

ЗАТВЕРДЖЕНО
ЄААД.468244.185-ЛУ

Інв. № орг.	
Підп. та дата	
Взам. інв. №	
Інв. № дубл	
Підп. та дата	

Центр сертифікації ключів ринку електричної енергії

Програма та методика попередніх випробовувань

ЄААД.468244.185.ПМ.01

2014 р.

ЗМІСТ

1 ОБ'ЄКТ ВИПРОБОВУВАНЬ	4
2 МЕТА ВИПРОБОВУВАНЬ	4
3 ЗАГАЛЬНІ ВІДОМОСТІ.....	4
3.1 Місце проведення випробовувань.....	4
4 ПРОГРАМА ВИПРОБУВАНЬ	5
4.1 Обсяг попередніх випробувань	5
4.2 Перелік етапів випробувань	5
4.3 Послідовність проведення та режими випробовувань.....	5
5 МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ВИПРОБОВУВАНЬ	7
6 ЗВІТНІСТЬ	8

ПЕРЕЛІК СКОРОЧЕНЬ

БД	- База даних
ЕОМ	- Електронно-обчислювальна машина
ЕЦП	- Електронний цифровий підпис
ІТС	- Інформаційно-телекомунікаційна система
КЗІ	- Криптографічний захист інформації
ЛОМ	- Локальна обчислювальна мережа
МЕ	- Міжмережний екран
ОС	- Операційна система
ПЗ	- Програмне забезпечення
ПТК	- Програмно-технічний комплекс
РС	- Робоча станція
СУБД	- Система управління базами даних
ЦСК	- Центр сертифікації ключів
HTTP	- Hyper Text Transfer Protocol
LDAP	- Lightweight Directory Access Protocol (протокол доступу до каталогу)
OCSP	- Online Certificate Status Protocol (протокол визначення статусу сертифіката)

1 ОБ'ЄКТ ВИПРОБОВУВАНЬ

Об'єктом випробовувань є програмно-технічний комплекс ЦСК ринку електричної енергії.

ПТК є технологічною основою ЦСК і призначений для реалізації регламентних процедур та механізмів обслуговування сертифікатів відкритих ключів користувачів ЦСК, надання послуг фіксування часу, надання користувачам засобів ЕЦП та шифрування, а також засобів генерації особистих і відкритих ключів.

ПТК ЦСК утворює ЛОМ, до якої через загальнодоступні телекомунікаційні мережі підключаються користувачі ЦСК.

2 МЕТА ВИПРОБОВУВАНЬ

Метою випробовувань ПТК ЦСК є перевірка роботоспроможності ЦСК та готовності до прийняття її у дослідну експлуатацію.

Випробовування проводяться також з метою опрацювання технічних та програмних засобів ПТК, технологічних та організаційних заходів щодо виконання ПТК регламентних процедур та механізмів роботи ЦСК з надання послуг ЕЦП користувачам ЦСК. Зокрема, опрацювання:

- 1) обслуговування сертифікатів відкритих ключів (далі - сертифікатів) користувачів, що включає:
 - реєстрацію користувачів;
 - сертифікацію відкритих ключів користувачів;
 - розповсюдження сертифікатів;
 - управління статусом сертифікатів та розповсюдження інформації про статус сертифікатів.
- 2) надання послуг фіксування часу;
- 3) надання користувачам та застосування:
 - засобів генерації особистих і відкритих ключів;
 - засобів ЕЦП та шифрування даних.

Зазначені регламентні процедури повинні перевірятися у взаємодії з користувачами ЦСК з використанням загальнодоступних телекомунікаційних каналів або у режимі імітації віддаленого доступу.

3 ЗАГАЛЬНІ ВІДОМОСТІ

3.1 Місце проведення випробовувань

Випробовування проводяться у приміщеннях ЦСК ринку електричної енергії (ДП "ЕНЕРГОРИНОК").

4 ПРОГРАМА ВИПРОБУВАНЬ

4.1 Обсяг попередніх випробувань

Обсяг попередніх випробувань визначається поставленою метою випробувань і включає проведення наступних перевірок :

- виконання вимог ТЗ щодо комплектності та якості документації, наданої на попередні випробування;
- виконання вимог ТЗ щодо функцій комплексу.

4.2 Перелік етапів випробувань

Випробовування ПТК ЦСК складається з:

- розгортання ПТК ЦСК;
- розгортання (імітація) ПТК відокремлених пунктів реєстрації;
- розгортання (імітація) технічних засобів користувачів ЦСК;
- опрацювання процедур ведення реєстру користувачів;
- опрацювання процедур формування сертифікатів відкритих ключів;
- опрацювання процедур розповсюдження інформації про статус сертифікатів;
- опрацювання процедур скасування, блокування та поновлення сертифікатів;
- опрацювання процедур доступу користувачів до електронних реєстрів сертифікатів та інформації про статус сертифікатів;
- опрацювання процедур резервного копіювання та архівування інформації;
- імітація роботи автоматичних сервісів із навантаженням.

4.3 Послідовність проведення та режими випробовувань

Послідовність та обсяг етапів проведення випробовувань наведені у табл. 4.1.

Таблиця 4.1

Етап дослідної експлуатації	Зміст та режим проведення
1 Розгортання ПТК ЦСК	1.1 Монтаж обладнання технічних засобів загального призначення (PC та серверів), комунікаційного обладнання та спеціальних апаратних засобів (КЗІ). 1.2 З'єднання технічних засобів у ЛОМ. 1.3 Інсталяція системного ПЗ (ОС, СУБД тощо) та функціональних програмних комплексів та засобів. 1.4 Налагодження системного та функціонального ПЗ. 1.5 Реєстрація адміністраторів реєстрації ЦСК. 1.6 Реєстрація серверів ЦСК. 1.7 Первинна організація ключової системи ЦСК - генерація ключів та формування сертифікатів ЦСК, серверів ЦСК та адміністраторів ЦСК. 1.8 Публікація сертифікатів ЦСК та серверів ЦСК на інформаційному ресурсі (web-сторінці та у LDAP-каталозі серверів взаємодії ЦСК) у ручному режимі з PC системного адміністратора. 1.9 Запуск всіх технічних засобів ПТК (серверів ЦСК, серверів взаємодії ЦСК та всіх PC) у штатний режим роботи. 1.10 Перевірка засобів синхронізації часу
2 Розгортання (імітація) технічних засобів користувачів ЦСК	3.1 Інсталяція програмних засобів користувачів ЦСК на PC та, за необхідністю, серверах користувачів ЦСК. 3.2 Налагодження програмних засобів користувачів ЦСК
3 Опрацювання процедур ведення реєстру користувачів	3.1 Реєстрація користувачів ЦСК та, за необхідністю, серверів користувачів ЦСК на PC адміністраторів реєстрації ЦСК. 3.2 Видалення та модифікація реєстраційних даних користувачів ЦСК та, за необхідністю, серверів користувачів ЦСК на PC адміністраторів реєстрації ЦСК.
4 Опрацювання процедур формування сертифікатів та публікації сертифікатів	4.1 Генерація ключів та формування запитів на формування сертифікатів користувачів ЦСК та, за необхідністю, серверів

на інформаційному ресурсі	користувачів ЦСК на відповідних технічних засобах користувачів. 4.2 Обробка запитів на формування сертифікатів користувачів ЦСК адміністраторами реєстрації ЦСК. 4.3 Публікація сертифікатів користувачів ЦСК на інформаційному ресурсі (web-сторінці та у LDAP-каталозі серверів взаємодії ЦСК) у ручному режимі з РС системного адміністратора та у автоматичному режимі засобами серверів ЦСК
5 Опрацювання процедур розповсюдження інформації про статус сертифікатів	5.1 Формування списків відкликаних сертифікатів (СВС) у ручному режимі з РС системного адміністратора та у автоматичному режимі засобами серверів ЦСК. 5.2 Публікація СВС у ручному режимі з РС системного адміністратора та у автоматичному режимі засобами серверів ЦСК
6 Опрацювання процедур скасування, блокування та поновлення сертифікатів	6.1 Формування та передача на обробку користувачами ЦСК запитів на блокування сертифікатів усіма можливими способами - через HTTP, електронну пошту та телефоном. 6.2 Формування адміністраторами реєстрації ЦСК запитів на скасування, блокування та поновлення сертифікатів користувачів ЦСК.
7 Опрацювання процедур доступу користувачів до електронних реєстрів сертифікатів та інформації про статус сертифікатів	7.1 Перевірка доступу користувачів до електронних реєстрів сертифікатів та інформації про статус сертифікатів - доступу до сертифікатів та СВС на web-сторінці і у LDAP-каталозі серверів взаємодії ЦСК. Перевірка завантаження та використання СВС засобами користувачів ЦСК. 7.2 Перевірка автоматизованого доступу до інформації про статус сертифікатів (роботи протоколу OCSP) засобами користувачів ЦСК
8 Опрацювання процедур резервного копіювання та архівування інформації	8.1 Виконання процедур реплікації БД серверів ЦСК. 8.2 Виконання процедур резервного копіювання БД серверів ЦСК. 8.3 Виконання процедур архівування БД серверів ЦСК. 8.4 Виконання процедур відновлення БД серверів ЦСК
9 Імітація роботи автоматичних сервісів із навантаженням	9.1 Перевірка роботи під навантаженням СМР-сервера. 9.2 Перевірка роботи під навантаженням OCSP-сервера. 9.3 Перевірка роботи під навантаженням TSP-сервера.

Результати перевірок вважаються позитивними, якщо результати нагляду за виконанням регламентних процедур окремих етапів відповідають функціональним характеристикам та експлуатаційній документації.

Результати перевірок вважаються негативними, якщо результати нагляду за виконанням регламентних процедур окремих етапів не відповідають функціональним характеристикам чи експлуатаційній документації.

Проведення окремих перевірок здійснюється згідно з експлуатаційною документацією на ПТК чи окремі програмні засоби і комплекси та технічні засоби.

5 МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ВИПРОБОВУВАНЬ

Проведення випробовувань здійснюється у автоматизованій системі на основі ПТК ЦСК, який включає до свого складу наступні технічні засоби:

- PC адміністратора безпеки;
- PC адміністратора сертифікації та системного;
- PC адміністратора реєстрації;
- центральні сервери ЦСК;
- сервери взаємодії;
- сервер моніторингу та синхронізації часу;
- комунікаційне обладнання (комутатор, комутатор PC, ME);
- PC генерації ключів користувачів.

При роботі ПТК з ним взаємодіють технічні засоби, які фізично не входять до його складу та імітуються PC чи серверами:

- технічні засоби користувачів ЦСК зовнішніх ІТС.

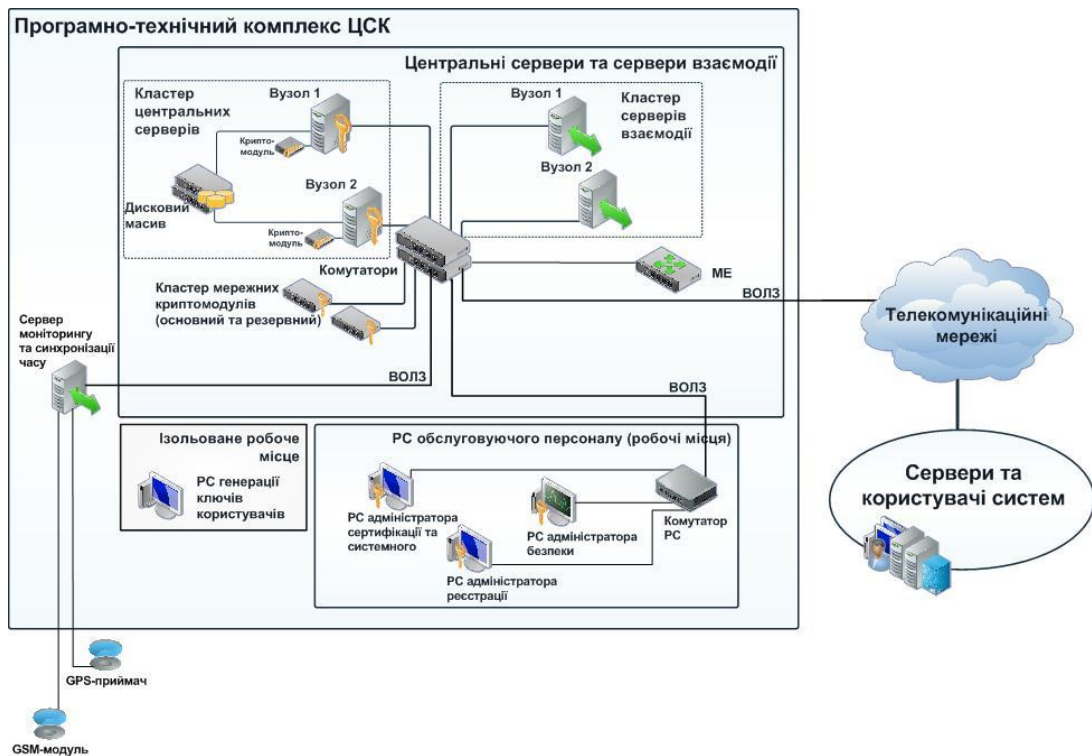


Рисунок 5.1 - Структурна схема ПТК ЦСК.

6 ЗВІТНІСТЬ

6.1 Результати попередніх випробувань ПТК в цілому оцінюються за результатами окремих видів перевірок, виконаних відповідно до розділу 4 даної програми. Результати випробувань не можуть вважатися позитивними, якщо не виконуються вимоги ТЗ.

6.2 Результати попередніх випробувань оформлюються протоколами, що складаються за результатами окремих видів перевірок, які підписуються і прикладаються до акту попередніх випробувань