

**ТЕХНІЧНЕ ЗАВДАННЯ**  
на створення  
автоматизованої системи центру сертифікації ключів  
ринку електричної енергії

ЄААД.468244.185 ТЗ.02

Шифр “ЦСК.ЕНЕРГОРИНОК”

2014 р.

**ЗМІСТ**

1 ЗАГАЛЬНІ ВІДОМОСТІ.....	4
2 ПРИЗНАЧЕННЯ ТА ЗАГАЛЬНІ ВИМОГИ ДО КОМПЛЕКСУ.....	5
3 ВИМОГИ ДО КОМПЛЕКСУ .....	6
3.1 Вимоги до функцій комплексу.....	6
3.2 Вимоги до структури та призначення комплексу технічних засобів .....	8
3.3 Вимоги до характеристик комплексу .....	11
3.4 Вимоги до режимів функціонування комплексу.....	11
3.5 Вимоги до експлуатації комплексу .....	12
3.6 Вимоги до персоналу, що відповідає за експлуатацію комплексу .....	13
3.7 Вимоги до комплексу технічних засобів.....	13
3.8 Додаткові вимоги .....	15
4 ПОРЯДОК СТВОРЕННЯ КОМПЛЕКСУ.....	20
5 ПОРЯДОК КОНТРОЛЮ ТА ПРИЙМАННЯ КОМПЛЕКСУ .....	21
6 ПОРЯДОК ПІДГОТОВКИ ДО ВВЕДЕННЯ КОМПЛЕКСУ В ДІЮ.....	22
7 ВИМОГИ ДО ДОКУМЕНТУВАННЯ.....	23

**ПЕРЕЛІК СКОРОЧЕНЬ**

ВОЛЗ	–	Волоконно-оптичні лінії зв'язку
ДБЖ	–	Джерело безперебійного живлення
ЕОМ	–	Електронно-обчислювальна машина
ЕЦП	–	Електронний цифровий підпис
ЗТМ	–	Зовнішні телекомунікаційні мережі
КЗЗ	–	Комплекс засобів захисту
КЗІ	–	Криптографічний захист інформації
КСЗІ	–	Комплексна система захисту інформації
ЛОМ	–	Локальна обчислювальна мережа
МЕ	–	Міжмережний екран
МКМ	–	Мережний криптомодуль
НКІ	–	Носій ключової інформації
НСД	–	Несанкціонований доступ
ПЕОМ	–	Персональна ЕОМ
ПК	–	Програмний комплекс
ПТК	–	Програмно-технічний комплекс
РС	–	Робоча станція
ТЗ	–	Технічне завдання
ТУ	–	Технічні умови
ЦСК	–	Центр сертифікації ключів
ЦЗО	–	Центральний засвідчувальний орган
СМР	–	Certificate Management Protocol (протокол управління обслуговуванням сертифікатів)
GPS	–	Global Positioning System (глобальна система позиціонування)
LDAP	–	Lightweight Directory Access Protocol (протокол доступу до каталогу)
OCSP	–	On-line Certificate Status Protocol (протокол визначення статусу сертифіката)
TSP	–	Time Stamp Protocol (протокол фіксування часу)

## 1 ЗАГАЛЬНІ ВІДОМОСТІ

1.1 Повна назва автоматизованої системи: програмно-технічний комплекс центру сертифікації ключів ринку електричної енергії (ЦСК) (далі – комплекс).

1.2 Шифр комплексу: “ЦСК.ЕНЕРГОРИНОК”.

1.3 Замовник: ДП "Енергоринок". Юридична адреса: 01032, м. Київ, вул. Симона Петлюри, 27. Код ЄДРПОУ: 21515381.

1.4 Виконавець: визначається за результатами тендерної процедури.

1.5 Розробка технічного завдання виконується у відповідності до договору № 2407 від 24.07.2014 р.

1.7 Результати робіт зі створення комплексу повинні оформлятися та пред'являтися згідно з порядком визначеним у п. 4, 5 та 7.

## **2 ПРИЗНАЧЕННЯ ТА ЗАГАЛЬНІ ВИМОГИ ДО КОМПЛЕКСУ**

2.1 Призначення комплексу: реалізація ЦСК регламентних процедур та механізмів обслуговування сертифікатів відкритих ключів користувачів (далі – користувачів), надання послуг фіксування часу, а також реалізація ЕЦП і шифрування даних та управління особистими ключами і сертифікатами відкритих ключів користувачів системи.

2.2 У комплексі може оброблятися відкрита інформація, інформація з обмеженим доступом, крім інформації, що становить державну таємницю, та службової інформації.

2.3 Захист інформації, яка обробляється у комплексі, повинен здійснюватися шляхом створення та забезпечення функціонування комплексної системи захисту інформації (КСЗІ) ЦСК.

2.4 Технічні засоби комплексу повинні бути об'єднані у ЛОМ з використанням внутрішньої телекомунікаційної мережі з підключенням частини засобів до зовнішніх телекомунікаційних мереж. Окремі технічні засоби комплексу можуть бути ізольовані від мереж передачі даних.

2.5 Реалізація регламентних процедур та механізмів обслуговування сертифікатів комплексу у складі ЦСК повинні відповідати вимогам правил посиленої сертифікації.

2.6 Комплекс повинен включати у своєму складі програмні засоби КЗІ (виду “Б”, підвид “Б2”, категорії “К”, “П” та “Ш”, класу В2), які можуть використовувати апаратні та апаратно-програмні засоби КЗІ (виду “Б”, підвид “Б2”, або виду “В”, категорії “П” або “П” та “Ш”, класу “Б1”).

### **3 ВИМОГИ ДО КОМПЛЕКСУ**

#### **3.1 Вимоги до функцій комплексу**

3.1.1 Комплекс повинен забезпечити реалізацію регламентних процедур та механізмів роботи ЦСК, пов'язаних з:

- 1) обслуговуванням сертифікатів відкритих ключів (далі – сертифікатів) користувачів, що включає:
  - реєстрацію користувачів;
  - сертифікацію відкритих ключів користувачів;
  - розповсюдження сертифікатів;
  - управління статусом сертифікатів;
  - розповсюдження інформації про статус сертифікатів;
- 2) наданням послуг фіксування часу;
- 3) реалізацією ЕЦП і шифрування даних та управління особистими ключами і сертифікатами користувачів.

3.1.3 Комплекс повинен забезпечити виконання наступних функцій, пов'язаних з обслуговуванням ЦСК сертифікатів користувачів:

- 1) реєстрацію користувачів, що включає:
  - введення реєстраційних даних користувачів до реєстру користувачів;
  - зберігання реєстру користувачів та забезпечення доступу до реєстраційних даних;
  - резервне копіювання та архівування реєстру користувачів;
  - зміну реєстраційних даних користувачів у реєстрі;
  - видалення реєстраційних даних користувачів з реєстру;
- 2) сертифікацію відкритих ключів користувачів, що включає:
  - приймання та реєстрацію запитів користувачів на формування сертифікатів;
  - зберігання запитів, отриманих від користувачів, у базі даних запитів;
  - архівування бази даних запитів;
  - формування сертифікатів користувачів;
  - внесення сформованих сертифікатів у реєстр сертифікатів;
  - зберігання реєстру сертифікатів;
  - архівування реєстру сертифікатів;
- 3) розповсюдження сертифікатів відкритих ключів користувачів, що включає:
  - публікацію реєстру сертифікатів на інформаційному ресурсі ЦСК (у LDAP-каталозі та на веб-сторінці);
  - забезпечення доступу користувачів до реєстру сертифікатів на інформаційному ресурсі ЦСК;
- 4) управління статусом сертифікатів відкритих ключів користувачів та розповсюдження інформації про статус сертифікатів, що включає:
  - приймання та реєстрацію запитів користувачів на скасування, блокування чи поновлення сертифікатів;
  - зберігання запитів, отриманих від користувачів, у базі даних запитів;
  - архівування бази даних запитів;
  - скасування, блокування або поновлення сертифікатів на основі запитів;
  - внесення інформації про поточний статус сертифіката до реєстру сертифікатів;
  - формування списків відкликаних сертифікатів користувачів;

- публікацію списків відкликаних сертифікатів на інформаційному ресурсі ЦСК (у LDAP-каталозі та на веб-сторінці);
- забезпечення доступу користувачів до списків відкликаних сертифікатів на інформаційному ресурсі ЦСК;
- забезпечення доступу користувачів до інформації про статус сертифікатів (та самих сертифікатів) з використанням протоколу визначення статусу сертифіката (OCSP).

3.1.4 Комплекс повинен забезпечити виконання наступних функцій, пов'язаних з наданням ЦСК послуг фіксування часу:

- приймання та реєстрацію запитів користувачів на формування позначок часу;
- формування позначок часу;
- передачу сформованих позначок часу користувачам;
- внесення сформованих позначок часу у базу даних;
- зберігання сформованих позначок у базі даних;
- архівування бази даних позначок часу.

3.1.5 Для забезпечення функціонування ЦСК комплекс також повинен виконувати наступні функції:

1) управління ключами ЦСК, що включає:

- генерацію особистого та відкритого ключів ЦСК;
- введення та використання особистого ключа ЦСК;
- створення резервних копій особистого ключа ЦСК, а також відновлення особистого ключа з резервних копій;
- формування та передачу запиту на формування сертифіката ЦСК до ЦЗО;
- отримання та запис сформованого сертифікату у реєстр сертифікатів;
- публікацію сформованого сертифікату на інформаційному ресурсі ЦСК (у LDAP-каталозі та на веб-сторінці);

2) ведення реєстру посадових осіб ЦСК (адміністраторів), що включає:

- введення реєстраційних даних посадових осіб до реєстру посадових осіб;
- зберігання реєстру посадових осіб та забезпечення доступу до реєстраційних даних;
- зміну реєстраційних даних посадових осіб у реєстрі;
- видалення реєстраційних даних посадових осіб з реєстру;

3) управління ключами посадових осіб ЦСК (адміністраторів), що включає:

- генерацію особистого та відкритого ключів посадових осіб;
- введення та використання особистих ключів посадових осіб;
- формування та передачу запиту на формування сертифіката посадової особи до ЦСК;
- формування сертифікату посадової особи;
- запис сформованого сертифікату у реєстр сертифікатів;
- отримання, зберігання та використання сертифікату посадовою особою;

4) забезпечення адміністрування окремих апаратних та програмних засобів комплексу, що включає:

- налагодження параметрів засобів комплексу;
- діагностування роботи засобів комплексу;
- моніторинг стану засобів комплексу;

5) ведення журналів реєстрації окремими технічними засобами комплексу, що включає:

- запис реєстраційної інформації засобами комплексу до журналів реєстрації;
- збір та аналіз реєстраційної інформації у журналах;

6) забезпечення захисту інформації, що обробляється у комплексі, від НСД.

### 3.2 Вимоги до структури та призначення комплексу технічних засобів

3.2.1 До складу комплексу повинні входити такі технічні засоби (структурна схема комплексу технічних засобів наведена на рис. 3.1):

- центральні сервери (сервери ЦСК);
- внутрішнє комунікаційне обладнання ЛОМ;
- дисковий масив;
- сервери взаємодії (кластер);
- міжмережний екран (МЕ) з системою попередження втручань (IPS);
- сервер моніторингу та синхронізації часу;
- обладнання синхронізації часу (GPS-приймач);
- мережні криптомодулі (кластер);
- криптомодулі;
- апаратно-програмні засоби КЗІ (далі – АПЗ КЗІ);
- РС обслуговуючого персоналу (адміністратора безпеки, системного адміністратора, адміністратора реєстрації та адміністратора сертифікації);
- РС генерації ключів користувачів (ізольована).

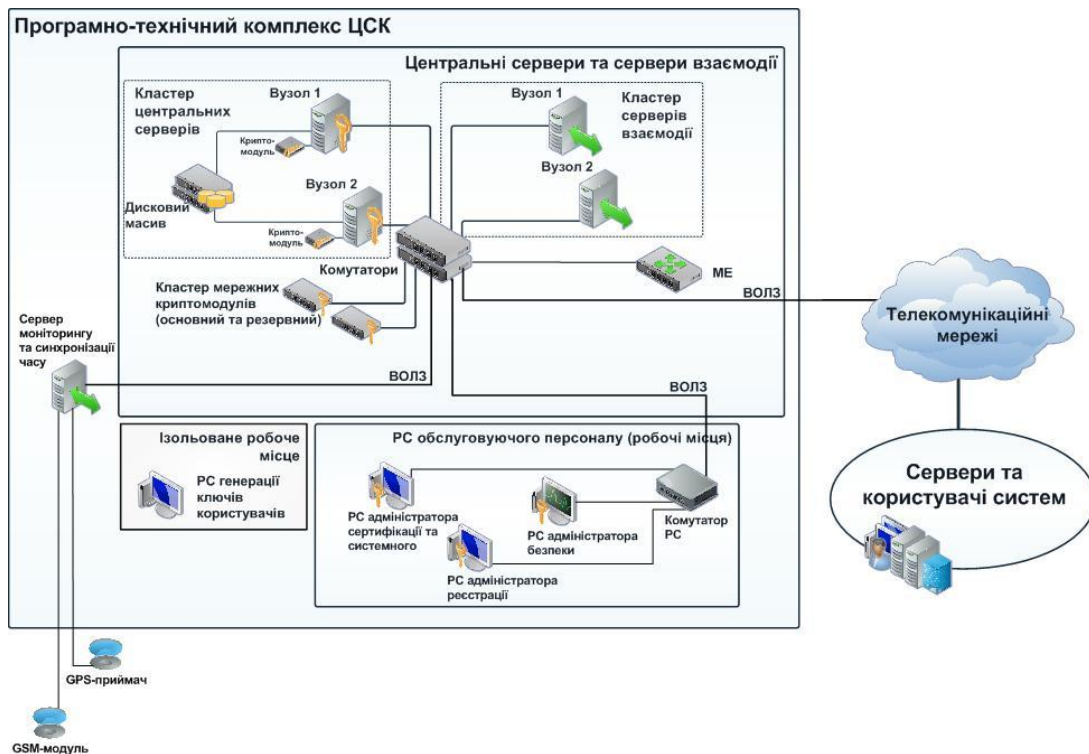


Рисунок 3.1 – Структурна схема комплексу.

#### 3.2.2 РС адміністратора безпеки призначена для:

- введення реєстраційних даних посадових осіб (адміністраторів) до реєстру посадових осіб;
- зміну реєстраційних даних посадових осіб у реєстрі;
- видалення реєстраційних даних посадових осіб з реєстру;
- виконання інших функцій, пов'язаних із забезпеченням та підтримкою безпеки інформації, що обробляється у комплексі. Детально вимоги до призначення РС адміністратора безпеки повинні визначатися у ТЗ на КСЗІ ЦСК.

#### 3.2.3 РС системного адміністратора призначена для:

- налагодження параметрів технічних засобів комплексу та системного програмного забезпечення;
- діагностування роботи технічних засобів комплексу;



- моніторингу та контролю стану технічних засобів комплексу та виконання ним окремих функцій.

#### 3.2.4 РС адміністратора реєстрації призначена для:

- генерації особистого та відкритого ключів адміністратора реєстрації;
- передачі запиту на формування сертифіката адміністратора реєстрації на центральний сервер;
- отримання, зберігання та використання сертифікату адміністратора реєстрації;
- введення та використання особистого ключа адміністратора реєстрації;
- введення реєстраційних даних користувачів до реєстру користувачів;
- зміни реєстраційних даних користувачів у реєстрі;
- видалення реєстраційних даних користувачів з реєстру;
- приймання запитів користувачів на формування сертифікатів, що включає перевірку володіння користувачем особистого ключа, відповідного до відкритого ключа у запиті;
- ініціювання формування сертифікатів користувачів шляхом ведення та передачі запитів користувачів на формування сертифікатів до центрального сервера, що включає підпис запитів користувачів адміністратором (з використанням особистого ключа адміністратора);
- ініціювання скасування, блокування чи поновлення сертифікатів користувачів шляхом ведення та передачі запитів на зміну статусу сертифікатів до центрального сервера, що включає підпис запитів адміністратором (з використанням його особистого ключа).

#### 3.2.5 РС адміністратора сертифікації призначена для:

- генерації особистого та відкритого ключів ЦСК;
- введення та використання особистого ключа ЦСК;
- створення резервних копій особистого ключа ЦСК, а також відновлення особистого ключа з резервних копій;
- формування та передачі запиту на формування сертифіката ЦСК до ЦЗО;
- отримання та запису сертифікату ЦСК у реєстр сертифікатів;
- публікації сертифікату ЦСК на інформаційному ресурсі (на веб-сторінці сервера взаємодії);
- публікації списків відкликаних сертифікатів на інформаційному ресурсі ЦСК (на веб-сторінці);
- приймання запитів на формування сертифікатів користувачів та посадових осіб (адміністраторів);
- формування сертифікатів на основі запиту шляхом, що включає підпис сертифікатів (з використанням особистого ключа ЦСК);
- формування списків відкликаних сертифікатів користувачів шляхом, що включає підпис списків відкликаних сертифікатів (з використанням особистого ключа ЦСК);
- ручного резервного копіювання та архівування реєстру сертифікатів;
- моніторингу та контролю виконання автоматизованих функцій, зокрема:
  - публікації реєстру сертифікатів на інформаційному ресурсі ЦСК (у LDAP-каталозі та на веб-сторінці) центральним сервером;
  - публікації списків відкликаних сертифікатів на інформаційному ресурсі центральним сервером;
  - публікації сертифікату ЦСК на інформаційному ресурсі центральним сервером.

#### 3.2.6 Центральні сервери (сервери ЦСК) призначені для:

- публікації сертифікату ЦСК на інформаційному ресурсі (у LDAP-каталозі);
- зберігання реєстру посадових осіб (адміністраторів) та забезпечення доступу до реєстраційних даних;
- використання реєстру посадових осіб;

- перевірки реєстраційних даних користувачів шляхом перевірки унікальності розпізнавального імені користувача;
- зберігання реєстру користувачів та забезпечення використання реєстраційних даних;
- використання реєстру користувачів;
- резервного копіювання та архівування реєстру користувачів;
- приймання та реєстрації запитів на формування сертифікатів користувачів та посадових осіб (адміністраторів);
- зберігання запитів на формування сертифікатів у базі даних запитів;
- архівування бази даних запитів на формування сертифікатів;
- перевірки унікальності відкритих ключів користувачів;
- зберігання реєстру сертифікатів;
- використання реєстру сертифікатів;
- автоматизованого резервного копіювання та архівування реєстру сертифікатів;
- публікації реєстру сертифікатів на інформаційному ресурсі ЦСК;
- приймання та реєстрації запитів користувачів і адміністраторів реєстрації на скасування, блокування чи поновлення сертифікатів;
- зберігання запитів на скасування, блокування чи поновлення сертифікатів у базі даних запитів;
- архівування бази даних запитів на скасування, блокування чи поновлення сертифікатів;
- скасування, блокування або поновлення сертифікатів на основі запитів;
- внесення інформації про поточний статус сертифіката до реєстру сертифікатів;
- публікації списків відкликаних сертифікатів на інформаційному ресурсі ЦСК;
- приймання через сервер взаємодії та обробку запитів користувачів на визначення статусу сертифікатів з використанням протоколу визначення статусу сертифіката (OCSP), шляхом формування інформації про статус сертифікатів;
- приймання через сервер взаємодії та обробку запитів користувачів на формування позначок часу, шляхом формування позначок часу та передачу сформованих позначок часу користувачам;
- внесення сформованих позначок часу у базу даних;
- зберігання сформованих позначок у базі даних;
- архівування бази даних позначок часу.

### 3.2.7 Сервери взаємодії призначені для:

- приймання та передачі запитів користувачів та адміністраторів реєстрації на формування сертифікатів користувачів на центральний сервер;
- забезпечення доступу користувачів до реєстру сертифікатів на інформаційному ресурсі ЦСК (у LDAP-каталозі та на веб-сторінці);
- приймання та передачі запитів користувачів та віддалених адміністраторів реєстрації на скасування, блокування чи поновлення сертифікатів користувачів на центральний сервер;
- забезпечення доступу користувачів до списків відкликаних сертифікатів на інформаційному ресурсі ЦСК;
- забезпечення доступу користувачів до інформації про статус сертифікатів з використанням протоколу визначення статусу сертифіката (OCSP), шляхом приймання та передачі запитів на визначення статусу сертифіката на центральний сервер та передачі інформації про статус у зворотному напрямку;
- приймання та передачі запитів користувачів на формування позначок часу на центральний сервер;
- передачі сформованих на центральному сервері позначок часу користувачам;
- забезпечення доступу до сертифікату ЦСК на інформаційному ресурсі.

### 3.2.8 Сервер моніторингу та синхронізації часу призначений для:

- синхронізації часу з Центральним засвідчувальним органом та системою GPS;

- надання даних точного часу усім іншим компонентам ЦСК;
- збирання і аналізу даних моніторингу.

3.2.9 Обладнання синхронізації часу (GPS-приймач) призначене для отримання сигналів точного часу від системи GPS.

3.2.10 Мережні криптомодулі призначені для:

- зберігання особистих ключів серверів ЦСК;
- виконання криптографічних операцій.

3.2.11 Криptomодулі призначені для:

- зберігання особистих ключів ЦСК;
- виконання криптографічних операцій.

3.2.12 АПЗ КЗІ призначені для

- зберігання особистих ключів персоналу ЦСК;
- виконання криптографічних операцій.

3.2.13 Комутатори та інше внутрішнє комунікаційне обладнання призначене для забезпечення внутрішньої взаємодії засобів комплексу та утворення ЛОМ.

3.2.14 МЕ з IPS призначені для фільтрації мережного трафіку між телекомунікаційними мережами та сервером взаємодії. Детально функції МЕ з IPS повинні визначатися у ТЗ на КСЗІ ЦСК.

3.2.15 РС генерації ключів користувачів призначена для:

- генерації особистого та відкритого ключів користувача та запис особистого ключа на носій ключової інформації (НКІ);
- формування та запису на носій інформації запиту на формування сертифіката користувача.

### 3.3 Вимоги до характеристик комплексу

3.3.1 Комплекс повинен забезпечувати характеристики, що наведені у табл. 3.1.

Таблиця 3.1 – Значення характеристик комплексу.

Показник	Значення
Кількість користувачів, яких обслуговує комплекс	не менше 1 000 000
Кількість користувачів, які можуть зареєструватися	не менше 5 000 за добу
Кількість користувачів, які одночасно мають доступ до сервера взаємодії (інформаційного ресурсу – LDAP-каталогу та web-сторінки)	не менше 5 000
Час обробки запитів користувачів на формування, блокування, поновлення та скасування сертифікатів центральним сервером	не більше 0,02 с (не менше 100 запитів/с)
Час обробки запитів зовнішніх користувачів на визначення статусу сертифіката	не більше 0,004 с (не менше 500 запитів/с)
Час обробки запитів зовнішніх користувачів на формування позначки часу	не більше 0,004 с (не менше 500 запитів/с)

### 3.4 Вимоги до режимів функціонування комплексу

3.4.1 Комплекс повинен забезпечувати функціонування та можливість надавати доступу до ЦСК користувачам цілодобово 7 днів на тиждень.

3.4.2 Центральні сервери та сервери взаємодії повинні функціонувати автоматизовано. Повинна існувати можливість роботи серверів у різних режимах – основний чи резервний з повним чи частковим дублюванням функцій.

3.4.3 Функціональні характеристики та режими експлуатації комплексу не повинні залежати від типів та характеристик технічних засобів (РС, серверів та комунікаційного обладнання).

### 3.5 Вимоги до експлуатації комплексу

#### 3.5.1 Умови та режими експлуатації комплексу

3.5.1.1 Технічні засоби комплексу повинні експлуатуватися в приміщеннях з нормальними кліматичними умовами:

- температура навколишнього середовища повітря плюс  $20 \pm 5$  °С;
- відносна вологість (навколишнього повітря  $60 \pm 15$ )%;
- атмосферний тиск від 84 до 107 кПа (від 630 до 800 мм. рт. ст.).

3.5.1.2 Комплекс повинен розміщатися у приміщенні ЦСК і взаємодіяти із зовнішніми користувачами через зовнішні телекомунікаційні мережі (ЗТМ).

#### 3.5.2 Вимоги до зберігання комплекту запасних технічних засобів

3.5.2.1 Порядок зберігання комплекту запасних технічних засобів, інсталяційних пакетів програмного забезпечення повинен бути визначений у відповідній інструкції зі складу експлуатаційної документації на комплекс та ЦСК, у складі якого він експлуатується.

3.5.2.2 Детально вимоги до зберігання комплекту запасних технічних засобів повинні визначатися у ТЗ на КСЗІ ЦСК.

#### 3.5.3 Вимоги до регламенту обслуговування технічних засобів

3.5.3.1 Технічне обслуговування РС та серверів комплексу повинне виконуватися відповідно до регламенту обслуговування ЕОМ.

3.5.3.2 Технічне обслуговування комунікаційного та іншого обладнання повинне виконуватися згідно експлуатаційної документації або ТУ підприємства-виробника обладнання.

3.5.3.3 Порядок технічного обслуговування повинен бути визначений у експлуатаційній документації на ЦСК.

#### 3.5.4 Вимоги до дій у разі виникнення аварійних ситуацій

3.5.4.1 Перелік можливих аварійних ситуацій при експлуатації комплексу та вимоги до дій у разі їх виникнення повинні бути визначені у відповідних інструкціях зі складу експлуатаційної документації на комплекс та ЦСК.

#### 3.5.5 Вимоги до зберігання та відновлення даних

3.5.5.1 Засоби центрального сервера повинні підтримувати можливість автоматичного резервного копіювання реєстру сертифікатів, реєстру користувачів, бази списків відкликаних сертифікатів та бази позначок часу.

3.5.5.2 Зберігання резервних копій повинне здійснюватися у приміщеннях, які територіально відокремлені від приміщення, де розміщений комплекс із забезпеченням захисту від НСД.

3.5.5.3 Порядок резервного копіювання та зберігання резервних копій повинен бути визначений у відповідній інструкції зі складу експлуатаційної документації на комплекс та ЦСК, у складі якого він експлуатується.

3.5.5.4 Детально вимоги до зберігання та відновлення даних повинні визначатися у ТЗ на КСЗІ ЦСК, у складі якого буде використовуватися комплекс.

### 3.6 Вимоги до персоналу, що відповідає за експлуатацію комплексу

#### 3.6.1 У експлуатації комплексу повинні бути задіяні наступні посадові особи:

- адміністратор безпеки;
- системний адміністратор;
- адміністратор сертифікації;
- адміністратор реєстрації;
- віддалений адміністратор реєстрації.

3.6.2 Загальні вимоги до посадових обов'язків зазначених осіб повинні відповідати вимогам правил посиленої сертифікації. Вимоги до посадових обов'язків адміністратора безпеки повинні визначатися у ТЗ на КСЗІ ЦСК, у складі якого буде використовуватися комплекс.

3.6.3 Настанови з експлуатації засобів визначеного персоналу повинні бути наведені у відповідних інструкціях зі складу експлуатаційної документації на комплекс та ЦСК.

3.6.4 Вимоги до підготовки персоналу та посадові обов'язки повинні бути визначені у експлуатаційній документації на ЦСК.

### 3.7 Вимоги до комплексу технічних засобів

#### 3.7.1 Вимоги до надійності та захисту від зовнішнього впливу

3.7.1.1 Вимоги до надійності технічних засобів, що входять до складу комплексу, повинні відповідати наступним показникам за ГОСТ 27.003-90 (група засобів II, вид – відновлюваний):

- середній наробіток на відмовлення повинний бути не менш 15 000 год.;
- середній час відновлення працездатного стану не більш 0,5 год.;
- середній термін служби повинний бути не менш 5 років;
- коефіцієнт технічного використання повинний бути не менш 0.95.

3.7.1.2 Вимоги електричної і механічної безпеки повинні відповідати ГОСТ 25861-83, клас захисту від поразки електричним струмом – перший.

3.7.1.3 Технічні засоби комплексу повинні бути стійким до зовнішніх впливів і чинників відповідно до вимог, які висуваються до наземної техніки класу 1, категорії технічних засобів, призначених для експлуатації в наземних стаціонарних приміщеннях і спорудах у кліматичному виконанні ПХЛ групи 1.1, відповідно до ГОСТ 21552-84.

#### 3.7.2 Вимоги до електроживлення, електричної міцності і опору ізоляції

3.7.2.1 Комплекс повинен бути працездатний при електроживленні обладнання від трьох- або однофазної мережі змінного струму з номінальною напругою 380/220 та 220 В відповідно і частотою змінного струму 50 Гц з параметрами у відповідності з ГОСТ 21552-84.

3.7.2.2 У разі зникнення електроживлення ДБЖ повинні забезпечити працездатність комплексу на час не менше ніж 15 хвилин для виконання завершення роботи окремих технічних засобів комплексу і виконання процедур, які забезпечують збереження інформації з метою уникнення пошкодження її цілісності.

3.7.2.3 Електрична міцність ізоляції комплексу технічних засобів системи між електричними струмопровідними ланцюгами, а також між струмопровідними ланцюгами і корпусом в нормальних кліматичних умовах експлуатації відповідно ГОСТ 21552-84 повинна забезпечувати відсутність пробойів і поверхневих перекриттів ізоляції при впливі випробувальної напруги не нижче 500 В для слабкострумових ланцюгів з робочою напругою до 100 В і не нижче 1500 В для ланцюгів електроживлення.

### 3.7.3 Вимоги до діагностування

3.7.3.1 Всі технічні засоби комплексу повинні забезпечувати можливість діагностування та отримання інформації про стан їх функціонування.

3.7.3.2 При виникненні збоїв або відмов при функціонуванні засобів повинна забезпечуватися можливість сигналізації про виникнення позаштатної ситуації (компоненти комплексу мають формувати відповідні коди повернення чи видавати повідомлення оператору).

### 3.7.4 Вимоги до ергономіки та естетики

3.7.4.1 Технічні засоби комплексу повинні задовольняти вимогам ергономіки за ГОСТ 12.2.049-80 і загальним вимогам естетики за ГОСТ 24750-81.

### 3.7.5 Вимоги до окремих технічних засобів

3.7.5.1 До складу всіх технічних засобів повинні входити джерела безперебійного живлення (ДБЖ).

3.7.5.2 До центрального сервера чи безпосередньо до РС адміністратора сертифікації має підключатися (входити до складу) апаратний або апаратно-програмний засіб КЗІ – криптомодуль, який призначений для:

- управління особистим ключем ЦСК (генерації, зберігання, введення, використання, резервного копіювання, відновлення та знищення);
- формування ЕЦП з використанням особистого ключа ЦСК.

3.7.5.3 До центрального сервера має підключатися (входити до складу) криптомодуль, який призначений для:

- управління особистими ключами серверів ЦСК (генерації, зберігання, введення, використання, резервного копіювання, відновлення та знищення);
- формування ЕЦП з використанням особистих ключів серверів ЦСК;
- направленою шифрування даних (реалізації протоколу розподілу ключів) з використанням особистих ключів серверів ЦСК (у разі, якщо криптомодуль підтримує реалізацію відповідного протоколу розподілу ключів).

3.7.5.4 Криptomодулі повинні бути апаратно-програмними засобами КЗІ виду “Б”, підвид “Б2”, або виду “В”, категорії “П” або “П” та “Ш”, класу “Б1” та повинні мати позитивні експертні висновки у галузі КЗІ (наприклад, криптомодуль “Гряда-61” – ТУ У 30.0-22723472-002:2007, МКМ “Гряда-301” – ТУ У 30.0-22723472-003:2008 чи ін.).

3.7.5.5 До складу одного з центральних серверів може входити пристрій резервного копіювання, який призначений для запису резервних копій даних та створення довгострокових архівів. Довгострокові архіви даних також можуть записуватися на оптичні компакт-диски. Для цього до складу центральних серверів повинні входити пристрої запису на оптичні компакт-диски.

3.7.5.6 До складу РС системного адміністратора повинен входити GPS-приймач, який призначений для отримання сигналів точного часу від GPS-супутників. Час має синхронізуватися з точністю до 1 с.

### 3.7.6 Вимоги до розміщення та взаємодії технічних засобів

3.7.6.1 Структурна схема комплексу технічних засобів наведена на рис. 3.3.

3.7.6.2 Технічні характеристики, кількість та розміщення технічних засобів комплексу може змінюватися. При цьому розміщення та порядок експлуатації технічних засобів повинні відповідати вимогам державних нормативних документів у сфері захисту інформації, зокрема, правил посиленої сертифікації.

3.7.6.3 РС адміністратора безпеки, системного адміністратора, адміністратора реєстрації, адміністратора сертифікації, центральні сервери (основний і резервний) та сервери взаємодії (основний і резервний) повинні взаємодіяти через внутрішню телекомунікаційну мережу на основі кабельної мережі та комутаторів і утворювати ЛОМ.

3.7.6.4 Центральні сервери, їх ДБЖ, дисковий масив та пристрій резервного копіювання (за наявності), комутатор (комутатор ЛОМ), комутатор терміналів з терміналом, мережні криптографічні модулі, а також сервери взаємодії та МЕ, повинні бути розміщені в окремій шафі у екранованому приміщенні (екранованій серверній кімнаті).

3.7.6.5 РС обслуговуючого персоналу (адміністратора безпеки, системного адміністратора, адміністратора реєстрації та адміністратора сертифікації) повинні бути підключені у окремий комутатор, який підключається окремим кабелем до комутатора ЛОМ у шафі з серверами.

3.7.6.6 Центральні сервери повинні утворювати стійкий до відмов кластер зі спільним дисковим масивом. Сервери взаємодії повинні утворювати стійкий до відмов кластер та мати однакову конфігурацію та інформаційне наповнення.

3.7.6.7 Сервери взаємодії повинні підключатися до телекомунікаційної мережі через МЕ із вбудованою IPS. Сервери повинні підключатися до МЕ за допомогою комутатора. Комутатор повинен забезпечувати утворення окремих віртуальних підмереж для цих підключень. Для підключення серверів взаємодії до віртуальної підмережі ЦСК та до віртуальної підмережі МЕ повинні використовуватися різні мережні адаптери.

3.7.6.8 МЕ з IPS повинні підключатися до телекомунікаційної мережі через комунікаційне обладнання.

3.7.6.9 Інші вимоги щодо розміщення та взаємодії технічних засобів з урахуванням вимог захисту оброблюваної інформації від НСД повинні визначатися у ТЗ на КСЗІ ЦСК (зокрема, використання ВОЛЗ тощо).

### 3.7.7 Вимоги до програмного забезпечення

3.7.7.1 До складу програмного забезпечення комплексу, яке реалізує логіку його роботи повинні входити:

- програмний комплекс ЦСК “ІТ ЦСК-1”;
- програмний комплекс користувача ЦСК “ІТ Користувач ЦСК-1”.

3.7.7.2 Зазначені програмні комплекси повинні бути комплексами програмних засобів КЗІ виду “Б”, підвид “Б2”, категорії “К”, “П” та “Ш”, класу В2.

### 3.8 Додаткові вимоги

#### 3.8.1 Загальні вимоги до засобів криптографічного захисту інформації

3.8.1.1 В програмних та апаратних засобах комплексу повинні використовуватися такі криптографічні алгоритми та протоколи:

- алгоритм шифрування за ДСТУ ГОСТ 28147:2009;
- алгоритм ЕЦП за ДСТУ 4145-2002;
- алгоритм гешування за ГОСТ 34.311-95;
- протокол розподілу ключових даних (направлене шифрування).

3.8.1.2 Алгоритм шифрування за ДСТУ ГОСТ 28147:2009 повинен використовуватися для:

- шифрування ключових та службових даних при зберіганні та передачі – у режимі простої заміни;
- шифрування даних, що передаються між користувачами ЦСК – у режимі гамування та гамування із зворотнім зв’язком;

- контролю цілісності ключових та службових даних при зберіганні та передачі – у режимі вироблення імітовставки.

3.8.1.3 Алгоритм ЕЦП за ДСТУ 4145-2002 повинен підтримувати всі параметри, що визначені у ДСТУ 4145-2002 та використовуватися для забезпечення цілісності:

- ключових даних (сертифікатів відкритих ключів) та службових даних (позначок часу, OCSP-відповідей та списків відкликаних сертифікатів);
- даних, що передаються між користувачами ЦСК.

3.8.1.4 Алгоритм гешування за ГОСТ 34.311-95 повинен використовуватися для

- гешування даних під час формування та перевіряння підпису за алгоритмом ЕЦП згідно ДСТУ 4145-2002;
- гешування паролів захисту ключових даних (особистих ключів);
- гешування спільного секретного значення під час реалізації протоколу розподілу ключових даних.

3.8.1.5 Протокол розподілу ключових даних повинен використовуватися для розподілу ключових даних під час направленою шифрування:

- службових даних, що передаються між посадовими особами ЦСК (адміністраторами) та центральним сервером чи сервером взаємодії ЦСК;
- даних, що передаються між користувачами ЦСК.

3.8.1.6 Протокол розподілу ключових даних повинен реалізовуватися згідно ДСТУ ISO/IEC 15946-3 (пп. 8.2) та вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв'язку України № 739 від 18.12.2012 р.

3.8.1.7 Генерація ключових даних повинна здійснюватися згідно методики генерації ключових даних, яка погоджена з ДСТСЗІ СБ України від 10.03.2005 р., вихідний № 85 від 01.11.2004 р.

### 3.8.2 Склад та організація ключової системи

3.8.2.1 У комплексі повинні використовуватися дві підгрупи ключових даних:

- ключові дані ЦСК;
- ключові дані користувачів.

3.8.2.2 До складу ключових даних ЦСК відносяться:

- особистий ключ та сертифікат відкритого ключа ЦСК;
- особисті ключі та сертифікати серверів ЦСК (TSP та OCSP, а також обробки запитів – CMP);
- особисті ключі та сертифікати посадових осіб ЦСК (адміністраторів).

3.8.2.3 Особистий ключ та сертифікат ЦСК повинні містити ключі ЕЦП для алгоритму ДСТУ 4145-2002 із ступенем розширення поля не менше 257 біт.

3.8.2.4 Особистий ключ ЦСК повинен зберігатися та застосовуватися у РС адміністратора сертифікації чи криптомодулі, що підключається до (входить до складу) центрального сервера або РС адміністратора сертифікації.

3.8.2.5 Особистий ключ ЦСК повинен використовуватися для формування ЕЦП сертифікатів та списків відкликаних сертифікатів.

3.8.2.6 Сертифікат ЦСК повинен використовуватися для перевірки ЕЦП, що накладається за допомогою особистого ключа ЦСК.



3.8.2.7 Особисті ключі та сертифікати серверів ЦСК (TSP та OSCP, а також CMP) повинні містити ключі ЕЦП для алгоритму ДСТУ 4145-2002 із ступенем розширення поля не менше 257 біт.

3.8.2.8 Особисті ключі серверів ЦСК (TSP та OSCP, а також CMP) можуть зберігатися та застосовуватися у криптомодулі, що підключається до (входить до складу) центрального сервера.

3.8.2.9 Особисті ключі серверів ЦСК повинні використовуватися для формування ЕЦП на позначках часу та інформації про статус сертифікатів.

3.8.2.10 Сертифікати серверів ЦСК повинні використовуватися для перевірки ЕЦП, що накладається за допомогою відповідних особистих ключів серверів ЦСК.

3.8.2.11 Особисті ключі та сертифікати посадових осіб ЦСК (адміністраторів) повинні містити ключі ЕЦП для алгоритму ДСТУ 4145-2002 та протоколу розподілу ключових даних із ступенем розширення поля не менше 257 біт.

3.8.2.12 Особисті ключі та сертифікати посадових осіб ЦСК (адміністраторів) призначені для направленою шифрування даних, що передаються між їх РС та центральним сервером.

3.8.2.13 Особисті ключі адміністраторів реєстрації та віддалених адміністраторів реєстрації призначені також для формування ЕЦП запитів на формування сертифікатів, а також запитів на блокування, поновлення та скасування, а сертифікати – для перевірки ЕЦП на вказаних типах даних.

3.8.2.14 Терміни дії особистих ключів та строки чинності сертифікатів ЦСК, серверів ЦСК та посадових осіб ЦСК (адміністраторів) повинні відповідати вимогам правил посиленої сертифікації.

3.8.2.15 До ключових даних користувачів відносяться особисті ключі та сертифікати користувачів, які призначені для формування та перевірки ЕЦП, а також для направленою шифрування даних, що передаються між користувачами. Ключі користувачів для алгоритму ЕЦП за ДСТУ 4145-2002 та протоколу розподілу ключів можуть бути суміщені (використовуватися і для підпису, і для направленою шифрування).

3.8.2.16 Терміни дії особистих ключів та строки чинності сертифікатів користувачів ЦСК повинні відповідати вимогам правил посиленої сертифікації.

3.8.2.17 Параметри еліптичних кривих для алгоритму ЕЦП за ДСТУ 4145-2002 повинні зберігатися у складі сертифікатів (у полі параметрів відкритого ключа). Параметри еліптичних кривих для протоколу розподілу ключів можуть зберігатися у складі особистих ключів або у складі сертифікатів.

3.8.2.18 Введення або вибір параметрів еліптичних кривих для алгоритму ЕЦП за ДСТУ 4145-2002 та протоколу розподілу ключів здійснюється під час генерації особистих та відкритих ключів.

3.8.2.19 Довгострокові ключові елементи (ДКЕ) для алгоритмів гешування за ГОСТ 34.311-95 та шифрування за ДСТУ ГОСТ 28147:2009 можуть бути обрані з дод. 1 до інструкції про порядок постачання і використання ключів до засобів КЗІ (що реалізують криптографічний алгоритм, визначений ДСТУ ГОСТ 28147:2009) або поставлені згідно вимог Адміністрації Держспецзв'язку України.

3.8.2.20 ДКЕ для алгоритму гешування за ГОСТ 34.311-95 зберігаються у складі сертифікатів (у полі параметрів відкритого ключа). ДКЕ для алгоритму шифрування за ДСТУ ГОСТ 28147:2009 повинні зберігатися у складі особистих ключів.

3.8.2.21 Введення або вибір ДКЕ для алгоритмів гешування за ГОСТ 34.311-95 та шифрування за ДСТУ ГОСТ 28147:2009 здійснюється під час генерації особистих та відкритих

ключів. Термін дії ДКЕ визначається терміном дії особистого ключа чи строком чинності сертифікату.

3.8.2.22 Особисті ключі, які зберігаються на носіях ключової інформації, повинні захищатися на паролях шляхом вироблення імітовставки за ДСТУ ГОСТ 28147:2009 та зашифрування в режимі простої заміни ДСТУ ГОСТ 28147:2009 на ключах, які отримані шляхом гешування строки пароля за ГОСТ 34.311-95. Паролі повинні відповідати наступним вимогам:

- алфавіт символів пароля – англійські букви “a” – “z”, “A” – “Z”, цифри “0” – “9” та символи “-”, “+” (потужність алфавіту –  $2^6$ , 6 біт/символ);
- довжина пароля – мінімальна 8, максимальна 42 символи (48-252 біт, потужність системи паролювання  $2^{46}$ - $2^{252}$ );
- обмеження до появи символів в паролі – не допускається введення більш ніж 2-ох символів, що розташовані поруч на розкладці клавіатури РС чи сервера, не допускається введення більш ніж 2-ох однакових символів на всій довжині пароля.

3.8.2.23 В якості носіїв ключової інформації для особистих ключів повинні використовуватися:

- гнучкі диски 3,5” (дискети);
- електронні диски (flash-диски);
- оптичні компакт-диски (CD-R, CD-RW, DVD-R або DVD-RW);
- криптомодулі “Гряда-61”;
- МКМ “Гряда-301”;
- електронні ключі “Кристал-1” (ТУ У 30.0-22723472-001:2007, “ІТ Е.ключ Кристал-1”);
- інші носії чи криптомодулі з бібліотеками підтримки, що відповідають внутрішнім вимогам розробника, які визначені у технічних описах інтерфейсів взаємодії з носіями ключової інформації та криптомодулями.

3.8.2.24 У випадку, якщо для зберігання та використання особистих ключів використовуються криптомодулі (апаратні або апаратно-програмні засоби КЗІ) виду “Б”, підвиду “Б2”, має забезпечуватися взаємна автентифікації криптомодулів та програмних комплексів (складових частин комплексу). Алгоритм (протокол) взаємної автентифікації повинен реалізовуватися відповідними бібліотеками підтримки (програмними компонентами), які є складовою частиною криптомодулів.

### 3.8.3 Інші вимоги до засобів криптографічного захисту інформації

3.8.3.1 Формати ключових даних та іншої спеціальної інформації повинні відповідати наступним вимогам:

- формати сертифікатів та списків відкликаних сертифікатів – згідно вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису, затверджених наказом Міністерства юстиції України та Адміністрації Держспецзв’язку України № 1236/5/453 від 20.08.2012 р.;
- формати підписаних даних (даних з ЕЦП) – згідно технічних рекомендацій RFC 5652 (PKCS#7) та вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису, затверджених наказом Міністерства юстиції України та Адміністрації Держспецзв’язку України № 1236/5/453 від 20.08.2012 р.;
- формати захищених даних (зашифрованих даних) – згідно технічних рекомендацій RFC 5652 (PKCS#7) та вимог до форматів криптографічних повідомлень, затверджених наказом Адміністрації Держспецзв’язку України № 739 від 18.12.2012 р.;
- формати запитів на отримання інформації про статус сертифіката та формати відповідей з інформацією про статус сертифіката – згідно технічних рекомендацій RFC 2560 та вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису, затверджених наказом Міністерства юстиції України та Адміністрації Держспецзв’язку України № 1236/5/453 від 20.08.2012 р.;

- формати запитів на формування позначок часу та самих позначок часу – згідно технічних рекомендацій RFC 3161 та вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису, затверджених наказом Міністерства юстиції України та Адміністрації Держспецзв’язку України № 1236/5/453 від 20.08.2012 р.;
- формати особистих ключів – згідно технічних рекомендацій PKCS#8.

3.8.3.2 ЦСК повинен формувати для кожного користувача два сертифікати з різними відкритими ключами:

- сертифікат з відкритим ключем ЕЦП (ДСТУ 4145-2002);
- сертифікат з відкритим ключем протоколу розподілу ключів (ДСТУ 4145-2002 – ДСТУ ISO/IEC 15946-3).

#### 3.8.4 Вимоги до комплексу засобів захисту

3.8.4.1 Вимоги до КЗЗ комплексу повинні визначатися у ТЗ на КСЗІ ЦСК, у складі якого буде використовуватися комплекс.

#### 4 ПОРЯДОК СТВОРЕННЯ КОМПЛЕКСУ

4.1 Стадії та етапи створення комплексу повинні відповідати вимогам ГОСТ 34.201-89 (наведені у табл. 4.1), а також включати роботи зі створення та атестації КСЗІ ЦСК, у відповідності до вимог нормативних документів у сфері захисту інформації.

Таблиця 4.1 – Стадії та етапи створення комплексу.

Стадія	Етапи робіт
1 Техноробочий проект	1.1 Розробка документації технічного проекту на ЦСК 1.2 Розробка робочої та експлуатаційної документації на ЦСК.
2 Введення в експлуатацію	2.1 Комплектація комплексу виробами, що підлягають закупівлі. 2.2 Облаштування приміщень. 2.3 Створення КСЗІ. 2.4 Підготовка персоналу. 2.5 Пусконаладжувальні роботи. 2.6 Проведення попередніх випробувань. 2.7 Проведення дослідної експлуатації та корегування робочої документації за результатами дослідної експлуатації. 2.8 Атестація КСЗІ (проведення державної експертизи у галузі ТЗІ). 2.9 Проведення приймальних випробувань та перехід до режиму штатної експлуатації (в т.ч. і підготовка до проведення акредитації)

## **5 ПОРЯДОК КОНТРОЛЮ ТА ПРИЙМАННЯ КОМПЛЕКСУ**

5.1 Порядок контролю та приймання комплексу повинен відповідати вимогам ГОСТ 34.603-92.

5.2 При впровадженні комплексу у складі ЦСК повинні виконуватися наступні види випробувань:

- 1) попередні випробування;
- 2) дослідна експлуатація;
- 3) приймальні випробування та перехід до режиму штатної експлуатації.

5.3 Випробування комплексу повинні проводитися безпосередньо у складі ЦСК.

5.4 Експертний заклад, який проводитиме експертні дослідження, у сфері КЗІ, складових частин комплексу, має бути призначений Адміністрацією Держспецв'язку на стадії робочого проекту розробки комплексу, для цього мають бути подані відповідні пропозиції щодо вибору експертного закладу.

## **6 ПОРЯДОК ПІДГОТОВКИ ДО ВВЕДЕННЯ КОМПЛЕКСУ В ДІЮ**

6.1 Порядок підготовки до введення комплексу в дію повинен визначатися у експлуатаційній документації на комплекс.

6.2 Інформація про порядок підготовки до введення комплексу в дію та необхідні зміни у системі повинна містити порядок та зміст робіт з переконфігурування програмно-технічних засобів, введення або закріплення відповідальних за експлуатацію комплексу осіб або підрозділів, вимоги до навчання персоналу тощо.

## 7 ВИМОГИ ДО ДОКУМЕНТУВАННЯ

7.1 Документування стадій розробки комплексу повинні відповідати вимогам РД 50-34.698-90.

7.2 До складу документації технічного проекту комплексу повинні входити наступні документи:

- пояснювальна записка;
- функціональна схема комплексу;
- структурна схема КТЗ;
- загальний опис комплексу;
- опис КТЗ;
- опис програмного забезпечення;
- схема організаційної структури.

7.3 До складу робочої документації на комплекс, окрім документації технічного проекту, повинні входити наступні документи:

- специфікація;
- програма та методика випробувань;
- формуляр;
- креслення установки технічних засобів;
- план розміщення обладнання та проводок.

7.4 До складу експлуатаційної документації на комплекс повинні входити наступні документи:

- інструкції з експлуатації КТЗ;
- інструкція щодо порядку генерації ключових даних та поводження з ключовими документами;
- інструкція щодо забезпечення безпеки експлуатації комплексу;
- програмна експлуатаційна документація на програмні засоби КЗІ, що входять до складу комплексу;
- експлуатаційна документація на апаратні та апаратно-програмні засоби КЗІ (криптомодулі), що входять до складу комплексу;
- експлуатаційна документація на КСЗІ.

7.5 Документування стадій розробки окремих складових частин комплексу (програмних комплексів та засобів) повинні відповідати вимогам ЄСПД.

7.6 Експлуатаційна документація на складові частини комплексу, окрім інших документів, повинна включати інструкцію щодо порядку генерації ключових даних та поводження з ключовими документами, а також інструкцію щодо забезпечення безпеки експлуатації складових частин комплексу.

7.7 Документування стадій впровадження комплексу у складі системи повинні відповідати вимогам РД 50-34.698-90.

7.8 Організаційно-розпорядчі документи, що пов'язані із впровадженням комплексу (акти, протоколи та накази), повинні розроблятися згідно з ГОСТ 34.603-92, РД 50-34.698-90 та включати документування етапів попередніх випробувань, дослідної експлуатації та впровадження у режимі штатної експлуатації.