

Навчально-науковий інститут інформаційних технологій  
Харківський національний економічний університет  
імені Семена Кузнеця

Звіт  
З Виконання лабораторної роботи №1  
за дисципліною: “Безпека банківських систем”  
на тему: “СИСТЕМА КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ  
«ШИФР-Х.509»”

Виконав: студент кафедри  
Кібербезпеки та інформаційних  
технологій

4 курсу, спец. Кібербезпека,  
групи 6.04.125.010.21.2

Бойко Вадим Віталійович

Перевірив:  
Лимаренко Вячеслав Володимирович

ХНЕУ ім. С. Кузнеця

2024

Мета: ознайомитися з системою криптографічного захисту інформації «Шифр-Х.509» (СКЗІ «Шифр-Х.509»), що призначена для створення РКІ (створення центрів сертифікації ключів (ЦСК), у тому числі кваліфікованих надавачів електронних довірчих послуг (КНЕДП), центрів реєстрації (ЦР) у рамках відповідності ЦСК, наданих користувачам засобів управління ключами), забезпечення послугами кваліфікованого електронного підпису (КЕП) органів державної влади, місцевого самоврядування, підприємств, установ та організацій будь-якої форми власності, фізичних осіб, отримати власний КЕП та виконати на практиці електронний підпис документу.

Завдання:

1. Виконати дослідження принципу роботи та алгоритму роботи шифруХ.509.
2. По результатам виконання п.1 скласти звіт (не менше 4 сторінок).
3. Отримати власний КЕП за допомогою застосунку «ДІЯ» або сервісу «ПриватБанку».
4. Виконати накладання власного КЕП на файл звіту лабораторної роботи.

Для цього використати один з сервісів:

- a. <https://id.gov.ua/>
  - b. <https://czo.gov.ua/>
  - c. <https://ca.dia.gov.ua>.
5. Отримати файл, що підписано, в форматі «CAdES. Дані та підпис зберігаються в CMS файлі (\*.p7s)».
  6. Файл з підписом завантажити до ПНС.

Контрольні питання:

1. Поняття цифрового підпису, вимоги до нього.
2. Класифікація схем цифрового підпису. Основні алгоритми (стандарти) ЕЦП.
3. Алгоритм роботи шифру-Х.509.
4. Призначення центрів сертифікації ключів.

## Виконання завдання №1

Виконю дослідження принципу роботи та алгоритму роботи шифру X.509.

Спочатку теоретичні відомості

Система криптографічного захисту інформації «Шифр-X.509» (СКЗІ «Шифр-X.509») призначена для створення інфраструктури відкритих ключів (створення центрів сертифікації ключів, у тому числі акредитованих, центрів реєстрації у рамках відповідності центрів сертифікації, наданих користувачам засобів управління ключами), забезпечення послугами електронного підпису органів державної влади, місцевого самоврядування, підприємств, установ та організацій будь-якої форми власності, а також фізичних осіб.

Система криптографічного захисту інформації «Шифр-X.509» має чинний експертний висновок в області криптографічного захисту інформації, наданий Державною службою спеціального зв'язку та захисту інформації України.

Поля сертифікату:

Поля для першої версії:

Назва	Опис
Версія	Ціле число, яке означає версію сертифікату
Серійний номер	Ціле унікальне число, для кожного сертифікату
Сигнатура	Ідентифікатор алгоритму шифрування
Хто видав сертифікат	Ім'я хто видав сертифікат
Срок дії	Час, доки сертифікат є валідним
Тема	Ім'я суб'єкту сертифікату

Інформація стосовно відкритого ключа	Відкритий ключ
--------------------------------------	----------------

Поля для другої версії мають ті самі, що й в першій версії, єдине додали

Назва	Опис
Унікальний ідентифікатор видавництва сертифікату	Ідентифікатор виданий центром сертифікації
Унікальний ідентифікатор суб'єкту	Ідентифікатор суб'єкту

Поля для третьої версії мають поля для другої версії та додали можливість розширення сертифікату

Назва	Опис
Розширення	Колекція стандартних розширень для сертифікатів для інтернету

Стосовно роботи X.509, є наступне:

1. Центр сертифікації (ЦС):
  - а. Це довірена організація, яка видає, оновлює та анулює цифрові сертифікати.
  - б. ЦС має свою пару ключів: приватний (для підпису сертифікатів) та публічний (для перевірки підписів).
  - с. Приклад ЦС: Let's Encrypt, DigiCert, Comodo.
2. Цифровий сертифікат:
  - а. Це електронний документ, який містить:
    - i. Вашу інформацію (ім'я, організацію, країну тощо).
    - ii. Ваш публічний ключ, який використовується для шифрування даних, що відправляються вам.

- iii. Підпис ЦС, який підтверджує, що саме ЦС видав цей сертифікат.
- iv. Іншу додаткову інформацію (наприклад, період дії сертифіката).

3. Процес перевірки:

- a. Коли ви підключаєтесь до веб-сайту, ваш браузер отримує сертифікат цього сайту.
- b. Браузер перевіряє підпис ЦС на сертифікаті, використовуючи публічний ключ ЦС.
- c. Якщо підпис дійсний, браузер вважає, що сертифікат справжній, а отже, ви підключилися саме до того сайту, який хотіли.
- d. Далі браузер використовує публічний ключ сайту (з сертифіката) для шифрування даних, які ви відправляєте на сайт, і дешифрування даних, які сайт відправляє вам.

Цей стандарт потрібен для:

- 1. Безпечне з'єднання: Забезпечує шифрування даних під час передачі по мережі, захищаючи їх від перехоплення.
- 2. Аутентифікація: Підтверджує, що ви дійсно спілкуєтесь з тим сайтом або сервісом, який стверджуєте.
- 3. Цілісність даних: Захищає дані від несанкціонованих змін під час передачі.

Цей стандарт використовується в наступних речах:

- 1. HTTPS: Протокол для безпечного з'єднання в Інтернеті.
- 2. VPN: Віртуальні приватні мережі для захищеного підключення до корпоративних мереж.
- 3. Електронний підпис: Для підтвердження авторства та цілісності документів.

4. Шифрування електронної пошти: Для захисту вмісту електронних листів.

Важливі поняття пов'язані із стандартом шифрування:

1. Публічний ключ: Відкрита частина криптографічної пари ключів, яка використовується для шифрування даних.
2. Приватний ключ: Закрита частина криптографічної пари ключів, яка використовується для дешифрування даних і створення цифрових підписів.
3. Цифровий підпис: Криптографічний засіб для підтвердження авторства і цілісності даних.
4. Центр сертифікації (ЦС): Довірена третя сторона, яка видає цифрові сертифікати.
5. Сертифікат: Електронний документ, який містить інформацію про власника і його публічний ключ.
6. CRL (Certificate Revocation List): Список анульованих сертифікатів.

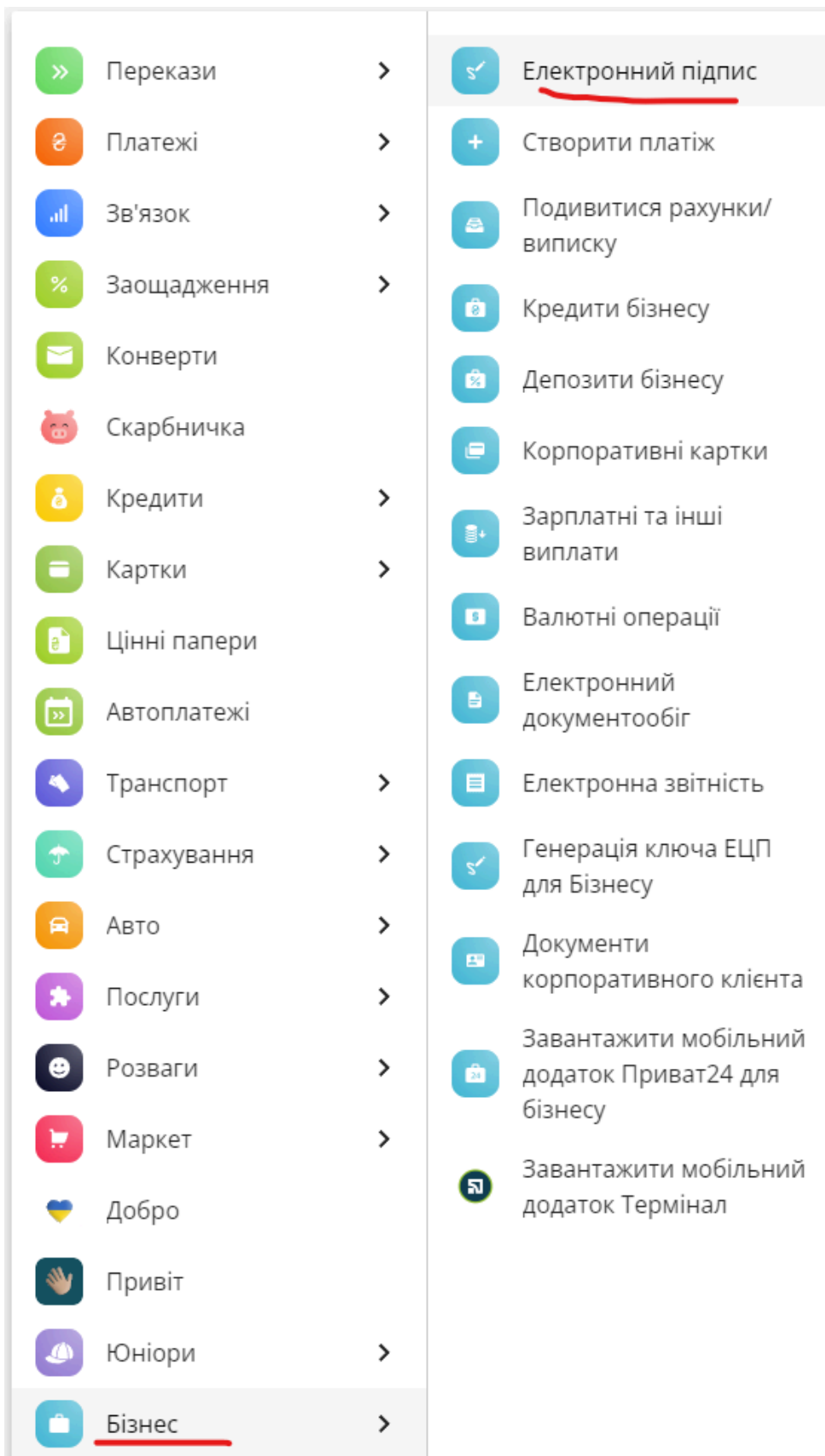
Висновок:

Х.509 відіграє важливу роль у забезпеченні безпеки в сучасному цифровому світі. Розуміння принципів роботи цього стандарту є необхідним для будь-кого, хто працює з мережевою безпекою. Однак важливо пам'ятати, що Х.509 – це не єдина технологія, яка використовується для забезпечення безпеки. Постійний розвиток технологій вимагає постійного оновлення знань і адаптації до нових загроз.

### Завдання № 3

Для створення ключа відкрию сайт приват банку

Після авторизації в меню оберу “Бізнес” та “Електронний підпис”



Далі відкриється нове вікно, де я підтверджую, що я, це я

**Дані для отримання сертифікату**

П.І.Б.	БОЙКО ВАДИМ ВІТАЛІЙОВИЧ
Населений пункт	ХАРКІВ
Область	ХАРКІВСЬКА

Ні, актуалізувати

Так, дані вірні

Й вигадаю пароль для сертифікату

**Вигадайте пароль для сховища ключів**

Мінімальна довжина пароля 8 символів, символи латинського алфавіту і цифри, пароль не повинен містити спеціальних символів

Вигадайте пароль до сховища ключів

Повторіть пароль до сховища ключів

☒ Підписати договір про надання електронних довірчих послуг та розписку про отримання сертифікату

< Назад

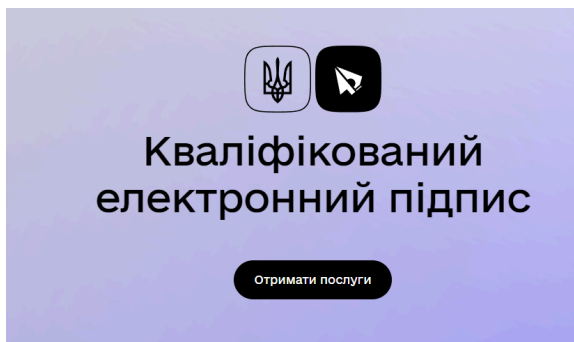
Далі >

Й завантажую ключ

Завдання № 4

Перейду на портал Дія для роботи з підписами

Для цього натискаю на “Отримати послугу”





Й обираю підписати документ

Придбати сертифікат

Підписати документ

Оновити сертифікат

Перевірити підпис

Знайти сертифікат

Даоі обираю Рідписати файл за допомогою електронного підпису

# Підписати документ

## Підписати файл за допомогою

---

Електронного підпису →

---

Дія.Підпис - UA →

---

Дія.Підпис - EU →

---

Версія від 2024.04.15 13:00

Й заповню поля, спочатку для ключа

# Підписати документ

Крок 1 з 4

## Зчитайте ключ

Файловий    Токен    Хмарний

Що таке файловий носій?

Кваліфікований надавач електронних довірчих послуг

Визначити автоматично

pb\_3721302355.jks

[Змінити](#)

Ім'я ключа

pb\_sign\_3721302355(БОЙКО ВАДИМ ВІТАЛІЙОВИЧ)

Пароль захисту ключа

Назад

Зчитати

Версія від 2024.04.15 13:00

Післязчитування можу перевірити дані

# Підписати документ

Крок 2 з 4

## Перевірте дані

Що таке сертифікат?

БОЙКО ВАДИМ ВІТАЛІЙОВИЧ

Організація  
ФІЗИЧНА ОСОБА  
РНОКПП  
3721302355

### Сертифікати

📄 ЕЦП (ДСТУ 4145), Неспростовність (ДСТУ 4145) ⬇  
EU-5E984D526F82F38F0400000003B23E0110057505.cer

📄 Протоколи розподілу ключів (ДСТУ 4145) ⬇  
EU-5E984D526F82F38F0400000003B23E0110057505.cer

Назад

Далі

Далі обираю тип підписання документів

# Підписати документ

Крок 4 з 4

## Підписати та зберегти

Виберіть, в якому форматі підписати документ

- ☐ XAdES. Дані та підпис зберігаються в XML файлі (\*.xml)
- ☐ PAdES. Дані та підпис зберігаються в PDF файлі (\*.pdf)
- ☒ CAdES. Дані та підпис зберігаються в CMS файлі (\*.p7s)
- NEW!

☐ ASIC. Дані та підпис зберігаються в архіві
  - ☐ ASIC-E. Дані та підпис зберігаються в архіві (розширений формат)
  - ☐ ASIC-S. Дані та підпис зберігаються в архіві (простий формат)

Алгоритм підпису

ДСТУ 4145

Тип підпису

Підпис та дані в одному файлі (enveloped)

Формат підпису

CAdES-X Long – Довгостроковий з повними даними Ц...

Перетягніть сюди файл(и)  
для підпису  
або завантажте його зі свого  
носія  
(doc, pdf, docx та інші)

Й натискаю підписати

Формат підпису

CAdES-X Long – Довгостроковий з повними даними Ц...▼

Файл(и) для підпису:

• ЛР 1 Бойко.txt


[Змінити](#)

Підписати


Назад

Версія від 2024.04.15 13:00

Йнатисну на зберегти файл з підписом


Документ підписано

⬇ Завантажити все архівом

Файл з підписом

ЛР 1 Бойко.txt.p7s

17.3 КБ



Відповіді на контрольні питання:

1. Поняття цифрового підпису, вимоги до нього

а. Цифровий підпис - дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних

б. Вимоги до цифрового підпису

Відповідно до закону України “Про електронний цифровий підпис”, Вимоги до сертифіката ключа, наступні:

і. Сертифікат ключа містить такі обов'язкові дані:

1. найменування та реквізити центру сертифікації ключів (центрального засвідчувального органу, засвідчувального центру);
2. зазначення, що сертифікат виданий в Україні;
3. унікальний реєстраційний номер сертифіката ключа;
4. основні дані (реквізити) підписувача - власника особистого ключа;
5. дату і час початку та закінчення строку чинності сертифіката;
6. відкритий ключ;
7. найменування криптографічного алгоритму, що використовується власником особистого ключа;
8. інформацію про обмеження використання підпису.

іі. Посилений сертифікат ключа, крім обов'язкових даних, які містяться в сертифікаті ключа, повинен мати ознаку посиленого сертифіката ключа.

ііі. Інші дані можуть вноситися у посилений сертифікат ключа на вимогу його власника.

2. Класифікація схем цифрового підпису. Основні алгоритми (стандарти) ЕЦП.

а. Класифікація схем цифрового підпису:

- i. За способом підтвердження:
    - 1. Прямі схеми: Підпис однозначно пов'язаний з документом і підписувачем.
    - 2. Схеми з відновленням документа: Підпис дозволяє відновити частину або весь документ.
  - ii. За криптографічними примітивами:
    - 1. Засновані на хеш-функціях: Використовують хеш-функції для створення відбитка документа, який потім підписується.
    - 2. Засновані на асиметричній криптографії: Використовують пари ключів (відкритий і закритий) для підписання та перевірки підпису.
  - iii. За рівнем безпеки:
    - 1. Безпечні при атаках з відомим відкритим ключем: Зловмисник не може підробити підпис, знаючи лише відкритий ключ.
    - 2. Безпечні при атаках з вибором повідомлення: Зловмисник не може підробити підпис для довільного повідомлення, навіть якщо він може вибрати повідомлення, які будуть підписані.
  - iv. За іншими критеріями:
    - 1. Детерміновані та імовірнісні: Детерміновані схеми завжди видають один і той же підпис для одного і того ж документа, імовірнісні – можуть видавати різні підписи.
    - 2. Одноразові та багаторазові: Одноразові схеми дозволяють підписати документ лише один раз, багаторазові – можуть бути використані багаторазово.
- b. Основні алгоритми (стандарти) ЕЦП:

- i. RSA: Один з найстаріших і найвідоміших алгоритмів, заснований на проблемі факторизації великих чисел.
- ii. DSA (Digital Signature Algorithm): Стандартний алгоритм цифрового підпису, розроблений NIST. Заснований на проблемі дискретного логарифмування в скінченному полі.
- iii. ECDSA (Elliptic Curve Digital Signature Algorithm): Аналог DSA, але використовує еліптичні криві. Забезпечує більш високий рівень безпеки при меншій довжині ключа.
- iv. EdDSA (Edwards-Curve Digital Signature Algorithm): Сучасний алгоритм, заснований на еліптичних кривих Edwards. Відрізняється високою швидкістю і простотою реалізації.
- v. Sm2: Китайський національний стандарт цифрового підпису, заснований на еліптичних кривих.

### 3. Алгоритм роботи шифру-X.509:

- a. X.509 використовується в шифруванні для:
  - i. Генерація ключів: Кожен учасник комунікації створює пару ключів: відкритий (публічний) та закритий (приватний).
  - ii. Створення сертифіката: Центр сертифікації (ЦС) перевіряє особу власника ключа і створює цифровий сертифікат. У цьому сертифікаті міститься:
    - 1. Відкритий ключ власника
    - 2. Інформація про власника
    - 3. Термін дії сертифікату
    - 4. Цифровий підпис ЦС
  - iii. Обмін сертифікатами: Учасники обмінюються своїми сертифікатами.
  - iv. Шифрування та підпис:
    - 1. Шифрування: Відправник шифрує повідомлення за допомогою відкритого ключа одержувача. Тільки

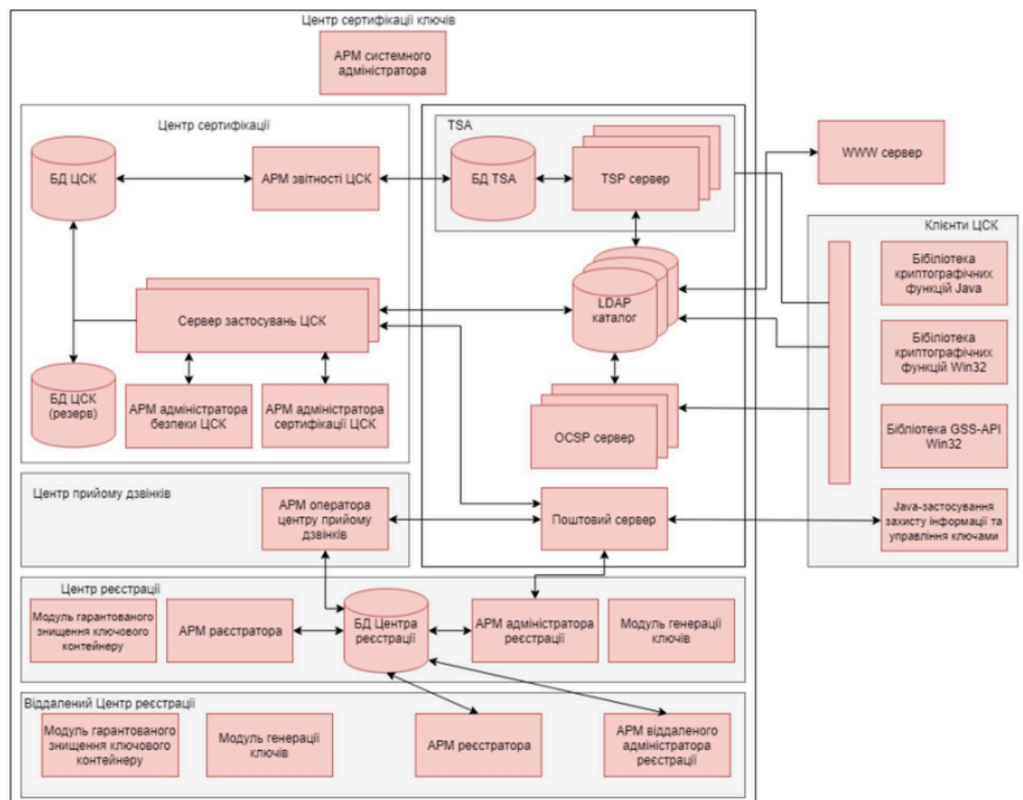


власник відповідного закритого ключа може розшифрувати це повідомлення.

2. Цифровий підпис: Відправник створює цифровий підпис повідомлення за допомогою свого закритого ключа. Цей підпис додається до зашифрованого повідомлення.

v. Перевірка підпису: Одержувач розшифровує повідомлення за допомогою свого закритого ключа і перевіряє цифровий підпис за допомогою відкритого ключа відправника (отриманого з сертифіката). Якщо підпис правильний, то одержувач впевнений, що повідомлення було відправлено саме цим відправником і не було підроблено.

Функціональна схема роботи СКЗІ «Шифр-Х.509»:



#### 4. Призначення центрів сертифікації ключів:

Центр сертифікації ключів (ЦСК) або надавач електронних довірчих послуг (ЕДП) – це інформаційно-комунікаційна система (ІКС), яка призначена для обслуговування сертифікатів та надання інших послуг (електронного підпису (ЕП), фіксування часу та ін.)

##### а. ЦСК (надавач ЕДП) забезпечує:

- i. обслуговування сертифікатів відкритих ключів (далі – сертифікатів) користувачів, що включає:
- ii. реєстрацію користувачів;
- iii. сертифікацію відкритих ключів користувачів;
- iv. розповсюдження сертифікатів через інформаційний ресурс;
- v. управління статусом сертифікатів
- vi. розповсюдження інформації про статус сертифікатів;
- vii. надання послуг фіксування часу;
- viii. надання користувачам засобів ЕП та шифрування даних, а також засобів генерації та управління ключами.