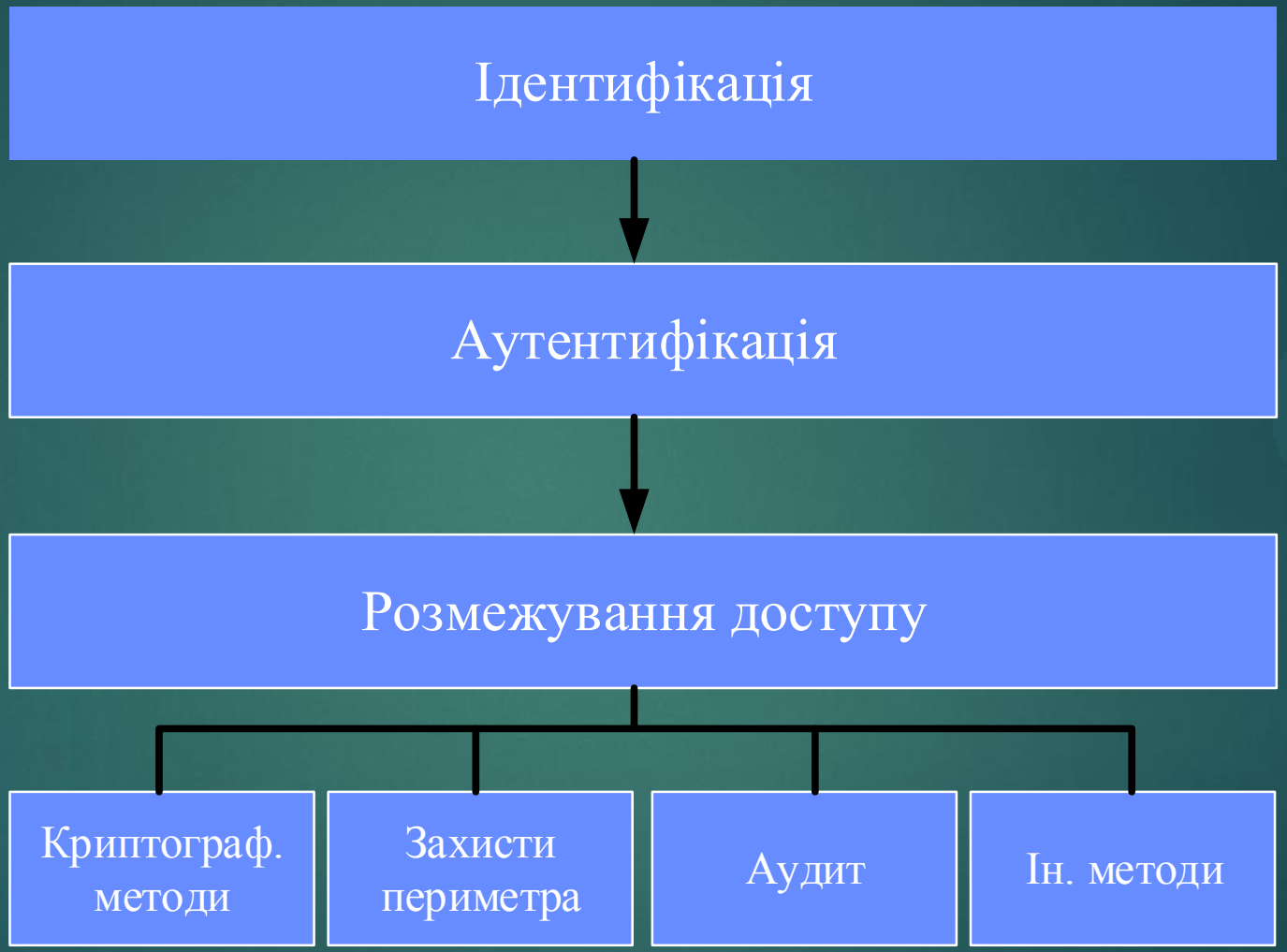
Презентація

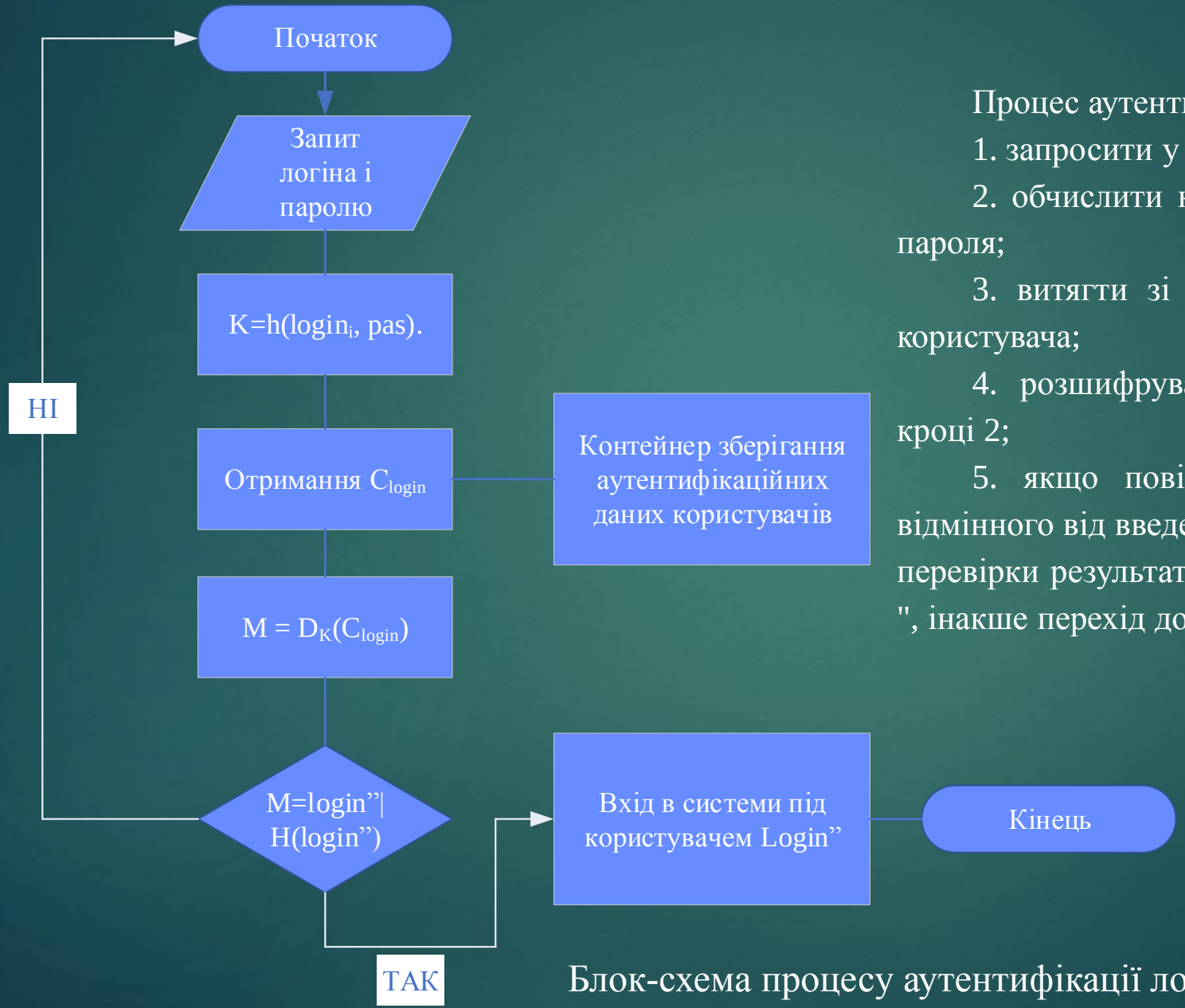
На тему:

ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БЕЗПРОВІДНИХ МЕРЕЖАХ WiMAX

Виконав: студент групи ТТК-18м
Чуба Валерій



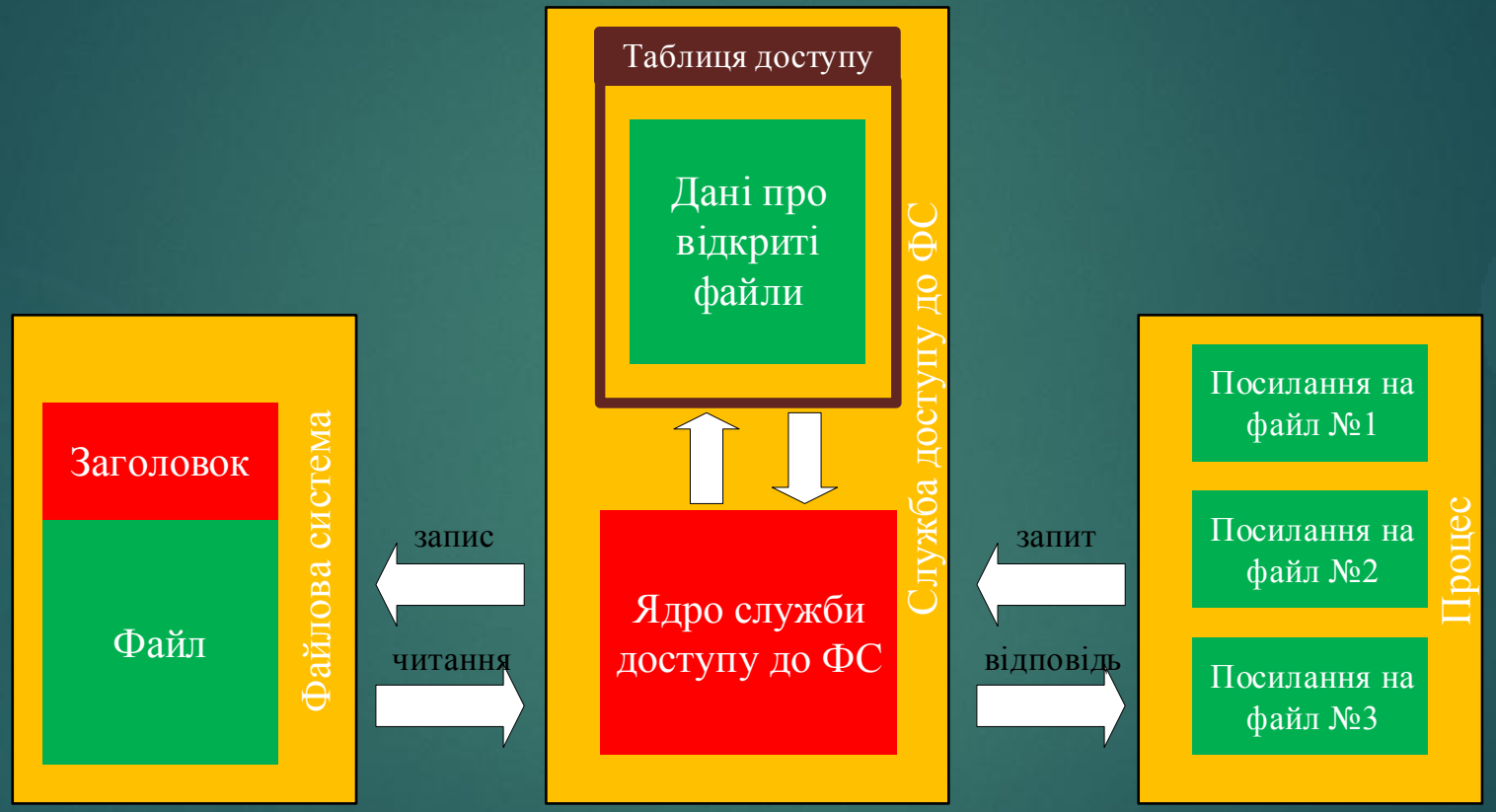
Структура системи захисту від загроз порушення конфіденційності



Процес аутентифікації полягає в наступному:

1. запросити у користувача логін і пароль;
2. обчислити ключ шифрування як хеш-значення логіна і пароля;
3. витягти зі сховища шифртекст, відповідно з логіном користувача;
4. розшифрувати повідомлення ключем, отриманим на кроці 2;
5. якщо повідомлення складається з login "(можливо відмінного від введеного) і хеш-значення отриманого login" (для перевірки результату), то вхід в систему під користувачем login ", інакше перехід до кроку 1.

Блок-схема процесу аутентифікації локальних користувачів



Структурна схема служби доступу до файлової системи

ПОВІДОМЛЕННЯ 1 (M1)

K1

Алгоритм шифрування

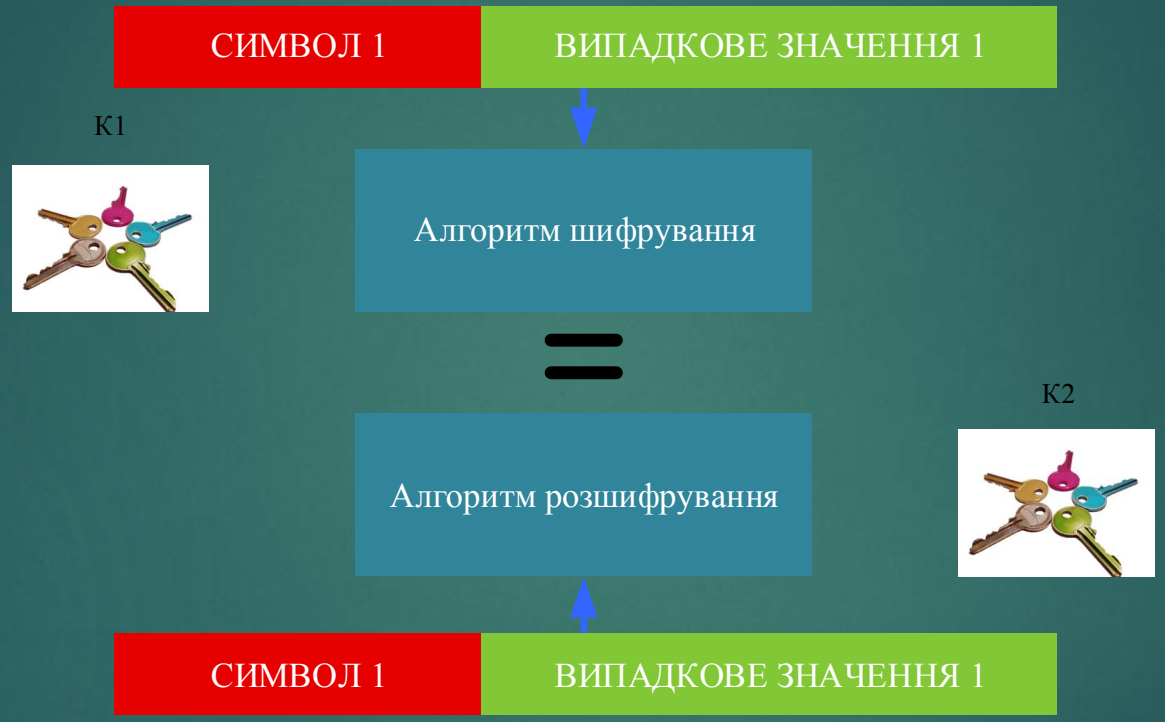
=

Алгоритм розшифрування

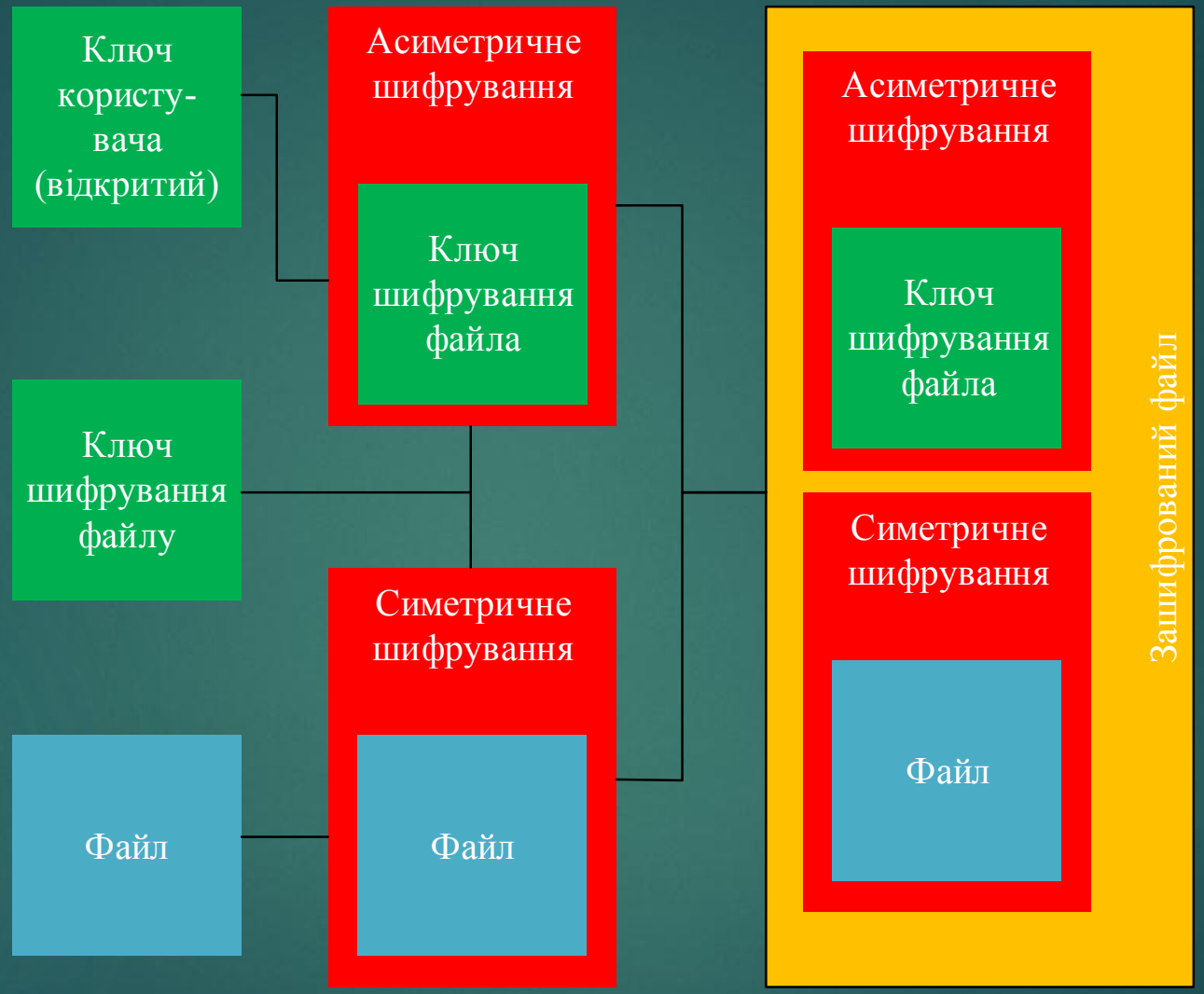
K2

ПОВІДОМЛЕННЯ 2 (M2)

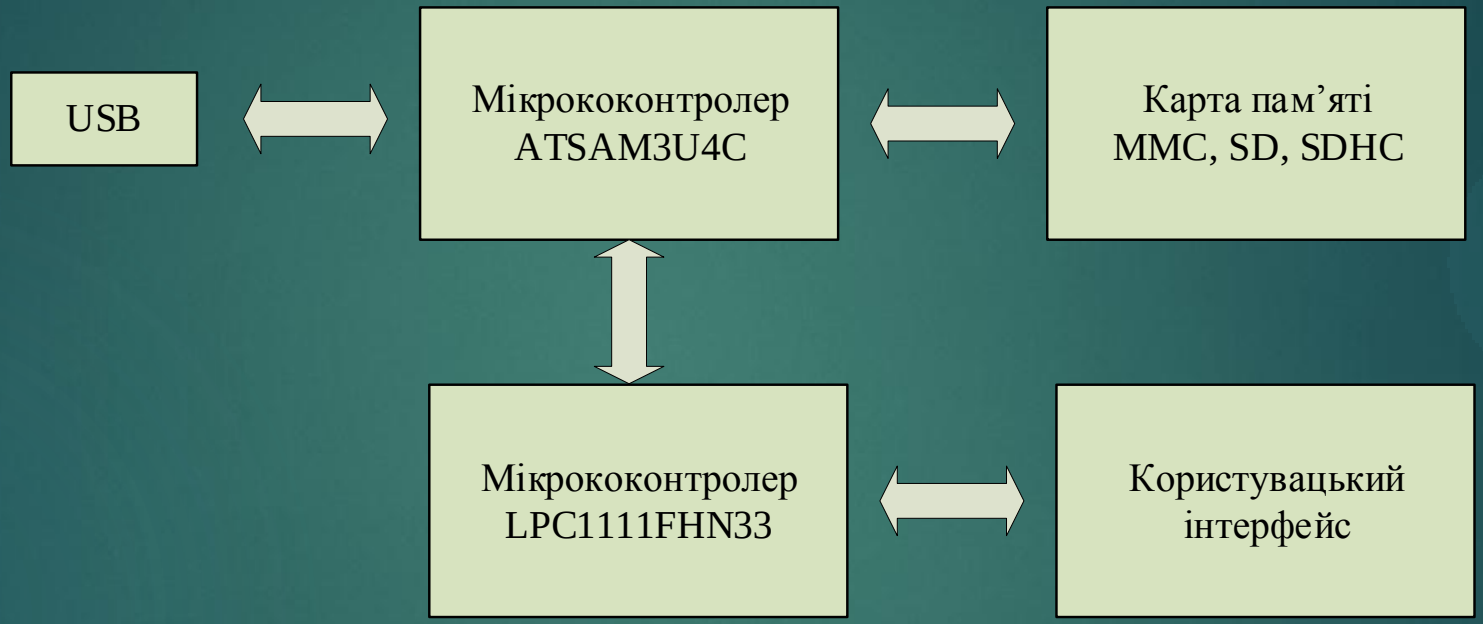
Алгоритм захисного перетворення з використанням складних операцій



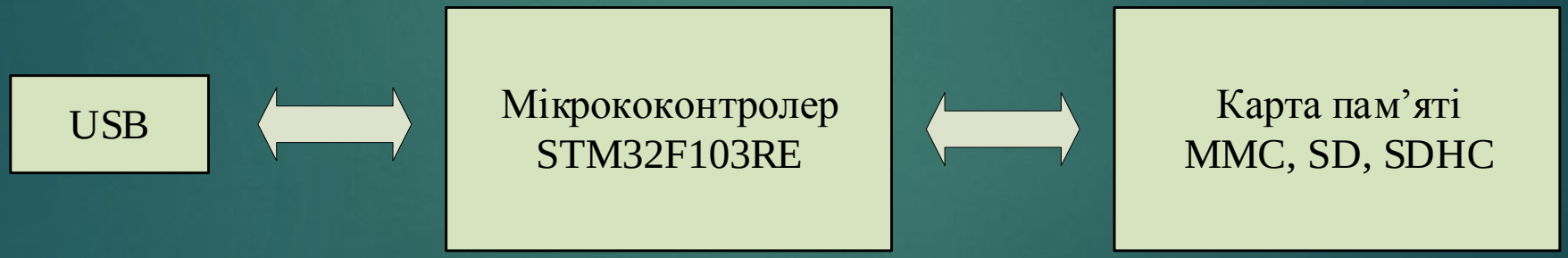
Алгоритм захисного перетворення на базі блокового шифрування



Алгоритм шифрування файлу в файловій системі EFS



Структурная схема стенду криптографічного сховища інформації



Структурна схема пристрою ідентифікації

Дякую за увагу