захисту реалізується у вигляді програм або пакетів програм.

ПЕРЕД СУЧАСНИМИ КРИПТОГРАФІЧНИМИ СИСТЕМАМИ ЗАХИСТУ ІНФОРМАЦІЇ СТАВЛЯТЬ НАСТУПНІ ВИМОГИ:

- зашифроване повідомлення повинне піддаватися читанню тільки при наявності ключа;
- число операцій, необхідних для визначення використаного ключа шифрування по фрагменту шифрованого повідомлення і відповідного йому відкритого тексту, повинне бути не менше загального числа можливих ключів;
- число операцій, необхідних для розшифровування інформації шляхом перебору ключів, повинно мати чітку нижню оцінку і виходити за межі можливостей сучасних комп’ютерів (з урахуванням можливості використання мережевих обчислень);

- знання алгоритму шифрування не повинне впливати на надійність захисту;
- незначна зміна ключа повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні того самого ключа;
- структурні елементи алгоритму шифрування повинні бути незмінними;
- додаткові біти, що вводяться в повідомлення в процесі шифрування, повинні бути цілком і надійно сховані в шифрованому тексті;

- довжина шифрованого тексту повинна бути рівна довжині вихідного тексту;
- не повинно бути простих (які легко встановлюються) залежностей між ключами, що послідовно використовуються в процесі шифрування;
- будь-який ключ з безлічі можливих повинен забезпечувати надійний захист інформації;
- алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна призводити до якісного погіршення алгоритму шифрування.

ШИФРУВАННЯ

- Криптографічний алгоритм, названий алгоритмом шифрування, представлений деякою математичною функцією, яка використовується для шифрування і розшифровки. Точніше таких функцій дві: одна використовується для шифрування, а інша — для розшифрування.
- Розрізняється шифрування двох типів:
- симетричне (із секретним ключем);
- несиметричне (з відкритим ключем).

- При симетричному шифруванні створюється ключ, файл разом з цим ключем пропускається через програму шифрування та отриманий результат пересилається адресатові, а сам ключ передається адресатові окремо, використовуючи інший (захищений або дуже надійний) канал зв’язку.

Несиметричне шифрування складніше, але і надійніше. Для його реалізації потрібні два взаємозалежних ключі: відкритий і закритий.

Одержувач повідомляє всім бажаючий свій відкритий ключ, що дозволяє шифрувати для нього повідомлення. Закритий ключ відомий тільки одержувачеві повідомлення. Коли комусь потрібно послати зашифрованет повідомлення, він виконує шифрування, використовуючи відкритий ключ одержувача. Одержавши повідомлення, останній розшифровує його за допомогою свого закритого ключа. За підвищену надійність несиметричного шифрування приходиться платити: оскільки обчислення в цьому випадку складніше, то процедура розшифровки займає більше часу.

КОНТРОЛЬ ЦІЛІСНОСТІ

В основі криптографічного контролю цілісності лежать два поняття:

- хеш-функція;
- електронний цифровий підпис (ЕЦП).

Хеш-функція — це складнозворстнє перетворення даних (однобічна функція), реалізована, як правило, засобами симетричного шифрування зі зв’язуванням блоків. Результат шифрування останнього блоку (що залежить від усіх попередніх) і слугує результатом хеш-функції.

АУДИТ

- Аудит — це аналіз накопиченої інформації, проведений оперативно, у реальному часі або періодично (наприклад, раз на день). Оперативний аудит з автоматичним реагуванням на виявлені позаштатні ситуації називається активним. При протоколюванні події рекомендується записувати, принаймні, наступну інформацію:
- дата й час події;
- унікальний ідентифікатор користувача — ініціатора дії;
- тип події;
- результат дії (успіх або невдача);
- джерело запиту (наприклад, ім’я термінала);
- імена порушених об’єктів (наприклад, відкритих або видалених файлів);
- опис змін, внесених у бази даних захисту (наприклад, нова мітка безпеки об’єкта).