ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ
УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

Лабораторна робота №1

з курсу «Безпека банківських систем»

СИСТЕМА КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ «ШИФР-Х.509»

Харків 2023

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.

1 ТЕОРЕТИЧНІ ВІДОМОСТІ

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

Система криптографічного захисту інформації «Шифр-Х.509» версія 2 має чинний експертний висновок в області криптографічного захисту інформації, наданий Державною службою спеціального зв’язку та захисту інформації України.

ЦСК «Шифр-Х.509» сумісний з іншими ЦСК, які реалізують стандарти сімейства Х.509, на рівні:

«Про встановлення вимог до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання електронних довірчих послуг», затверджених наказом Міністерством юстиції України та Адміністрацією Державної служби спеціального зв'язку та захисту інформації України від 18.11.2019 № 3563/5/610.

«Про порядок обчислення геш-значення». Лист Міністерства юстиції України від 15.10.2012 г. №12776-026-12-133.

Система «Шифр-Х.509» успішно інтегрується з наступними системами:

– eFOUR, iFOBS, B2, EMOS;

– Nimbus;

– IB Pentagy;

– ProFIX/Bank;

– Ensemble.

Шифр-Х.509 підтримує роботу із захищеними ключовими носіями за інтерфейсом PKCS#11.

№	Виробник	Модель	Тип
1	ТОВ Автор, Україна	Author Secure Token-337	Token
2	ТОВ Автор, Україна	Author Secure SmartCard-336	SmartCard
3	ТОВ Мікрокрипт, Україна	Armorino	Token + Flash
4	Giesecke & Devrient, Німеччина	StarSign Crypto USB Token	Token, Token + Flash
5	Giesecke & Devrient, Germany	StarSign Crypto SmartCard	SmartCard
6	Технотрейд, Україна	uaToken	Token
7	ТОВ Авест Україна, Україна	Avest UA	Token
8	SafeNet, США	SafeNet Crypto eToken	Token
9	Gemalto, США	Gemalto ID Prime Series	Token, SmartCard

ЦСК є головним елементом СКЗІ «Шифр-Х.509», який здійснює управління ключами, видачу та відкликання сертифікатів, формування та видачу списків відкликаних сертифікатів.

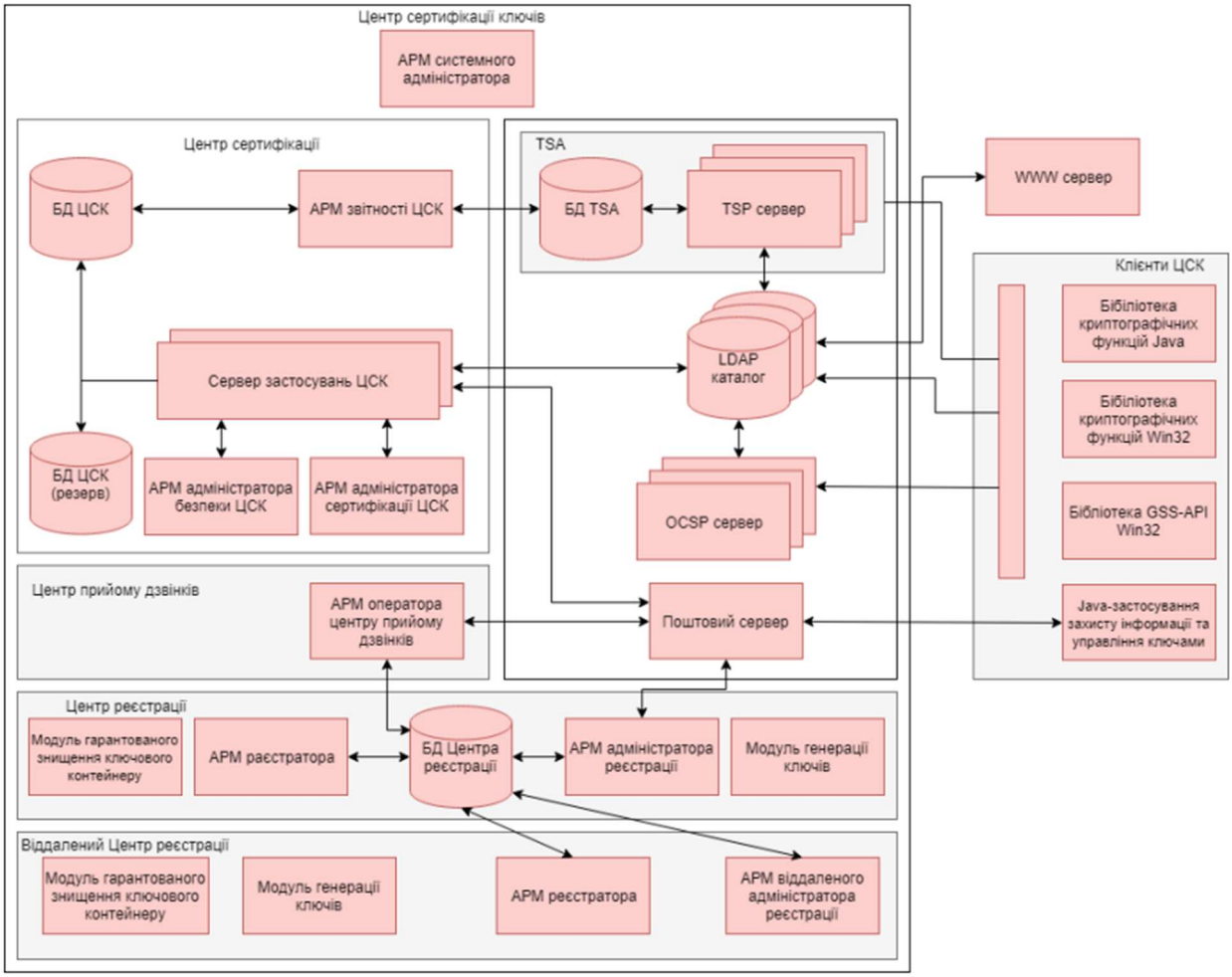

Рисунок 1.1 – Функціональна схема роботи СКЗІ «Шифр-Х.509»

Складові елементи є:

– Сервер застосувань

– АРМ Адміністратора безпеки та аудиту

– АРМ Адміністратора сертифікації

– Поштовий модуль ЦСК

– БД ЦСК

Програмні засоби центру реєстрації мають ідентифікувати, зареєструвати користувача для одержання сертифікату та надання послуг з генерації ключів користувачам, які хочуть одержати послугу безпосередньо в Центрі реєстрації (ЦР).

Засоби ЦР складаються з наступних програмних засобів:

– АРМ адміністратора реєстрації;

– АРМ реєстратора (оператора реєстрації);

– Комунікаційний модуль ЦР;

– БД ЦР;

– АРМ оператора ЦПД;

– АРМ віддаленого адміністратора реєстрації;

– Модуль генерації ключів;

– Модуль гарантованого знищення ключового контейнера;

– Модуль імпорту запитів у форматі PKCS#10;

– Довідник сертифікатів на базі LDAP-сервера.

Основними функціями ЦР є наступними [20]:

– Розмежування доступу до функцій та даних ЦР;

– Управління ключами адміністратора реєстрації;

– Управління ключами операторами реєстрації;

– Управління ключами оператора ЦПД;

– Управління ключами віддаленого адміністратора реєстрації;

– Ідентифікація та реєстрація користувачів;

– Видача стартових сертифікатів користувачів;

– Генерація робочих ключів для користувачів, які хочуть одержати робочі сертифікати безпосередньо в ЦР, формування запитів на сертифікати;

– Гарантоване знищення ключового контейнера, як на файловому носії, так і на носії ключової інформації;

– Прийом та перевірка автентичності запитів на сертифікати користувачів;

– Прийом та перевірка автентичності запитів на блокування/відновлення/скасування сертифікатів користувачів;

– Засвідчення запитів на сертифікати користувачів за підписом оператора реєстрації;

– Засвідчення запитів на сертифікати користувачів за підписом адміністратора реєстрації;

– Засвідчення запитів на блокування/відновлення/скасування сертифікатів користувачів за підписом адміністратора реєстрації;

– Засвідчення запитів на сертифікати користувачів за підписом віддаленого адміністратора реєстрації;

– Засвідчення запитів на блокування/відновлення/скасування сертифікатів користувачів за підписом віддаленого адміністратора реєстрації;

– Засвідчення запитів на блокування/відновлення/скасування сертифікатів користувачів за підписом оператора ЦПД;

– Передача запитів на сертифікати до ЦСК електронною поштою чи експорт в заданий каталог у вигляді файлу чи на носій ключової інформації;

– Передача запитів на блокування/відновлення/скасування сертифікатів в ЦСК електронною поштою чи експорту заданий каталог у вигляді файлу чи на носій ключової інформації;

– Прийом та контроль автентичності сертифікатів користувачів та СВС;

– Видача сертифікатів користувачам, які забажали отримати їх безпосередньо на ЦР чи віддаленому ЦР;

– Передача сертифікатів та СВС на адресу користувача, який генерує свої ключі самостійно;

– Введення та аудит локальної БД сертифікатів ЦР чи віддаленого ЦР, а також запитів на сертифікат та запитів на відкликання сертифікатів;

– Управління локальним довідником сертифікатів: розміщення, видалення сертифікатів у LDAP-каталозі.

Вся функціональність по роботі з сертифікатами, списком відкликаних сертифікатами, КЕП та електронними позначками часу реалізується у бібліотеках функції реєстрації та сертифікації. Для інтеграції в інші системи документообігу та захисту даних, дані бібліотеки надаються для наступних платформ: Win32, JRE, Android OS.

3 ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

1. Виконати дослідження принципу роботи та алгоритму роботи шифру-Х.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:

– *https://id.gov.ua/*

– *https://czo.gov.ua/*

– *https://ca.diia.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.