



**Особистий та відкритий
ключі. Сертифікат
відкритого ключа OSC-
технології для
розпізнавання паперових
документів**

Дізнаєтесь:



що таке відкритий ключ



що таке особистий ключ



ознайомитися з сертифікатом відкритого
ключа



що таке OCR-технології для розпізнавання
паперових документів



Ключі

Ключ - параметр криптографічної системи, який використовується для шифрування і/або дешифрування повідомлення при шифруванні; накладення та перевірки коду автентифікації повідомлень або електронний цифрового підпису

У асиметричних криптосистемах ключі зазвичай створюються парами: **ключ шифрування**, та **ключ дешифрування**. Якщо знаючи один можна легко отримати інший, та навпаки, то криптосистема називається шифруванням з симетричними ключами

Якщо ж з одного можна отримати інший, але навпаки дуже важко, то така система називається шифруванням з несиметричними ключами

Ключі

Відкритий ключ - ключ, котрий дозволяється передавати по відкритому каналу зв'язку, а таємний ключ - мусить зберігатися таємно, або передаватися з використанням закритого каналу зв'язку

Сеансовий ключ - ключ, що використовується під час сеансу обміну повідомленнями для захисту каналу зв'язку



Ключі



Час його дії ключа має минати автоматично, подібно дозвільним документам, оскільки:

- **чим довше використовується ключ, тим більша ймовірність його компрометації;**
- **чим довше використовується ключ, тим більші втрати при компрометації ключа;**
- **чим довше використовується ключ, тим більша спокуса прикласти необхідні зусилля для його розкриття;**
- **у низці випадків трудомісткість криптоаналізу визначається кількістю шифротекстів, отриманих у результаті шифрування одним ключем**

Класифікація ключів



За типом криптосистеми:

- Симетрична (симетричні ключі)
- Несиметрична (особистий (таємний) ключ та відкритий ключ)

За призначенням:

- Системи шифрування (ключі шифрування, ключі дешифрування, вектори ініціалізації)
- Системи автентифікації (ключі печаток (MAC), ключі підпису, ключі перевірки підпису)

Класифікація ключів



За ієрархією:

- Головні ключі
- Ключі шифрування ключів
- Транспортні ключі
- Ключі даних

За часом використання:

- Короткострокові ключі
- Довгострокові ключі

Ключі



Генерація **ключів** повинна здійснюватись апаратними генераторами випадкових чисел або стійкими генераторами псевдовипадкових чисел криптографічно

Ключі повинні **зберігатись і використовуватись** у апаратних криптографічних модулях, смарт-картках та токенах, які не дозволяють експорт ключа у незашифрованому вигляді

Після виведення з дії ключі повинні знищуватись способом, який не допускає їх відновлення. Найнадійнішим способом є знищення носія ключів

Ключі



Для забезпечення безпеки і виключення підміни відкритих ключів Центр «Україна» проводить сертифікацію відкритих ключів ЕП шляхом підписання відкритого ключа користувача своїм секретним ключем - ключем Центру

Власнику ключа ЕП видається сертифікат відкритого ключа, який містить такі відомості:

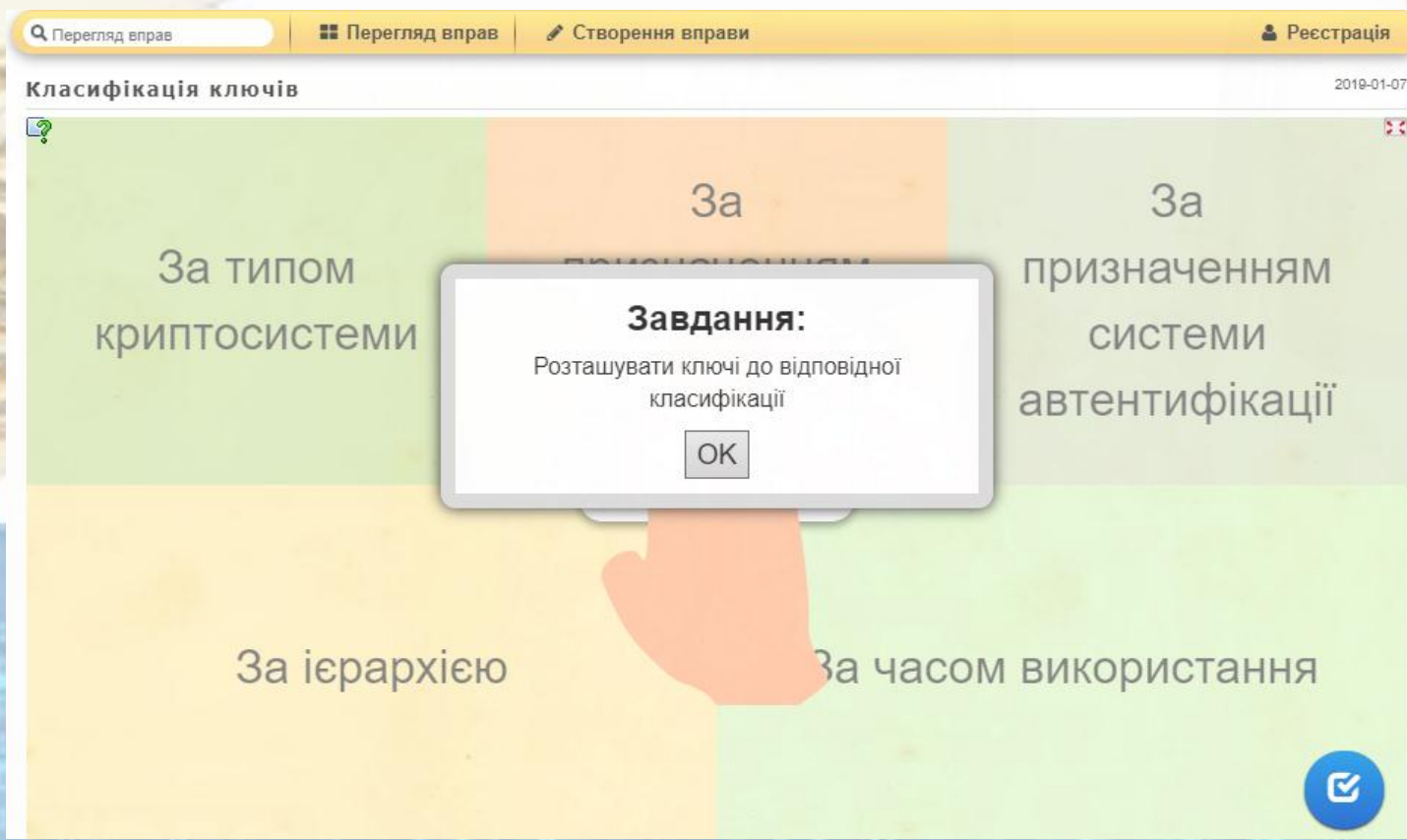
- відкритий ключ ЕП;
- ім'я власника, інші ідентифікуючі дані;
- терміни дії ключа;
- унікальний номер сертифіката відкритого ключа ЕП;
- найменування центру, який видав сертифікат

Відпрацьовуємо навички

Завдання 1.

Виконати завдання за посиланням

<https://learningapps.org/display?v=pr34c4owk19>



The screenshot displays a web application interface for a task titled "Класифікація ключів" (Classification of keys). The interface includes a top navigation bar with options: "Перегляд вправ" (View exercises), "Створення вправи" (Create exercise), and "Реєстрація" (Registration). The main content area is divided into four colored quadrants, each representing a classification criterion: "За типом криптосистеми" (By type of cryptosystem) in green, "За призначенням" (By purpose) in orange, "За часом використання" (By time of use) in light green, and "За ієрархією" (By hierarchy) in yellow. A central modal window with the title "Завдання:" (Task:) contains the instruction "Розташувати ключі до відповідної класифікації" (Arrange keys to the corresponding classification) and an "OK" button. A hand cursor is visible over the bottom quadrants. The date "2019-01-07" is shown in the top right corner of the application area.