

**ТЕХНІЧНЕ ЗАВДАННЯ**  
на комплексну систему захисту інформації  
в інформаційно-телекомунікаційній системі центру сертифікації ключів  
ринку електричної енергії

Шифр "КСЗІ.ЦСК.ЕНЕРГОРИНОК"

ЄААД.468244.185 ТЗ

2014 р.

**ЗМІСТ**

1 ЗАГАЛЬНІ ВІДОМОСТІ .....	4
2 МЕТА Й ПРИЗНАЧЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ .....	5
3 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІТС ТА УМОВ ЇЇ ФУНКЦІОНУВАННЯ .....	7
4 ВИМОГИ ТА ФУНКЦІЇ КЗЗ ІТС ЦСК .....	12
5 ВИМОГИ ДО КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ .....	20
6 ВИМОГИ ДО СКЛАДУ ПРОЕКТНОЇ ТА ЕКСПЛУАТАЦІЙНОЇ ДОКУМЕНТАЦІЇ .....	37
7 ЕТАПИ ВИКОНАННЯ РОБІТ .....	38
8 ПОРЯДОК ВНЕСЕННЯ ЗМІН І ДОПОВНЕНЬ ДО ТЗ .....	38
9 ПОРЯДОК ПРОВЕДЕННЯ ВИПРОБУВАНЬ КСЗІ .....	39

## ПЕРЕЛІК СКОРОЧЕНЬ

БД	– База даних
ВПП	– Відокремлений пункт реєстрації
ЕЦП	– Електронний цифровий підпис
ІзОД	– Інформація з обмеженим доступом
ІТС	– Інформаційно-телекомунікаційна система
КЗЗ	– Комплекс засобів захисту
КСЗІ	– Комплексна система захисту інформації
КТЗ	– Комплекс технічних засобів
ЛОМ	– Локальна обчислювальна мережа
МЕ	– Міжмережний екран
НКІ	– Носій ключової інформації
НСД	– Несанкціонований доступ
ОС	– Операційна система
ПД	– Персональні дані
ПК	– Програмний комплекс
РС	– Робоча станція
СКБД	– Система керування базами даних
СЗІ	– Служба захисту інформації
ТЗ	– Технічне завдання
ТЗІ	– Технічний захист інформації
ЦСК	– Центр сертифікації ключів

## ТЕРМІНИ ТА ВИЗНАЧЕННЯ

У цьому ТЗ використовуються терміни та визначення згідно з:

- ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення";
- НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу".

## 1 ЗАГАЛЬНІ ВІДОМОСТІ

### 1.1 Повне найменування КСЗІ та її умовне позначення

Комплексна система захисту інформації (далі – КСЗІ) в інформаційно-телекомунікаційній системі (далі – ІТС) центру сертифікації ключів ринку електричної енергії (далі – ЦСК).

### 1.2 Шифр теми

Шифр КСЗІ: "КСЗІ.ЦСК.ЕНЕРГОРИНОК".

### 1.3 Відомості про підприємство-замовника та підприємство-виконавця

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

Виконавець: визначається за результатами тендерної процедури.

### 1.4 Перелік документів, на підставі яких створюється КСЗІ, ким і коли затверджені ці документи

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

### 1.5 Відомості про джерела й порядок фінансування робіт

Фінансування робіт здійснюється за \_\_\_\_\_.

### 1.6 Порядок оформлення та подання результатів

Порядок оформлення та подання результатів робіт зі створення КСЗІ в ІТС ЦСК повинен відповідати вимогам: ДСТУ 3396.0-96, ДСТУ 3396.1-96, РД 50-34.698-90, НД ТЗІ 2.5-004-99, НД ТЗІ 3.7-003-05.

## 2 МЕТА Й ПРИЗНАЧЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

### 2.1 Мета створення КСЗІ

Метою створення КСЗІ є забезпечення захисту інформації, яка циркулює у ІТС ЦСК, від несанкціонованого доступу (далі – НСД) шляхом здійснення протидії загрозам, які можна очікувати внаслідок дій порушника. Захист інформації повинен забезпечуватися на всіх технологічних етапах її обробки і в усіх режимах функціонування ІТС ЦСК.

При розробці та впровадженні КСЗІ в ІТС ЦСК повинні бути враховані існуючі тенденції розвитку захищених інформаційних технологій, розробки відповідних засобів захисту інформації, вимоги державної нормативної бази з технічного захисту інформації (далі – ТЗІ).

Для здійснення захисту інформації на всіх стадіях життєвого циклу ІТС ЦСК у КСЗІ має бути передбачено застосування наступних заходів та засобів захисту інформації:

- організаційно-правові заходи, які реалізуються поза обчислювальною системою ІТС ЦСК;
- інженерно-технічні заходи, що реалізуються поза обчислювальною системою ІТС ЦСК;
- апаратні, програмно-апаратні та програмні засоби:
  - захисту від НСД;
  - криптографічного захисту інформації (далі – КЗІ);
  - забезпечення доступності інформації, що обробляється в ІТС ЦСК.

### 2.2 Функціональне призначення КСЗІ

КСЗІ в ІТС ЦСК призначена для:

- реалізації політики безпеки інформації заданої у ІТС ЦСК;
- забезпечення конфіденційності, цілісності, доступності інформації під час її обробки засобами ІТС ЦСК;
- забезпечення конфіденційності та цілісності інформації під час її передачі каналами зв'язку;
- недопущення витоку інформації з обмеженим доступом (далі - ІЗОД) та втрати її матеріальних носіїв;
- створення механізму та умов оперативного реагування на зовнішні та внутрішні загрози з метою забезпечення безпеки інформації;
- керування засобами захисту інформації, розмежування доступу користувачів до ресурсів ІТС ЦСК, контроль за їхньою роботою з боку осіб, які відповідають за забезпечення безпеки інформації в ІТС ЦСК;
- створення умов для забезпечення максимально можливого рівня локалізації негативних наслідків, що завдаються неправомірними та несанкціонованими діями порушників, зменшення негативного впливу наслідків порушення безпеки на функціонування ІТС ЦСК;
- реєстрації, збору, зберігання, обробки даних про всі події в ІТС ЦСК, які мають відношення до безпеки інформації;
- забезпечення доступності ресурсів ІТС ЦСК для його користувачів;
- захисту інформації від зовнішніх впливів відповідно до вимог Правил посиленої сертифікації (Наказ ДСТСЗІ СБУ від 10.05.06 №50).

## 2.3 Нормативно-правові акти та нормативні документи, що є основою створення КСЗІ

Захист інформації та створення КСЗІ в ІТС ЦСК повинні здійснюватись згідно вимог наступних керівних і нормативно-методичних документів:

- Закон України "Про інформацію";
- Закон України "Про захист інформації в інформаційно-телекомунікаційних системах";
- Закон України "Про захист персональних даних";
- Закон України "Про електронний цифровий підпис";
- Концепція технічного захисту інформації в Україні, затверджена Постановою Кабінету Міністрів України від 08.10.97 № 1126;
- Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229/99;
- ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення;
- ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт;
- НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;
- НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі;
- НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі;
- НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;
- НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки;
- НД ТЗІ 2.7-009-09. Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу;
- НД ТЗІ 2.7-010-09. Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу;
- НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.
- НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу;
- Положення про державну експертизу в сфері технічного захисту інформації. Затверджено наказом Адміністрації Держспецзв'язку від 16.05.2007 № 93. Зареєстровано в Міністерстві юстиції України 16.07.2007 за № 820/14087;
- Правила посиленої сертифікації, затверджені наказом ДСТСЗІ СБ України від 13.01.2005 № 3, зареєстровані в Міністерстві юстиції України від 27.01.2005 за № 104/10384 (із змінами).

### **3 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІТС ТА УМОВ ЇЇ ФУНКЦІОНУВАННЯ**

#### **3.1 Загальна характеристика**

ІТС ЦСК є розподіленим багатомашинним багатокористувачевим комплексом, до складу якого входять обчислювальна система, фізичне середовище, в якому вона знаходиться і функціонує, середовище користувачів, оброблювана інформація та технологія її обробки.

Згідно НД ТЗІ 3.7-003-2005 ІТС ЦСК є інтегрованою, а згідно НД ТЗІ 2.5-005-99 класифікується як ІТС класу "3".

#### **3.2 Основні функціональні завдання**

ІТС ЦСК призначена для забезпечення реалізації регламентних процедур та механізмів, пов'язаних з обслуговуванням посилених 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;
- надання послуг фіксування часу.

#### **3.3 Склад ІТС ЦСК**

##### **3.3.1 До складу ІТС ЦСК входять:**

- центральний сегмент ІТС ЦСК, у складі:
  - локальна обчислювальна мережа (далі – ЛОМ) серверів ЦСК;
  - робочих місць обслуговуючого персоналу (далі – РМ обслуговуючого персоналу);
  - РС генерації ключів;

3.3.2 До складу комплексу технічних засобів (далі – КТЗ) центрального сегменту ІТС ЦСК входять:

- КТЗ ЛОМ серверів ЦСК, у складі:
  - центральні сервери (сервери ЦСК) (кластер);
  - сервери взаємодії (кластер);
  - дискові масиви;
  - сервер моніторингу та синхронізації часу;
  - обладнання синхронізації часу (GPS-приймач);
  - міжмережний екран (далі – МЕ);
  - мережні криптомодулі (кластер);
  - криптомодулі;
  - комутатори ЛОМ;
- КТЗ робочих місць обслуговуючого персоналу:
  - РС адміністратора безпеки;
  - РС адміністратора реєстрації;
  - РС адміністратора сертифікації та системного адміністратора;
  - апаратно-програмні засоби КЗІ (далі – АПЗ КЗІ);
- РС генерації ключів.

Структурна схема КТЗ ІТС ЦСК наведена на рисунку 3.1.

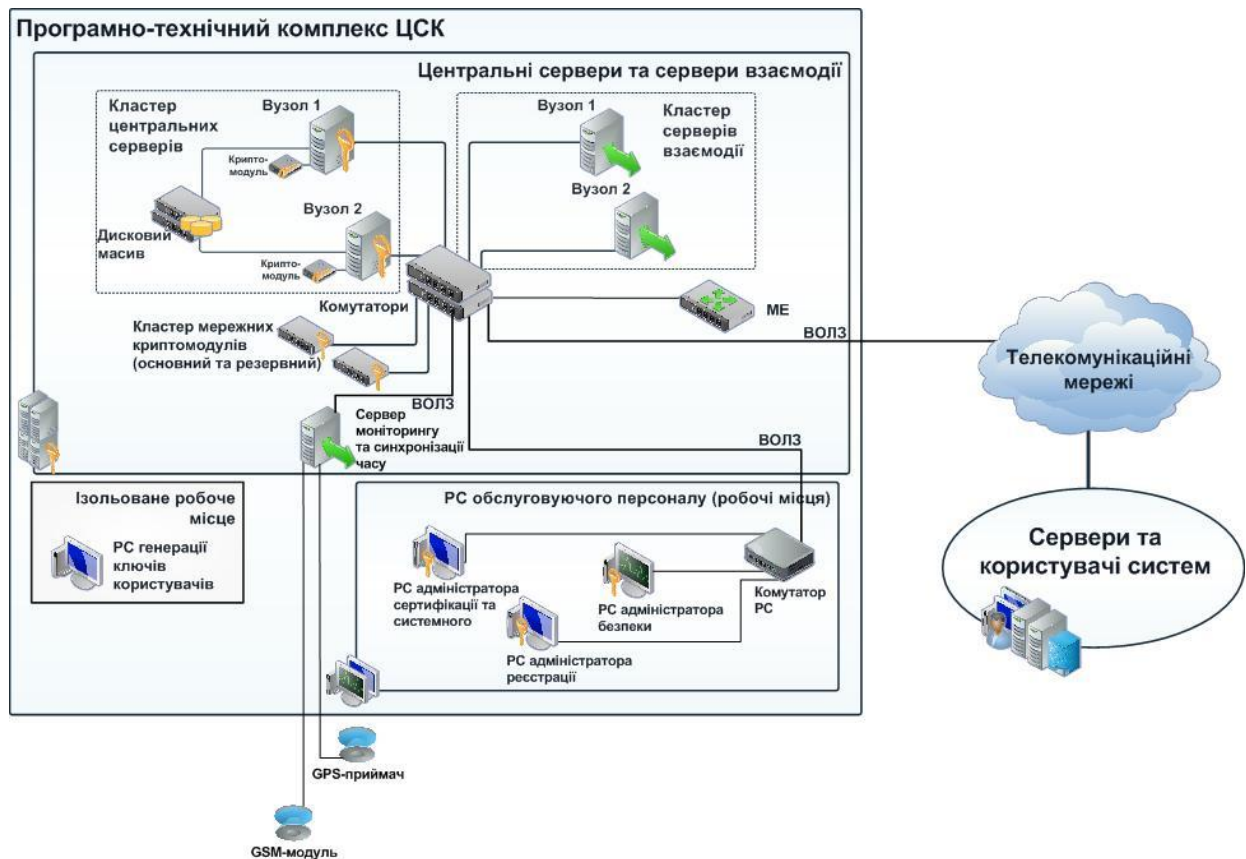


Рисунок 3.1 – Структурна схема КТЗ ІТС ЦСК

### 3.3.4 Програмне забезпечення

3.3.3.1 До складу програмного забезпечення (далі – ПЗ) ЛОМ серверів ЦСК входять:

- операційні системи (далі – ОС) центральних серверів;
- ОС серверів взаємодії;
- ОС серверу моніторингу та синхронізації часу;
- система керування базами даних (далі – СКБД) центральних серверів;
- СКБД серверів взаємодії;
- ПЗ HTTP-серверу;
- ПЗ LDAP-серверу;
- програмний комплекс (далі – ПК) центральних серверів;
- ПК серверів взаємодії;
- ПЗ моніторингу;
- засоби антивірусного захисту (далі – ЗАЗ) для центральних серверів.

3.3.3.2 До складу ПЗ<sup>1</sup> РМ обслуговуючого персоналу входять:

- ОС РМ обслуговуючого персоналу;
- ПЗ RDP клієнта.

3.3.3.3 До складу ПЗ РМ генерації ключів входять:

- ОС РМ генерації ключів;
- ЗАЗ для РМ генерації ключів;

<sup>1</sup> Функціональне (спеціалізоване) ПЗ адміністраторів (системного, безпеки, реєстрації) встановлено на серверах ЛОМ серверів ЦСК і запускається/виконується безпосередньо на них із використанням засобів віддаленого доступу або локального підключення до відповідних серверів



- ПК РС генерації ключів.

### 3.4 Характеристика оброблюваної інформації

3.4.1 За змістом вимог щодо захисту, оброблювана в ІТС ЦСК інформація підрозділяється на такі категорії:

- загальнодоступна інформація;
- персональні дані;
- особисті ключі ЦСК, серверів ЦСК, персоналу ЦСК, заявників;
- технологічна інформація.

3.4.2 Загальнодоступна інформація, що обробляється у ЦСК відноситься до відкритої інформації, доступ на її читання мають усі користувачі веб-ресурсу ЦСК, доступ на модифікацію – тільки персонал ІТС ЦСК в межах посадових обов'язків. До інформації цієї категорії висуваються підвищені вимоги із забезпечення цілісності та доступності.

3.4.3 Персональні дані (далі – ПД) осіб, які є зареєстрованими користувачами (абонентами) ЦСК, є ІзОД та відноситься до конфіденційної інформації. Доступ до ПД має тільки персонал ІТС ЦСК в межах посадових обов'язків. ПД є інформацією вимога щодо захисту якої встановлена законом "Про захист персональних даних". До інформації цієї категорії висуваються підвищені вимоги із забезпечення конфіденційності, цілісності та доступності.

3.4.4 Особисті ключі ЦСК, серверів ЦСК, персоналу ЦСК, заявників є ІзОД та повинні бути доступні лише власникам у відповідності до закону "Про електронний цифровий підпис". До інформації цієї категорії висуваються підвищені вимоги із забезпечення конфіденційності, цілісності та доступності.

3.4.5 Технологічна інформація складається з технологічної інформації комплексу засобів захисту (далі – КЗЗ) ІТС ЦСК та технологічної інформації щодо адміністрування та управління обчислювальною системою ІТС ЦСК. До інформації цієї категорії висуваються підвищені вимоги із забезпечення конфіденційності та цілісності.

### 3.5 Середовище користувачів

#### 3.5.1 Групи користувачів

Користувачі ІТС ЦСК поділяються на дві групи:

- внутрішні користувачі;
- зовнішні користувачі<sup>2</sup>.

#### 3.5.2 Група внутрішніх користувачів

Для надання внутрішнім користувачам повноважень з доступу до інформації, що обробляється у ІТС ЦСК, та дозволів на виконання певних робіт у процесі функціонування ІТС ЦСК їм можуть бути надані такі композитні ролі<sup>3</sup>:

- адміністратори безпеки<sup>4</sup>;
- системні адміністратори та сертифікації;
- адміністратори реєстрації;
- адміністратори реєстрації (чергова зміна).

<sup>2</sup> Критерієм віднесення користувача до групи "Зовнішні" чи "Внутрішні" є його належність до персоналу ІТС ЦСК (ІТС ВПР)

<sup>3</sup> Композитна роль - характеристика користувача, яка є логічним поєднанням деякої не порожньої множини локальних ролей. По тексту цього ТЗ у якості синоніму терміну "композитна роль" використовується термін "роль". У разі, якщо треба наголосити на тому, що роль підтримується (реалізується) конкретним компонентом КЗЗ у цьому ТЗ використовується термін "локальна роль"

<sup>4</sup> Заборонено сумішати роль адміністратора безпеки з ролями системного адміністратора, адміністратора сертифікації, адміністратора реєстрації

### 3.5.3 Група зовнішніх користувачів

Зовнішні користувачі поділяються на:

- підписувачі;
- анонімні користувачі ЦСК;
- заявники.

### 3.5.4 Функції внутрішніх користувачів

3.5.4.1 Основними функціями користувача з роллю "Адміністратори безпеки" є:

- налаштування КЗЗ програмного забезпечення центрального сегменту ІТС ЦСК;
- налаштування КЗЗ комплексу технічних засобів центрального сегменту ІТС ЦСК;
- контроль за функціонуванням КЗЗ центрального сегменту ІТС ЦСК;
- управління (генерація, знищення) особистими і відкритими ключами ЕЦП та протоколу розподілу ключів;
- генерація, резервне копіювання, знищення, відновлення з резервної копії, контроль за використанням особистого ключа ЦСК та особистих ключів серверів ЦСК;
- контроль за дотриманням вимог політики безпеки у ІТС ЦСК.

3.5.4.2 Основними функціями користувача з роллю "Системні адміністратори" є:

- налаштування ПЗ центрального сегменту ІТС ЦСК (у частині, що не стосується параметрів безпеки);
- налаштування КТЗ центрального сегменту ІТС ЦСК (у частині, що не стосується параметрів безпеки);
- контроль працездатності ПЗ та КТЗ центрального сегменту ІТС ЦСК;
- технічне обслуговування КТЗ центрального сегменту ІТС ЦСК.

3.5.4.3 Основними функціями користувача з роллю "Адміністратори сертифікації" є:

- генерація, резервне копіювання, знищення, відновлення з резервної копії, контроль за використанням особистого ключа ЦСК та особистих ключів серверів ЦСК;
- формування сертифіката ЦСК та сертифікатів серверів ЦСК;
- формування сертифікатів для персоналу ЦСК (адміністратора сертифікації, адміністраторів реєстрації, віддалених адміністраторів реєстрації);
- погодження запитів на формування та зміну статусу сертифікатів для підписувачів;
- формування списків відкликаних сертифікатів;
- наповнення інформаційного ресурсу ЦСК.

3.5.4.4 Основними функціями користувача з роллю "Адміністратори реєстрації" є:

- ведення реєстру користувачів;
- формування запитів на формування сертифікатів для заявників;
- підтвердження запитів на формування сертифікатів для заявників;
- формування запитів на зміну статусу сертифікатів для заявників.

3.5.4.5 Основними функціями користувача з роллю "Адміністратори реєстрації (чергова зміна)" є:

- ведення реєстру користувачів;
- формування запитів на зміну статусу сертифікатів для заявників.

### 3.5.5 Функціональні можливості зовнішніх користувачів

3.5.5.1 Анонімний користувач ЦСК має право на перегляд та скачування інформації, що розміщена на інформаційному ресурсі ЦСК (веб-сторінці), отримання позначки часу, отримання статусу сертифіката.

3.5.5.2 Підписувач має право на подання запитів на зміну статусу власного сертифіката і права анонімного користувача.

3.5.5.3 Заявник має право на генерацію ключової пари на РС генерації ключів.

### 3.6 Умови розташування об'єкта

3.6.1 Розміщення обчислювальної системи компонентів ІТС ЦСК має виконуватися, виходячи з:

- локалізації технічних засобів у приміщеннях, фізичний доступ до яких є обмеженим;
- технічних характеристик обладнання і вимог щодо його встановлення і умов експлуатації визначених їх виробником.

3.6.2 Приміщення де розміщуються компоненти ІТС ЦСК, повинні мати пропускний і внутріоб'єктовий режими, що визначені діючими нормативними та розпорядчими документами Замовника.

### 3.7 Можливі загрози безпеки інформації

Порушення конфіденційності, цілісності та доступності інформації, що обробляється у ІТС ЦСК можуть проявлятися внаслідок таких загроз:

- порушення правил розмежування доступу до інформації, що обробляється в компонентах ІТС ЦСК внаслідок неправильної конфігурації та/або обходу механізмів КЗЗ;
- несанкціоноване перехоплення або викривлення даних, що передаються незахищеними каналами зв'язку між компонентами ІТС ЦСК;
- втрата атрибутів доступу внутрішніх користувачів ІТС ЦСК, що призводить до неможливості використання функцій ІТС ЦСК;
- несанкціоноване отримання (перехоплення) або викривлення даних початкової ідентифікації та автентифікації користувачів ІТС ЦСК;
- відмова в обслуговуванні авторизованих користувачів внаслідок надмірного використання ресурсів ІТС ЦСК з боку авторизованого/неавторизованого користувача;
- несанкціоноване використання обчислювальних ресурсів ІТС ЦСК для досягнення цілей, які не відповідають призначенню ІТС ЦСК;
- неправильне функціонування складових ІТС ЦСК у наслідок порушення цілісності програмних або апаратно-програмних засобів чи інших відмов;
- відмова користувачів ІТС ЦСК від факту створення інформації певного виду;
- модифікація або видалення даних аудиту.

### 3.8 Технологія обробки інформації в ІТС ЦСК

3.8.1 Центральний сегмент ІТС ЦСК забезпечує виконання таких функцій:

- керування (генерація, використання, резервне копіювання, знищення) особистими ключами ЦСК, серверів ЦСК та персоналу ЦСК;
- ведення реєстру користувачів;
- керування (формування, публікація, блокування та скасування) сертифікатів відкритих ключів ЦСК, серверів ЦСК, персоналу ЦСК та користувачів;
- резервне копіювання особистих ключів ЦСК та серверів ЦСК, сертифікатів, списків відкликаних сертифікатів та реєстру користувачів;
- архівування сертифікатів та реєстру користувачів.

## 4 ВИМОГИ ТА ФУНКЦІЇ КЗЗ ІТС ЦСК

### 4.1 Загальні вимоги до КСЗІ в ІТС ЦСК

КСЗІ повинна забезпечити захист інформаційних ресурсів ІТС ЦСК від зовнішніх загроз, атак та несанкціонованого витоку інформації шляхом створення й підтримки безпечних інформаційних технологій, в рамках яких доступ до інформації різних категорій організується таким чином, що тільки уповноваженим користувачам або процесам надається можливість роботи з конкретною інформацією, доступ до якої обмежується і гарантується цілісність при її обробці засобами ІТС ЦСК.

КЗЗ ІТС ЦСК повинен забезпечувати:

- цілісність та доступність загальнодоступної інформації;
- конфіденційність, цілісність та доступність персональних даних, які зберігаються й обробляються в компонентах ІТС ЦСК, а також передається між ними;
- конфіденційність, цілісність та доступність особистих ключів, що використовується компонентами ЦСК, окремими його користувачами;
- конфіденційність та цілісність технологічної інформації, яка забезпечує функціонування КЗЗ ІТС ЦСК;
- доступ до інформації та ресурсів ІТС ЦСК користувачам ІТС ЦСК згідно з правилами встановленими політикою безпеки (зокрема, правами доступу);
- спостереженість за діями користувачів шляхом впровадження механізмів і процедур контролю, реєстрації та проведення аудиту зареєстрованих подій.

### 4.2 Вимоги до складу КЗЗ ІТС ЦСК

4.2.1 Враховуючи результати аналізу загроз та цілі безпеки, пропонується такий склад програмних, апаратних та апаратно-програмних компонентів КЗЗ центрального сегменту ІТС ЦСК:

а) Компоненти КЗЗ центрального сегменту ІТС ЦСК, що розташовані у ЛОМ серверів ЦСК:

- КЗЗ ОС центральних серверів;
- КЗЗ ОС серверів взаємодії;
- КЗЗ ОС сервера моніторингу та синхронізації часу;
- КЗЗ СКБД центральних серверів;
- КЗЗ СКБД серверів взаємодії;
- КЗЗ ПЗ HTTP-серверу;
- КЗЗ ПЗ LDAP-серверу;
- КЗЗ ПК центральних серверів;
- КЗЗ ПК серверів взаємодії;
- ЗАЗ центральних серверів;
- МЕ;
- комутатори ЛОМ;
- мережні криптомодулі;
- криптомодулі;
- КЗЗ ПЗ моніторингу.

б) Компоненти КЗЗ центрального сегменту ІТС ЦСК, що розташовані на РМ обслуговуючого персоналу:

- КЗЗ ОС РМ обслуговуючого персоналу;
- АПЗ КЗІ.

в) Компоненти КЗЗ центрального сегменту ІТС ЦСК, що розташовані на РС генерації ключів:

- КЗЗ ОС РС генерації ключів;

- ЗАЗ для РС генерації ключів;
- КЗЗ ПК РС генерації ключів.

#### 4.3 Функції складових (компонентів) КЗЗ ІТС ЦСК

Зазначені у п. 4.3.1 - 4.3.21 основні функції компонентів КЗЗ ІТС ЦСК слід розглядати як відповідні<sup>5</sup> підмножини функцій<sup>6</sup> КЗЗ центрального сегменту ІТС ЦСК.

##### 4.3.1 Основні функції КЗЗ ОС центральних серверів

- забезпечення цілісності власних модулів КЗЗ шляхом розмежування доступу на модифікацію до відповідних системних файлів;
- забезпечення цілісності КЗЗ програмних компонентів, що функціонують під її керуванням шляхом розмежування доступу до відповідних виконуваних файлів;
- розмежування доступу на читання, модифікацію та запуск до об'єктів файлової системи;
- ідентифікація та автентифікація користувачів ОС на основі логіна та пароля;
- надання достовірного каналу для введення атрибутів користувачів ОС;
- реєстрація подій, що відбуваються на рівні ОС;
- підтримка можливості об'єднання кількох ОС у відмовостійкий кластер;
- приймання на себе керування операційною системою резервного сервера у разі відмови програмних/апаратних компонентів основного сервера (у т.ч. криптомодулів, що підключені до нього);
- автоматичне відновлення ОС після збоїв;
- відновлення стану ОС на певний момент часу;
- очищення залишкової інформації у оперативній пам'яті центрального сервера;
- контроль запуску процесів;
- підтримка множини локальних<sup>7</sup> адміністративних та користувацьких ролей на рівні ОС.

##### 4.3.2 Основні функції КЗЗ ОС серверів взаємодії

- забезпечення цілісності власних модулів КЗЗ шляхом розмежування доступу на модифікацію до відповідних системних файлів;
- забезпечення цілісності КЗЗ програмних компонентів, що функціонують під її керуванням шляхом розмежування доступу до відповідних виконуваних файлів;
- розмежування доступу на читання, модифікацію та запуск до об'єктів файлової системи;
- ідентифікація та автентифікація користувачів ОС на основі логіна та пароля;
- надання достовірного каналу для введення атрибутів користувачів ОС;
- реєстрація подій, що відбуваються на рівні ОС;
- підтримка можливості об'єднання кількох ОС у відмовостійкий кластер;
- приймання на себе керування операційною системою резервного сервера у разі відмови програмних/апаратних компонентів основного сервера;
- автоматичне відновлення ОС після збоїв;
- відновлення стану ОС на певний момент часу;
- очищення залишкової інформації у оперативній пам'яті сервера взаємодії;
- контроль запуску процесів;
- підтримка множини локальних адміністративних та користувацьких ролей на рівні ОС.

<sup>5</sup> Інформація щодо "місця застосування" компонентів КЗЗ ІТС ЦСК наведена у п. 4.2

<sup>6</sup> Функції КЗЗ центрального сегменту ІТС ЦСК розглядаються як суперпозиція функцій відповідних компонентів КЗЗ ІТС ЦСК

<sup>7</sup> Під "локальною" роллю тут і далі розуміється роль, що надається/реалізується конкретним апаратним, програмним чи апаратно-програмним компонентом КЗЗ ІТС ЦСК

#### 4.3.3 Основні функції КЗЗ ОС сервера моніторингу та синхронізації часу

- забезпечення цілісності власних модулів КЗЗ шляхом розмежування доступу на модифікацію до відповідних системних файлів;
- забезпечення цілісності КЗЗ програмних компонентів, що функціонують під її керуванням шляхом розмежування доступу до відповідних виконуваних файлів;
- розмежування доступу на читання, модифікацію та запуск до об'єктів файлової системи;
- ідентифікація та автентифікація користувачів ОС на основі логіна та пароля;
- надання достовірного каналу для введення атрибутів користувачів ОС;
- реєстрація подій, що відбуваються на рівні ОС;
- автоматичне відновлення ОС після збоїв;
- відновлення стану ОС на певний момент часу;
- очищення залишкової інформації у оперативній пам'яті сервера моніторингу та синхронізації часу;
- контроль запуску процесів;
- підтримка множини локальних адміністративних та користувацьких ролей на рівні ОС.

#### 4.3.4 Основні функції КЗЗ СКБД центральних серверів

- розмежування доступу на читання та модифікацію об'єктів (таблиць, відображень, процедур, що зберігаються) БД центральних серверів;
- відкат БД центральних серверів у випадку помилок;
- ідентифікація та автентифікація користувачів СКБД на основі логіна та пароля;
- реєстрація подій, що відбуваються на рівні СКБД;
- керування максимальним часом виконання запитів, що надходять з віддаленого вузла;
- керування максимальною кількістю конкурентних з'єднань;
- керування мінімальним та максимальним розміром оперативної пам'яті, що виділяється процесу СКБД;
- забезпечення відновлення після збоїв шляхом повернення БД у відомий безпечний стан з використанням резервних копій;
- підтримка множини локальних адміністративних та користувацьких ролей на рівні ОС.

#### 4.3.5 Основні функції КЗЗ СКБД серверів взаємодії

- розмежування доступу на читання та модифікацію об'єктів (таблиць, відображень, процедур, що зберігаються) БД серверів взаємодії;
- відкат БД серверів взаємодії у випадку помилок;
- ідентифікація та автентифікація користувачів СКБД на основі логіна та пароля;
- реєстрація подій, що відбуваються на рівні СКБД;
- керування максимальним часом виконання запитів, що надходять з віддаленого вузла;
- керування максимальною кількістю конкурентних з'єднань;
- забезпечення відновлення після збоїв шляхом повернення БД у відомий безпечний стан з використанням резервних копій;
- підтримка множини локальних адміністративних та користувацьких ролей на рівні СКБД;
- **реплікація вмісту БД із основного на резервний сервер взаємодії.**

#### 4.3.6 Основні функції КЗЗ ПЗ НТТР-серверу

- розмежування доступу до підмножин веб-сторінок сайту на основі мережного інтерфейсу з якого надходять запити;

- обмеження прав процесу на доступ до об'єктів файлової системи, що розміщені поза директорію сайту;
- ведення журналу реєстрації фактів доступу до файлів сайту;
- обмеження максимальної кількості користувачів, що можуть одночасно отримувати доступ до ПЗ HTTP-серверу;
- керування кількістю обробників запитів користувачів ПЗ HTTP-серверу;
- перевірка синтаксису конфігураційного файлу.

#### 4.3.7 Основні функції КЗЗ ПЗ LDAP-серверу

- розмежування доступу на читання та модифікацію до даних, що зберігаються у LDAP-директорії;
- підтримка локальної ролі "Адміністратори ПЗ LDAP-серверу" та локальної ролі "Неавтентифіковані користувачі ПЗ LDAP-серверу";
- автентифікацій адміністратора за логіном та паролем.

#### 4.3.8 Основні функції КЗЗ ПК центральних серверів

- формування обмеженого набору запитів на читання та модифікацію даних, що зберігаються у БД центральних серверів згідно з локальними ролями, що підтримуються ПК центральних серверів;
- ідентифікація та автентифікація користувачів ПК центральних серверів (адміністраторів реєстрації) на основі сертифікату та доказу володіння особистим ключем;
- ідентифікація та автентифікація користувачів ПК центральних серверів (адміністратора безпеки, адміністратора сертифікації) на основі логіна та пароля (використовуючи механізми безпеки СКБД центральних серверів);
- одночасний експорт даних до основного та резервного серверів взаємодії;
- ведення журналів подій у спеціальній таблиці БД зі складу СКБД центральних серверів;
- підтримка локальної адміністративної ролі "Адміністратори безпеки" та локальних користувальницьких ролей "Адміністратори сертифікації", "Адміністратори реєстрації";
- надсилання запитів до апаратних засобів КЗІ на формування ЕЦП;
- перевіряння ЕЦП.

#### 4.3.9 Основні функції КЗЗ ПК серверів взаємодії

- трансляція до сервісів ПК центральних серверів запитів (надходять за протоколом http) від підписувачів та анонімних користувачів ЦСК;
- автентифікація адміністраторів ПК серверу взаємодії на основі логіна та пароля;
- підтримка локальної адміністративної ролі "Адміністратори ПК серверу взаємодії" та локальних користувальницьких ролей "Неавтентифіковані користувачі";
- надання доступу до налаштувань ПК серверу взаємодії тільки адміністратору ПК серверу взаємодії;
- ведення журналів помилок та результатів дій з адміністрування ПК серверу взаємодії.

#### 4.3.10 Основні функції ЗАЗ центральних серверів

- контроль власної цілісності;
- захист від зловмисного ПЗ та вірусних заражень;
- ідентифікація та автентифікація користувача з локальною роллю "Адміністратори ЗАЗ" за паролем та належністю до адміністративної групи на рівні ОС;
- підтримка локальної адміністративної ролі "Адміністратори ЗАЗ" та локальної користувальницької ролі "Звичайні користувачі ЗАЗ";
- тестування на предмет вірусного зараження при старті та за запитом уповноваженого користувача;

- аудит виявлених порушень.

#### 4.3.11 Основні функції МЕ

- розмежування мережних потоків за правилами встановленими користувачем з локальною роллю "Адміністратори МЕ";
- розмежування доступу на читання та модифікацію до об'єктів, що зберігаються у ПЗП та ОЗП МЕ;
- ідентифікація та автентифікація користувачів з локальною роллю "Адміністратори МЕ" за логіном та паролем;
- підтримка можливості об'єднання кількох МЕ у кластер (паралельна обробка запитів, що надходять);
- забезпечення безперервності надання функцій МЕ за умови працездатності хоча б одного з МЕ, що входить до кластеру;
- відновлення налаштувань МЕ на певний момент часу з використанням резервних копій;
- підтримка локальної адміністративної ролі "Адміністратори МЕ" та локальної користувальницької ролі "Інші користувачі МЕ";
- контроль цілісності вбудованого програмного забезпечення;
- надання інтерфейсу для консольного підключення;
- ведення записів про мережні підключення;
- реєстрація подій щодо дій користувача з локальною роллю "Адміністратори МЕ".

#### 4.3.12 Основні функції комутаторів ЛОМ

- розмежування мережних потоків за правилами встановленими користувачем з локальною роллю "Адміністратори комутатора ЛОМ";
- розмежування доступу на читання та модифікацію до об'єктів, що зберігаються у ПЗП та ОЗП комутатора ЛОМ;
- ідентифікація та автентифікація користувача з локальною роллю "Адміністратори комутатора ЛОМ" за логіном та паролем;
- підтримка можливості об'єднання кількох комутаторів у стек (паралельна обробка запитів, що надходять);
- забезпечення безперервності надання функцій комутації за умови працездатності хоча б одного з комутатора, що входить до стеку;
- відновлення налаштувань комутатора ЛОМ на певний момент часу з використанням резервних копій;
- підтримка локальної адміністративної ролі "Адміністратори комутатора ЛОМ" та локальної користувальницької ролі "Інші користувачі комутатора ЛОМ";
- надання інтерфейсу для консольного підключення;
- контроль цілісності вбудованого програмного забезпечення;
- реєстрація подій щодо дій користувача з локальною роллю "Адміністратори комутатора ЛОМ".

#### 4.3.13 Основні функції мережних криптомодулів

- розмежування доступу до особистих ключів, криптографічних параметрів, журналів аудиту згідно з локальними ролями користувачів мережного криптомодулю;
- резервне копіювання і відновлення з резервної копії особистих ключів;
- ідентифікація та автентифікація користувачів мережного криптомодуля за паролем та портом підключення;
- підтримка локальних адміністративних ролей "Адміністратори безпеки МКМ", "Адміністратори МКМ" та локальної користувальницької ролі "Оператори МКМ";
- забезпечення конфіденційності та контролю цілісності даних, які передаються між мережним криптомодулем та автентифікованими програмними засобами користувача (ЕОМ);



- аудит подій пов'язаних із функціонуванням мережного криптомодуля (входом/виходом, генерацією ключів, параметрів тощо);
- підтримка можливості об'єднання кількох мережних криптомодулів у кластер;
- формування та перевірка ЕЦП від даних, що надійшли від автентифікованих програмних засобів користувача (ЕОМ);
- автентифікація програмних засобів користувачів (ЕОМ);
- контроль цілісності вбудованого програмного забезпечення;
- тестування правильності криптографічних перетворень.

#### 4.3.14 Основні функції криптомодулів

- розмежування доступу до особистих ключів, криптографічних параметрів, журналів аудиту згідно з локальними ролями користувачів криптомодуля;
- резервне копіювання і відновлення з резервної копії особистих ключів;
- ідентифікація та автентифікація користувачів криптомодуля за паролем;
- підтримка локальної адміністративної ролі "Адміністратори криптомодуля" та локальної користувальницької ролі "Оператори криптомодуля";
- забезпечення конфіденційності та контролю цілісності даних, які передаються між криптомодулем та автентифікованими програмними засобами користувача (ЕОМ);
- формування ЕЦП від даних, що надійшли від автентифікованих програмних засобів користувача (ЕОМ);
- автентифікація програмних засобів користувачів (ЕОМ);
- контроль цілісності вбудованого програмного забезпечення;
- тестування правильності криптографічних перетворень.

#### 4.3.15 Основні функції АПЗ КЗІ

- розмежування доступу до особистих ключів, криптографічних параметрів згідно з локальними ролями користувачів АПЗ КЗІ;
- ідентифікація та автентифікація користувачів АПЗ КЗІ за паролем;
- підтримка локальної адміністративної ролі "Адміністратори АПЗ КЗІ" та локальної користувальницької ролі "Оператори АПЗ КЗІ";
- забезпечення конфіденційності та контролю цілісності даних, які передаються між АПЗ КЗІ та автентифікованими програмними засобами користувача (ЕОМ);
- формування ЕЦП від даних, що надійшли від автентифікованих програмних засобів користувача (ЕОМ);
- автентифікація програмних засобів користувачів (ЕОМ);
- контроль цілісності вбудованого програмного забезпечення;
- тестування правильності криптографічних перетворень.

#### 4.3.16 Основні функції КЗЗ ОС РМ обслуговуючого персоналу

- забезпечення цілісності власного КЗЗ шляхом розмежування доступу до системних файлів;
- забезпечення цілісності КЗЗ програмних компонентів, що функціонують під її керуванням шляхом розмежування доступу до відповідних виконуваних файлів;
- розмежування доступу на читання, модифікацію та запуск до об'єктів файлової системи;
- ідентифікація та автентифікація користувачів ОС на основі логіна та пароля;
- надання достовірного каналу для введення атрибутів користувачів ОС;
- реєстрація подій, що відбуваються на рівні ОС;
- підтримка множини локальних адміністративних та користувальницьких ролей на рівні ОС;
- автоматичне відновлення ОС після збоїв;
- відновлення стану ОС на певний момент часу;
- очищення залишкової інформації у оперативній пам'яті РМ обслуговуючого персоналу;

- розмежування мережних потоків і захист від мережних атак.

#### 4.3.17 Основні функції КЗЗ ПЗ користувача ЦСК у варіанті виконання Java Applet

- надання механізмів контролю цілісності модулів КЗІ зі складу ПЗ користувача ЦСК у варіанті виконання Java Applet;
- перевірка ЕЦП на відповідях, що надійшли від ПК центральних серверів;
- забезпечення конфіденційності і контроль цілісності підмножини даних, що передаються до ПК центральних серверів;
- забезпечення достовірного каналу для введення атрибутів доступу до особистого ключа;
- тестування правильності криптографічних перетворень.

#### 4.3.18 Основні функції ПЗ моніторингу

- діагностика функціонування мережних вузлів та перевірка функціонування спеціалізованих програмних сервісів;
- ведення журналів з результатами діагностики;
- сповіщення вповноважених користувачів засобами електронної пошти/мобільного зв'язку (sms);
- підтримка локальної ролі "Адміністратори ПЗ моніторингу" та локальної ролі "Користувачі, що отримують діагностичну інформацію";
- ідентифікація та автентифікація адміністраторів та користувачів за логіном та паролем;
- розмежування доступу користувачів на читання на рівні окремих записів журналів з результатами діагностики.

#### 4.3.19 Основні функції КЗЗ ОС РС генерації ключів

- забезпечення цілісності власного КЗЗ шляхом розмежування доступу до системних файлів;
- забезпечення цілісності КЗЗ програмних компонентів, що функціонують під її керуванням шляхом розмежування доступу до відповідних виконуваних файлів;
- розмежування доступу на читання, модифікацію та запуск до об'єктів файлової системи;
- ідентифікація та автентифікація користувачів ОС на основі логіна та пароля;
- надання достовірного каналу для введення атрибутів користувачів ОС;
- реєстрація подій, що відбуваються на рівні ОС;
- підтримка множини локальних адміністративних та користувальницьких ролей на рівні ОС;
- автоматичне відновлення ОС після збоїв;
- відновлення стану ОС на певний момент часу;
- блокування спроб користувача запуску виконуваних файлів із зовнішнього носія;
- очищення залишкової інформації у оперативній пам'яті РС генерації ключів.

#### 4.3.20 Основні функції ЗАЗ для РС генерації ключів

- контроль власної цілісності;
- розмежування доступу на читання та модифікацію налаштувань ЗАЗ;
- захист від зловмисного ПЗ та вірусних заражень;
- ідентифікація та автентифікація користувача з локальною роллю "Адміністратори ЗАЗ" за паролем та належністю до адміністративної групи на рівні ОС;
- підтримка локальної адміністративної ролі "Адміністратори ЗАЗ" та локальної користувальницької ролі "Звичайні користувачі ЗАЗ";
- тестування на предмет вірусного зараження при старті та за запитом уповноваженого користувача;
- аудит виявлених порушень.

## 4.3.21 Основні функції КЗЗ ПК РС генерації ключів

- формування ЕЦП від вмісту запиту на формування сертифіката користувача;
- налаштування параметрів КЗЗ ОС для РС генерації ключів;
- запобігання спробам несанкціонованого запуску ПЗ, що не входить до складу ПК РС генерації ключів;
- мінімізація функцій користувачів ПК РС генерації ключів;
- очищення залишкової інформації щодо згенерованого особистого ключа користувача з локальною роллю "Користувачі ПК РС генерації ключів";
- підтримка локальної адміністративної ролі "Адміністратори ПК РС генерації ключів" та локальної користувальницької ролі "Користувачі ПК РС генерації ключів";
- надання достовірного каналу для введення паролю до особистого ключа, що генерується користувачем з локальною роллю "Користувачі ПК РС генерації ключів";
- реєстрація подій, що пов'язані із використанням функції ПК РС генерації ключів.

## 5 ВИМОГИ ДО КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

### 5.1 Вимоги до КСЗІ в ІТС ЦСК в частині захисту від несанкціонованого доступу

5.1.1 У процесі функціонування ІТС ЦСК об'єктами захисту є: програмно-інформаційні ресурси, в яких знаходиться, або може знаходитись інформація, яка підлягає захисту, а також програмне забезпечення, що реалізує технології оброблення такої інформації, для виконання персоналом ІТС ЦСК своїх функцій.

5.1.2 Відповідно до функціонального призначення та виду подання, політикою безпеки визначається узагальнений перелік інформаційних ресурсів, що є об'єктами захисту (таблиця 5.1).

#### 5.1.3 Вимоги до користувачів

За рівнем повноважень щодо доступу до програмних засобів та інформації, що циркулює у ІТС ЦСК, характером та змістом робіт, які виконуються в процесі функціонування, користувачі можуть мати одну або кілька ролей наведених у п. 3.5.

#### 5.1.4 Вимоги до взаємодії об'єктів-користувачів і об'єктів захисту ІТС ЦСК

5.1.4.1 КЗЗ ІТС ЦСК повинен реалізовувати розмежування доступу до об'єктів захисту (п. 5.1.2) з боку об'єктів-користувачів (п. 5.1.3) на основі атрибутів доступу об'єктів захисту та об'єктів-користувачів. Об'єкт-користувач є поданням фізичного користувача у ІТС ЦСК, що створюється в процесі входження (здійснення процедури ідентифікації та автентифікації) користувача у ІТС ЦСК і повністю характеризується унікальним набором атрибутів (наприклад, власним ідентифікатором та ідентифікатором локальної<sup>8</sup> ролі).

5.1.4.2 Ролі, що можуть бути призначені як атрибути доступу для користувачів (об'єктів-користувачів)

У ІТС ЦСК визначаються такі ролі:

- роль "Адміністратори безпеки" (P\_АБ);
- роль "Системні адміністратори" (P\_АС);
- роль "Адміністратори сертифікації" (P\_АЦ);
- роль "Адміністратори реєстрації" (P\_АР);
- роль "Адміністратори реєстрації (чергова зміна)" (P\_АРЧЗ);
- роль "Підписувачі" (P\_ЗПП);
- роль "Анонімні користувачі ЦСК" (P\_ЗАН);
- роль "Заявники" (P\_ЗЗЯ).

#### 5.1.4.3 Атрибути доступу

Атрибути доступу користувачів використовуються для їх ідентифікації та автентифікації. Атрибути доступу об'єктів-користувачів використовуються для розмежування доступу до об'єктів захисту ІТС ЦСК. Деякі атрибути можуть одночасно використовуватися із різною метою як користувачами так і об'єктами-користувачами.

Для анонімних користувачів ЦСК використовуються тимчасові об'єкти типу об'єкт-користувач, що ідентифікуються за мережною адресою.

<sup>8</sup>

Перелік локальних ролей, що підтримуються компонентами КЗЗ ІТС ЦСК наведені у п. 4.3

Таблиця 5.1 – Перелік та позначення інформаційних ресурсів ІТС ЦСК

№	Позначення	Назва	Ступінь обмеження доступу
1	{Д_ТІКс}	Технологічна інформація КЗЗ ЛОМ серверів ЦСК	ІзОД
2	{Д_ТІКo}	Технологічна інформація КЗЗ РМ обслуговуючого персоналу	ІзОД
3	{Д_ТІКг}	Технологічна інформація КЗЗ РС генерації ключів	ІзОД
4	{Д_ТІУс}	Технологічна інформація управління компонентами ЛОМ серверів ЦСК	ІзОД
5	{Д_ТІУo}	Технологічна інформація управління РМ обслуговуючого персоналу	ІзОД
6	{Д_ТІУг}	Технологічна інформація управління РС генерації ключів	ІзОД
7	{Д_ЖУРС}	Журнали аудиту, що ведуться КЗЗ ЛОМ серверів ЦСК	ІзОД
8	{Д_ЖУРо}	Журнали аудиту, що ведуться КЗЗ РМ обслуговуючого персоналу	ІзОД
9	{Д_ЖУРг}	Журнали аудиту, що ведуться КЗЗ РС генерації ключів	ІзОД
10	{Д_ОКП}	Особисті ключі персоналу ІТС ЦСК	ІзОД
11	{Д_ОКЦ}	Особисті ключі ЦСК та серверів ЦСК	ІзОД
12	{Д_ОКк}	Особисті ключі заявників, що генеруються на РС генерації ключів	ІзОД (ПД)
13	{Д_КФА}	Ключова фраза автентифікації, яка може бути використана підписувачем для подання запиту на блокування/скасування свого сертифікату (по телефону)	ІзОД (ПД)
14	{Д_РП}	Реєстр підписувачів	ІзОД (ПД)
15	{Д_СЕР}	Сертифікати ЦСК, серверів ЦСК, персоналу ЦСК та користувачів <sup>9</sup> , списки відкликаних сертифікатів	Відкрита
16	{Д_ВЕБ}	Загальнодоступна інформація веб-сторінки	Відкрита
17	{Д_ЗМЧ}	Запит на мітку часу	Відкрита
18	{Д_МЧ}	Мітка часу	Відкрита
19	{Д_ЗСС}	Запит статусу сертифіката	Відкрита
20	{Д_СС}	Статус сертифіката	Відкрита
21	{Д_ЗКСС}	Запит на керування статусом сертифіката	Відкрита
21	{Д_ЗКФС}	Запит на формування сертифікату	Відкрита

Атрибути доступу, які мають<sup>10</sup> користувачі (об'єкти-користувачі) з відповідними ролями наведені у таблиці 5.2.

<sup>9</sup> Сертифікати користувачів, публікація яких на веб-сторінці або директорії ЦСК заборонений їх власниками, відносяться до ІзОД

<sup>10</sup> Атрибути доступу можуть уточнюватися за результатами техноробочого проектування

Таблиця 5.2 – Опис атрибутів доступу, що мають користувачі ІТС ЦСК згідно наданих ролей

Назва атрибуту	Роль користувача							
	P_AB	P_AC	P_AЦ	P_AP	P_APЧЗ	P_ЗПП	P_ЗАН	P_ЗЗЯ
Ідентифікатори локальних ролей та паролі до облікових записів ОС центральних серверів	+	+	+	+	+			
Ідентифікатори локальних ролей та паролі до облікових записів ОС серверів взаємодії	+	+	+					
Ідентифікатори локальних ролей та паролі до облікових записів ОС сервера моніторингу та синхронізації часу	+	+						
Ідентифікатори локальних ролей та паролі до облікових записів ОС РМ обслуговуючого персоналу	+	+	+	+	+			
Ідентифікатори локальних адміністративних ролей та паролі до облікових записів ОС РС генерації ключів	+	+						
Ідентифікатори локальної користувальницької ролі ОС РС генерації ключів <sup>11</sup>								+
Ідентифікатори локальних ролей та паролі до облікових записів СКБД центральних серверів	+	+						
Ідентифікатори локальних ролей та паролі до облікових записів СКБД серверів взаємодії	+	+						
Ідентифікатори локальних ролей та паролі до керованого комутаційного обладнання	+	+						
Ідентифікатори локальних ролей та паролі до облікових записів ПЗ LDAP-серверу	+	+						
Ідентифікатори локальних ролей ПК центральних серверів	+		+	+	+			
Паролі до облікових записів ПК центральних серверів	+		+					
Ідентифікатори локальних ролей та паролі до облікових записів ПК серверів взаємодії	+		+					
Ідентифікатори локальних ролей та паролі до облікових записів ПЗ моніторингу	+	+						
Ідентифікатори локальних ролей та паролі до ЗАЗ для центральних серверів та ЗАЗ для РС генерації ключів	+							
Мережна адреса	+	+	+	+	+		+	
Особистий ключ ЕЦП			+	+	+	+		+
Пароль до особистого ключа ЕЦП			+	+	+	+		+
Сертифікат відкритого ключа			+	+	+	+		+
Ідентифікатори локальних ролей та паролі до облікових записів МЕ	+							
Ідентифікатори локальних ролей та паролі до криптомодулів	+	+	+					
Ідентифікатори локальних ролей та паролі до мережних криптомодулів	+	+	+					

<sup>11</sup> Пароль до облікового запису ОС РС генерації ключів від імені якого запускається ПК РС генерації ключів вводиться співробітником ІТС ЦСК

Узагальненими переліком атрибутів доступу об'єктів захисту, що використовується КЗЗ ІТС ЦСК для розмежування доступу до них є:

- ідентифікатор (найменування) об'єкту захисту;
- асоційований список доступу;
- використовуваний порт;
- IP-адреса;
- позначка про можливість публікації сертифіката.

#### 5.1.5 Правила розмежування доступу

КЗЗ ІТС ЦСК повинен підтримувати види доступу об'єктів-користувачів до об'єктів захисту, що є програмними ресурсами (налаштування, інсталяція/деінсталяція, застосування) та види доступу до об'єктів захисту, що є інформаційними ресурсами (читання, модифікація, створення, видалення). Права доступу, що їх має контролювати КЗЗ ІТС ЦСК, об'єктів-користувачів до інформаційних ресурсів визначені у таблиці 5.3.

Право на налаштування та інсталяцію/деінсталяцію компонентів ПЗ центрального сегменту ІТС ЦСК надано тільки користувачам з ролями Р\_АБ або Р\_АС. При цьому Р\_АС має дозвіл на модифікацію<sup>12</sup> налаштувань, що не стосуються безпеки.

Права користувачів на використання ПЗ ІТС ЦСК (центрального сегменту ІТС ЦСК) визначаються наявністю атрибутів доступу, що зведені до таблиці 5.2.

#### 5.1.6 Принципи розмежування доступу

Усі запити користувачів на доступ до об'єктів захисту мають оброблятися КЗЗ ІТС ЦСК. Доступ до пасивного об'єкту захисту має дозволятися/заборонятися згідно правил розмежування доступу за результатами порівняння атрибутів доступу об'єкта-користувача та призначених йому прав.

КЗЗ ІТС ЦСК надає доступ об'єкту-користувачу до об'єкта захисту, якщо виконуються усі умови:

- у асоційованому списку об'єкта захисту для об'єкта-користувача (або ролі до якої він входить) у явному вигляді надано необхідний вид доступу;
- у асоційованому списку об'єкта захисту для об'єкта-користувача (або ролі до якої він входить) відсутні заборони на необхідний вид доступу.

5.1.7 Забезпечення безпеки об'єктів захисту у ІТС ЦСК має здійснюватися шляхом комплексного використання організаційних (адміністративних) заходів, правових і законодавчих норм, фізичних і технічних (програмних, апаратно-програмних і апаратних) засобів захисту інформації.

---

<sup>12</sup> За необхідності це має контролюватися із залученням організаційних заходів та засобів моніторингу дій користувачів адміністративних груп

Таблиця 5.3 – Максимальні права доступу до інформаційних ресурсів, які можуть мати користувачі ІТС ЦСК згідно наданих їм ролей

№	Позначення	Право доступу			
		Читання	Створення	Модифікація	Видалення <sup>13</sup>
1	{Д_ТІКс}	Р_АБ	Р_АБ	Р_АБ	Р_АБ
2	{Д_ТІКо}	Р_АБ	Р_АБ	Р_АБ	Р_АБ
4	{Д_ТІКГ}	Р_АБ	Р_АБ	Р_АБ	Р_АБ
5	{Д_ТІУс}	Р_АБ, Р_АС	Р_АБ, Р_АС	Р_АБ, Р_АС	Р_АБ, Р_АС
6	{Д_ТІУо}	Р_АБ, Р_АС	Р_АБ, Р_АС	Р_АБ, Р_АС	Р_АБ, Р_АС
8	{Д_ТІУГ}	Р_АБ, Р_АС	Р_АБ, Р_АС	Р_АБ, Р_АС	Р_АБ, Р_АС
9	{Д_ЖУРС}	Р_АБ, Р_АС	–	–	Р_АБ, Р_АС
10	{Д_ЖУРо}	Р_АБ, Р_АС	–	–	Р_АБ, Р_АС
12	{Д_ЖУРГ}	Р_АБ, Р_АС	–	–	Р_АБ, Р_АС
13	{Д_ОКП} <sup>14</sup>	Р_АЦ, Р_АР, Р_АРЧЗ	Р_АЦ, Р_АР, Р_АРЧЗ	–	Р_АЦ, Р_АР, Р_АРЧЗ
14	{Д_ОКЦ}	Р_АЦ <sup>15</sup>	Р_АБ, Р_АЦ <sup>16</sup>	–	Р_АБ
15	{Д_ОКк}	Р_ЗЗЯ	Р_ЗЗЯ	–	–
16	{Д_КФА}	Р_АР, Р_АРЧЗ	Р_АР	Р_АР	Р_АР
17	{Д_РП}	Р_АЦ, Р_АР, Р_АРЧЗ	Р_АР	Р_АР	Р_АР
18	{Д_СЕР}	УСІ	Р_АЦ	–	Р_АР, Р_АЦ
19	{Д_ВЕБ}	Р_ЗАН, Р_АЦ	Р_АЦ	Р_АЦ	Р_АЦ
20	{Д_ЗМЧ}	–	Р_ЗАН	–	–
21	{Д_МЧ}	Р_АБ, Р_АС	–	–	–
22	{Д_ЗСС}	–	Р_ЗАН	–	–
23	{Д_СС}	Р_ЗАН	–	–	–
24	{Д_ЗКСС}	Р_АБ, Р_АС	Р_АР, Р_АРЧЗ, Р_ЗЗЯ	–	–
25	{Д_ЗКФС}	Р_АБ, Р_АС	Р_АР, Р_ЗЗЯ	–	–

Основні організаційні заходи повинні передбачати:

- створення відповідального підрозділу, якому надаються повноваження щодо організації й впровадження технології захисту інформації, контролю стану захищеності інформації – служби захисту інформації у ІТС ЦСК (далі – СЗІ);
- організацію проведення обстеження середовищ функціонування ІТС ЦСК;
- облік ресурсів ІТС ЦСК, що захищаються (інформації, програм тощо), на основі використання відповідних формулярів;
- визначення політики безпеки інформації у ІТС ЦСК;
- розробку й впровадження плану захисту інформації у ІТС ЦСК;
- порядок реєстрації у ІТС ЦСК всіх користувачів і їх дій з об'єктами захисту, забезпечення контролю за її копіюванням, розмноженням, поширенням в електронному виді;

<sup>13</sup> Під правом "видалення" для {Д\_ЖУРС}, {Д\_ЖУРо}, {Д\_ЖУРв}, {Д\_ЖУРГ} мається на увазі їх повне очищення

<sup>14</sup> Кожен користувач має права доступу тільки до власного особистого ключа

<sup>15</sup> Під правом "читання" мається на увазі право на ініціювання процесу з використання особистого ключа відповідним засобом КЗІ

<sup>16</sup> Процедура генерації {Д\_ОКЦ} здійснюється спільними зусиллями користувачів з ролями Р\_АБ та Р\_АЦ



- регламентацію доступу користувачів різних категорій до об'єктів захисту ІТС ЦСК;
- порядок відновлювальних робіт і забезпечення безперервного функціонування ІТС ЦСК;
- порядок проведення модернізації КСЗІ в ІТС ЦСК та її окремих складових.

Фізична цілісність апаратних компонентів повинна забезпечуватися організаційними заходами й застосуванням пломб (наклейок, печаток та ін.) на блоках і пристроях засобів обчислювальної техніки. Повсякденний контроль цілісності й відповідності печатки (пломб, наклейок) на системному блоці ПЕОМ повинен здійснюватися користувачами. Періодичний контроль – співробітниками СЗІ.

На правовому рівні для забезпечення безпеки інформації повинні бути розроблені рішення, відносно:

- системи нормативно-правового забезпечення робіт із захисту інформації у ІТС ЦСК;
- процедур доведення до персоналу ІТС ЦСК основних положень політики безпеки інформації, їхнього навчання й підвищення кваліфікації з питань безпеки інформації;
- системи контролю своєчасності, ефективності й повноти реалізації у ІТС ЦСК рішень із захисту інформації, дотримання персоналом положень політики безпеки.

На технічному рівні для блокування загроз НСД до інформаційних ресурсів ІТС ЦСК необхідне застосування КЗЗ (вимоги, що висуваються та функції складових КЗЗ ЦСК наведені у п. 4) у складі обчислювальної системи ІТС ЦСК.

5.1.8 У ІТС ЦСК адміністратор безпеки є спеціально авторизованим користувачем (роль "розпорядника (власника)"), якому надані повноваження щодо керування потоками інформації від захищених об'єктів до користувачів.

5.1.9 Адміністративний принцип розмежування доступу до об'єктів захисту, що зберігаються на машинних носіях великої ємності, повинен забезпечуватися впровадженням таких організаційних заходів:

- фізичний доступ у приміщення де розміщуються компоненти центрального сегменту ІТС ЦСК здійснюється згідно списку та контролюється співробітниками СЗІ (штатної охорони);
- склад компонентів центрального сегменту ІТС ЦСК визначено формуляром і його незмінність контролюється адміністратором безпеки;
- у складі програмного забезпечення ІТС ЦСК відсутні програми, які не призначені для вирішення дозволених функціональних завдань.

5.1.10 На адміністратора безпеки покладається виконання таких функцій:

- призначення, введення в дію, модифікація та скасування ідентифікаційних імен користувачів згідно затверджених керівником СЗІ заявок;
- адміністрування облікових записів користувачів і груп;
- адміністрування захисту (списків контролю доступу);
- адміністрування моніторингу подій і ресурсів ОС;
- адміністрування засобів антивірусного захисту;
- адміністрування засобів КЗІ;
- адміністрування копіювання й відновлення даних.

5.1.11 Адміністратор безпеки повинен мати можливість контролювати всі пов'язані з безпекою події, оперативно корегувати список контрольованих подій безпеки, переглядати їх та заносити в архів. Доступ до цих даних повинен бути обмежений.

5.1.12 Дозволи користувачам на виконання дій з ресурсами ІТС ЦСК повинні регулюватися правами доступу. Права доступу визначають правомірність виконання користувачем конкретних дій з ресурсами.

Управління правами доступу користувачів до об'єктів і параметрами засобів центрального сегменту ІТС ЦСК повинне здійснюватися тільки адміністратором безпеки. Адміністративний принцип розмежування доступу реалізується відповідно до принципу мінімуму повноважень, згідно з яким право доступу до захищеного ресурсу може бути надане користувачеві лише за фактом службової необхідності.

Перелік фізичних осіб, що мають доступ до компонентів ІТС ЦСК, їх повноваження й службові обов'язки повинні визначатися відповідними розпорядженнями керівництва.

5.1.13 У ІТС ЦСК внутрішній користувач, який намагається одержати доступ до ресурсів, повинен виконати в обов'язковому порядку процедуру входу (реєстрації) у систему. При вході в систему повинна здійснюватися ідентифікація (розпізнавання) і автентифікація (підтвердження автентичності) користувача (суб'єкта) з використанням атрибутів, що визначені у п. 5.1.4.3.

5.1.14 Незмінність системного й функціонального ПЗ повинна перевірятися при завантаженні системи й забезпечуватися відсутністю засобів модифікації об'єктного коду програм у процесі обробки, а також функціонуванням засобів антивірусного захисту.

5.1.15 Технічний персонал ІТС ЦСК, постачальники устаткування й фахівці, що здійснюють монтаж і обслуговування технічних засобів ІТС ЦСК і не мають дозволу на доступ до даних, можуть мати доступ до програмних і апаратних засобів ІТС ЦСК лише під час робіт з тестування й інсталяції програмного забезпечення, установки й регламентного обслуговування устаткування та ін. Зазначені категорії осіб повинні мати дозвіл на доступ тільки до відомостей, які утримуються в програмній і технічній документації на ОС або на окремі її компоненти, і необхідні їм для виконання функціональних обов'язків.

5.1.16 Експлуатація КЗЗ центрального сегменту ІТС ЦСК повинна здійснюватися СЗІ.

5.2 Визначення функціональних профілів захищеності і рівня гарантій для КЗЗ складових частин ІТС ЦСК

5.2.1 Семантика профілів прийнята відповідно до НД ТЗІ 2.5-004-99.

5.2.2 Послуги безпеки, що реалізуються у КЗЗ складових частин ІТС ЦСК, повинні бути реалізовані з рівнем гарантій Г-2. Специфікації всіх критеріїв гарантій повинні в повному обсязі відповідати НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".

5.2.3 КЗЗ центрального сегменту ІТС ЦСК має реалізовувати такий профіль захищеності:

{КА-2, КО-1, КВ-1, ЦА-1, ЦВ-1, ДС-1, ДЗ-1, ДЗ-2, ДВ-2, ДР-1,  
НР-3, НИ-2, НИ-3, НК-1, НО-3, НЦ-1, НЦ-2, НТ-3, НВ-1, НА-2}.

5.2.4 Вимог до КЗЗ робочих станцій підписувачів та анонімних користувачів ЦСК не висувається.

5.2.5 Специфікації вимог (п. 5.3 – 5.4), які визначають правила взаємодії користувачів та об'єктів захисту для кожної послуги, повинні повністю відповідати описам, наведеним у НД ТЗІ 2.5-004-99 з урахуванням того, що взаємодія користувачів (об'єктів-користувачів) та об'єктів захисту ІТС ЦСК здійснюється відповідно до загальних правил розмежування доступу, атрибутів доступу визначеними у п. 5.1.4.3 та таблицях 5.1 – 5.3 цього ТЗ.

5.3 Специфікації вимог для КЗЗ центрального сегменту ІТС ЦСК

5.3.1 Базова адміністративна конфіденційність (КА-2)

КЗЗ центрального сегмента ІТС ЦСК має надавати адміністраторам можливість керувати потоками інформації від пасивних об'єктів захисту до об'єктів-користувачів з метою захисту пасивних об'єктів захисту від несанкціонованого ознайомлення з їх вмістом (компрометації).

Політика послуги має відноситися до наступних підмножин пасивних об'єктів захисту:

- {Д\_ТІКс}, {Д\_ТІУс}, {Д\_ЖУРс}, {Д\_КФА}, {Д\_РП}, {Д\_СЕР} (під час їх обробки засобами ЛОМ серверів ЦСК);
- {Д\_ТІКо}, {Д\_ТІУо}, {Д\_ЖУРо}, {Д\_ОКП}, {Д\_ОКЦ}, {Д\_ОКШс};
- {Д\_ТІКг}, {Д\_ТІУг}, {Д\_ЖУРг}.

КЗЗ центрального сегменту ІТС ЦСК повинен здійснювати розмежування доступу на підставі атрибутів доступу об'єктів-користувачів і пасивних об'єктів захисту.

КЗЗ центрального сегменту ІТС ЦСК має аналізувати усі запити на доступ від імені об'єктів-користувачів, що надаються з метою одержання інформації, яка міститься в пасивних об'єктах захисту. КЗЗ центрального сегменту ІТС ЦСК має забороняти/надавати відповідний доступ згідно загальних правил розмежування доступу (таблиці 5.3), а також значень, що містяться у списках керування доступом.

Запити на зміну прав доступу до пасивних об'єктів захисту повинні оброблятися КЗЗ центрального сегменту ІТС ЦСК тільки у тому випадку, якщо вони надходять від користувача з роллю Р\_АБ.

КЗЗ центрального сегменту ІТС ЦСК повинен надавати можливість користувачу з роллю Р\_АБ визначати конкретних користувачів та/або ролі (групи користувачів) які мають право на одержання інформації, що міститься в пасивних об'єктах захисту.

Права користувачів ІТС ЦСК, на використання об'єктів-процесів, що можуть бути використані для доступу до пасивних об'єктів захисту, визначаються наявністю атрибутів доступу, що зведені до таблиці 5.2.

При експорті (резервному копіюванні) об'єктів {Д\_ОКЦ} повинен зберігатися атрибут доступу – пароль. Вимог щодо збереження атрибутів доступу до інших пасивних об'єктів захисту під час їх експорту та імпорту не висувається.

#### 5.3.2 Повторне використання об'єктів (КО-1)

КЗЗ центрального сегмента ІТС ЦСК повинен забезпечувати коректність повторного використання поділюваних ресурсів, гарантуючи, що у випадку, якщо поділюваний ресурс виділяється новому об'єкту-користувачу або процесу, він не містить інформації, що залишилася від попереднього об'єкта-користувача або процесу.

У якості поділюваного ресурсу повинні розглядатися:

- оперативна пам'ять компонентів центрального сегменту ІТС ЦСК (центрального серверів, серверів взаємодії, серверу моніторингу та синхронізації часу, РМ обслуговуючого персоналу);
- тимчасові змінні ПК РМ генерації ключів в яких містяться значення {Д\_ОКк}.

Перш ніж процес, що працює з правами об'єкта-користувача, зможе одержати в своє розпорядження звільнений іншим процесом пасивний об'єкт, встановлені для попереднього об'єкта-користувача або процесу права доступу до даного пасивного об'єкта повинні бути скасовані.

Перш ніж процес, що працює з правами об'єкта-користувача, зможе одержати в своє розпорядження звільнений іншим процесом пасивний об'єкт, вся інформація, що міститься в даному пасивному об'єкті, повинна стати недосяжною.

#### 5.3.3 Мінімальна конфіденційність при обміні (КВ-1)

Політика конфіденційності при обміні, що реалізується КЗЗ центрального сегменту ІТС ЦСК, повинна відноситись до (реалізовуватися для) наступних підмножин пасивних об'єктів захисту:

- {Д\_ТІКс}, {Д\_ТІУс}, {Д\_ЖУРс}, {Д\_РП}, {Д\_КФА}, {Д\_СЕР} (під час їх передачі між компонентами ЛОМ серверів ЦСК та РМ обслуговуючого персоналу);
- {Д\_ТІКс}, {Д\_ТІУс}, {Д\_ЖУРс} засобів КЗІ (мережних криптомодулів, криптомодулів, АПЗ КЗІ) (під час їх передачі між відповідними засобами КЗІ та програмними засобами, що встановлені на компонентах центрального сегменту ІТС ЦСК (центрального сервера, сервера взаємодії, РМ обслуговуючого персоналу);
- {Д\_РП}, {Д\_КФА} (під час їх передачі між компонентами ЛОМ серверів ЦСК та РМ віддалених адміністраторів реєстрації).

При реалізації політики послуги КЗЗ центрального сегменту ІТС ЦСК має використовувати:

- {Д\_ОКП}, {Д\_ОКЦ}, {Д\_СЕР}.

Політика конфіденційності при обміні, що реалізується КЗЗ центрального сегменту ІТС ЦСК, повинна реалізовуватись за рахунок використання функцій шифрування за алгоритмом ДСТУ ГОСТ 28147:2009 (режим простої заміни, режим гамування). Користувачі не повинні мати можливості впливати на рівень захисту.

КЗЗ центрального сегменту ІТС ЦСК повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається.

#### 5.3.4 Мінімальна адміністративна цілісність (ЦА-1)

КЗЗ центрального сегмента ІТС ЦСК має надавати адміністраторам можливість керувати потоками інформації від об'єктів-користувачів до пасивних об'єктів захисту з

метою захисту пасивних об'єктів захисту від несанкціонованого створення, модифікації або видалення.

Політика послуги має відноситися до наступних підмножин пасивних об'єктів захисту:

- {Д\_ТІКс}, {Д\_ТІУс}, {Д\_ЖУРс}, {Д\_КФА}, {Д\_РП}, {Д\_СЕР}, {Д\_МЧ}, {Д\_ЗКСС} та {Д\_ЗКСС} (під час їх обробки засобами ЛОМ серверів ЦСК);
- {Д\_ТІКо}, {Д\_ТІУо}, {Д\_ЖУРо}, {Д\_ОКП}, {Д\_ОКЦ};
- {Д\_ТІКГ}, {Д\_ТІУГ}, {Д\_ЖУРГ}.

КЗЗ центрального сегменту ІТС ЦСК повинен здійснювати розмежування доступу на підставі атрибутів доступу об'єктів-користувачів і пасивних об'єктів захисту.

КЗЗ центрального сегменту ІТС ЦСК має аналізувати усі запити на доступ від імені об'єктів-користувачів, що надаються з метою модифікації інформації, яка міститься в пасивних об'єктах захисту. КЗЗ центрального сегменту ІТС ЦСК має забороняти/надавати відповідний доступ згідно загальних правил розмежування доступу (таблиці 5.3), а також значень, що містяться у списках керування доступом.

Запити на зміну прав доступу до пасивних об'єктів захисту повинні оброблятися КЗЗ центрального сегменту ІТС ЦСК тільки у тому випадку, якщо вони надходять від користувача з роллю Р\_АБ.

КЗЗ центрального сегменту ІТС ЦСК повинен надавати можливість користувачу з роллю Р\_АБ визначати конкретних користувачів та/або ролі (групи користувачів) які мають право на модифікацію інформації, що міститься в пасивних об'єктах захисту.

При експорті (резервному копіюванні) об'єктів {Д\_ОКЦ}, {Д\_ОКк} повинен зберігатися атрибут доступу – пароль. Вимог щодо збереження атрибутів доступу до інших пасивних об'єктів захисту під час їх експорту та імпорту не висувається.

#### 5.3.5 Мінімальна цілісність при обміні (ЦВ-1)

Політика цілісності при обміні, що реалізується КЗЗ центрального сегменту ІТС ЦСК, повинна відноситись до (реалізовуватися для) наступних підмножин пасивних об'єктів захисту:

- {Д\_ТІКс}, {Д\_ТІУс}, {Д\_ЖУРс}, {Д\_РП}, {Д\_КФА}, {Д\_СЕР}, {Д\_ЗКСС} та {Д\_ЗКФС} (під час їх передачі між компонентами ЛОМ серверів ЦСК та РМ обслуговуючого персоналу);
- {Д\_ТІКс}, {Д\_ТІУс}, {Д\_ЖУРс} засобів КЗІ (мережних криптомодулів, криптомодулів, АПЗ КЗІ) (під час їх передачі між відповідними засобами КЗІ та програмними засобами, що встановлені на компонентах центрального сегменту ІТС ЦСК (центральної сервера, сервера взаємодії, РМ обслуговуючого персоналу);

При реалізації політики послуги КЗЗ центрального сегменту ІТС ЦСК має використовувати:

- {Д\_ОКП}, {Д\_ОКЦ}, {Д\_СЕР}.

Політика цілісності при обміні, що реалізується КЗЗ центрального сегменту ІТС ЦСК, повинна реалізовуватись за рахунок використання функцій обчислення імітовставки за алгоритмом ДСТУ ГОСТ 28147:2009. Користувачі не повинні мати можливості впливати на рівень захисту.

КЗЗ центрального сегменту ІТС ЦСК повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається.

### 5.3.6 Стійкість при обмежених відмовах (ДС-1)

КЗЗ центрального сегменту ІТС ЦСК повинен забезпечувати, що відмова підмножини компонентів центрального сегмента ІТС ЦСК не призведе до неможливості функціонування центрального сегмента ІТС ЦСК у цілому.

**Відмова одного із задубльованих компонентів центрального сегменту ІТС ЦСК:**

- ОС центральних серверів;
- ОС серверів взаємодії;
- ОС РМ обслуговуючого персоналу;
- СКБД серверів взаємодії;
- ПК центральних серверів;
- ПК серверів взаємодії;
- МЕ;
- комутаторів ЛОМ;
- мережних криптомодулів
- криптографічних модулів;

не повинна призводити до недоступності послуг, що надаються підписувачам, заявникам та анонімним користувачам ЦСК. У гіршому випадку допускається збільшення часу їх обслуговування.

Відмова РС генерації ключів повинна призводити лише до неможливості генерації ключів користувачів у ЦСК, але не до погіршення характеристик обслуговування інших користувачів.

**Відмова сервера моніторингу та синхронізації часу повинна призводити лише до неможливості моніторингу центрального сегменту ІТС ЦСК та неможливості синхронізації часу з сервісами точного часу.**

Технічні засоби КЗЗ центрального сегменту ІТС ЦСК повинні мати засоби індикації та/або оповіщення адміністраторів про відмову будь-якого захищеного компонента.

Перелік припустимих відмов компонентів центрального сегменту ІТС ЦСК має бути уточнений на етапі технічного проектування.

### 5.3.7 Модернізація (ДЗ-1)

КЗЗ центрального сегменту ІТС ЦСК повинен надавати можливість проведення модернізації компонентів центрального сегменту ІТС ЦСК, при цьому модернізація не повинна призводити до переривання виконання КЗЗ центрального сегменту ІТС ЦСК функцій захисту та необхідності проведення додаткової державної експертизи КСЗІ.

КЗЗ центрального сегменту ІТС ЦСК повинен надавати можливість заміни/модернізації:

а) засобів КЗІ на такі самі або аналогічні засоби, за умови наявності у останніх експертного висновку Адміністрації Держспецзв'язку у сфері КЗІ та дотримання вимог визначених у ТЗ та технічних умовах на засіб КЗІ, що проходить випробування в ході державної експертизи КСЗІ в центральному сегменті ІТС ЦСК.

б) засобів ТЗІ (МЕ, комутатори ЛОМ, ЗАЗ центральних серверів, ЗАЗ для РМ генерації ключів) на такі самі або аналогічні засоби, за умови реалізації останніми функцій захисту (що вимагаються у цьому ТЗ). Відповідність функцій захисту має бути підтверджена експертним висновком Адміністрації Держспецзв'язку у сфері ТЗІ.

Заміна компонентів має бути доступна користувачам з роллю Р\_АБ та/або Р\_АС.

Порядок модернізації та здійснення випробувань після модернізації складу компонентів центрального сегменту ІТС ЦСК має бути визначений у методиці модернізації.

На етапі техноробочого проектування має бути уточнено склад компонентів до яких відноситься політика послуги.

#### 5.3.8 Обмежена гаряча заміна (ДЗ-2)

КЗЗ центрального сегменту ІТС ЦСК повинен забезпечувати доступність послуг і ресурсів центрального сегмента ІТС ЦСК під час заміни його окремих компонентів (за рахунок дублювання компонентів, організації кластерів).

Політика послуги має поширюватися на такі компоненти центрального сегменту ІТС

ЦСК:

- центральні сервери;
- сервери взаємодії;
- РМ обслуговуючого персоналу;
- СКБД центральних серверів;
- СКБД серверів взаємодії;
- МЕ;
- комутатори ЛОМ;
- мережні криптомодулі;
- криптомодулі.

Заміна компонентів має бути доступна користувачам з роллю Р\_АБ та/або Р\_АС.

Модернізація не повинна призводити до необхідності проведення додаткової державної експертизи КСЗІ в центральному сегменті ІТС ЦСК.

На етапі техноробочого проектування має бути уточнено склад компонентів до яких відноситься політика послуги.

#### 5.3.9 Автоматизоване відновлення (ДВ-2)

КЗЗ центрального сегменту ІТС ЦСК повинен забезпечити доступність послуг і ресурсів центрального сегмента ІТС ЦСК шляхом автоматизованого відновлення після відмов окремих компонентів, а саме:

- ОС центральних серверів;
- ОС серверів взаємодії;
- ОС сервера моніторингу та синхронізації часу;
- ОС РМ обслуговуючого персоналу;
- ОС РМ генерації ключів;
- СКБД центральних серверів;
- СКБД серверів взаємодії.

У разі неможливості відновити працездатність компонента, що відмовив, КЗЗ центрального сегменту ІТС ЦСК повинен перевести відповідні компоненти до стану із якого повернути до нормального функціонування може тільки користувачі з роллю Р\_АБ та/або Р\_АС.

КЗЗ центрального сегменту ІТС ЦСК повинен надавати можливість користувачам з роллю Р\_АБ та/або Р\_АС відновити працездатність компонентів, що відмовили, у ручному режимі із застосуванням резервних/еталонних копій. Повинні існувати ручні процедури для:

а) відновлення безпечних параметрів:

- ОС центральних серверів;
- ОС серверів взаємодії;
- ОС сервера моніторингу та синхронізації часу;
- ОС РМ обслуговуючого персоналу;
- ОС РМ генерації ключів;
- СКБД центральних серверів;

- СКБД серверів взаємодії;
- МЕ;
- комутаторів ЛОМ.

б) відновлення особистих ключів:

- мережних криптомодулів;
- криптомодулів.

Рівні відмов та склад компонентів на які поширюється політика послуги може бути уточнений на етапі технічного проектування.

#### 5.3.10 Квоти (ДР-1)

КЗЗ центрального сегменту ІТС ЦСК повинен забезпечувати доступність послуг і ресурсів центрального сегмента ІТС ЦСК шляхом керування обсягом ресурсів, що виділяються користувачам.

Обмеження на ресурси СКБД центральних серверів та СКБД серверів взаємодії:

- максимальний час виконання запитів, що надходять з віддаленого вузла;
- максимальна кількість конкурентних з'єднань.

Обмеження на ресурси ПЗ НТТР-серверу:

- максимальна кількість користувачів, що можуть одночасно отримувати доступ до ПЗ НТТР-серверу;
- кількість обробників запитів користувачів ПЗ НТТР-серверу.

Запити на зміну встановлених обмежень повинні оброблятися КЗЗ центрального сегменту ІТС ЦСК тільки в тому випадку, якщо вони надходять від Р\_АБ або Р\_АС.

На етапі техноробочого проектування обмеження на ресурси можуть бути уточнені.

#### 5.3.11 Сигналізація про небезпеку (НР-2)

КЗЗ центрального сегменту ІТС ЦСК повинен здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки, а саме:

- отримання чи спроба отримання користувачем доступу (будь-якого виду) до об'єктів захисту;
- результати ідентифікації та автентифікації користувачів ІТС ЦСК;
- викриття порушення цілісності або відмова компонентів, що входять до складу центрального сегменту ІТС ЦСК;
- відновлення працездатності компонентів, що входять до складу центрального сегменту ІТС ЦСК.

Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача (об'єкта-користувача), програмного засобу зі складу центрального сегменту ІТС ЦСК, що мали відношення до кожної зареєстрованої події.

КЗЗ центрального сегменту ІТС ЦСК повинен контролювати одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушення політики безпеки ІТС ЦСК, а саме відмова компонентів, що входять до складу центрального сегменту ІТС ЦСК.

КЗЗ центрального сегменту ІТС ЦСК повинен негайно інформувати користувачів з ролями Р\_АБ, Р\_АС про події засобами електронної пошти/мобільного зв'язку (sms).

Користувачі з ролями Р\_АБ, Р\_АС повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.



КЗЗ центрального сегменту ІТС ЦСК повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Має бути заборонено редагування вмісту журналів реєстрації. Єдиною операцією, що визначена над об'єктам типу журнал реєстрації, що призводить до зміни її вмісту має бути повне очищення.

#### 5.3.12 Одиночна ідентифікація і автентифікація (НИ-2)

КЗЗ центрального сегменту ІТС ЦСК повинен визначати і перевіряти особистість користувача, що намагається одержати доступ до апаратно-програмних та апаратних компонентів ІТС ЦСК шляхом безпосереднього підключення або підключення через контрольоване середовище.

Атрибути, що використовується для ідентифікації та автентифікації користувачів у компонентах центрального сегмента ІТС ЦСК наведені у таблиці 5.2.

Послуга повинна реалізовуватися КЗЗ центрального ІТС ЦСК із застосуванням захищеного механізму одного з типів:

- "знання чогось", а саме: логін та/або пароль;
- "володіння чимось", а саме: АПЗ КЗІ.

Кожний користувач, до якого відноситься політика послуги, повинен однозначно ідентифікуватися КЗЗ центрального сегмента ІТС ЦСК.

КЗЗ центрального сегменту ІТС ЦСК повинен забезпечувати захист даних автентифікації від несанкціонованого читання та модифікації.

#### 5.3.13 Множина ідентифікація і автентифікація (НИ-3)

КЗЗ центрального сегменту ІТС ЦСК повинен визначати і перевіряти особистість користувача, що намагається одержати доступ до апаратно-програмних та апаратних компонентів ІТС ЦСК шляхом підключення через неконтрольоване середовище.

Атрибути, що використовується для ідентифікації та автентифікації користувачів у компонентах центрального сегмента ІТС ЦСК наведені у таблиці 5.2.

Послуга повинна реалізовуватися КЗЗ центрального сегмента ІТС ЦСК із одночасним застосуванням захищених механізму таких типів:

- "знання чогось", а саме: логін та/або пароль;
- "володіння чимось", а саме: АПЗ КЗІ.

Кожний користувач, до якого відноситься політика послуги, повинен однозначно ідентифікуватися КЗЗ центрального сегмента ІТС ЦСК.

КЗЗ центрального сегменту ІТС ЦСК повинен забезпечувати захист даних автентифікації від несанкціонованого читання та модифікації.

#### 5.3.14 Однонаправлений достовірний канал (НК-1)

КЗЗ центрального сегменту ІТС ЦСК має гарантувати користувачам можливість безпосередньої взаємодії з ним.

Політика послуги має поширюватися на:

- внутрішніх користувачів усіх категорій;
- заявників.

Встановлення достовірного зв'язку між користувачем до якого поширюється політика послуги, і КЗЗ центрального сегменту ІТС ЦСК, повинно здійснюватися з використанням захищеного (від перехоплення чи підміни) механізму введення користувачем свого паролю.

Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації користувачів, до яких відноситься політика послуги. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

### 5.3.15 Розподіл обов'язків на підставі привілеїв (НО-3)

КЗЗ центрального сегменту ІТС ЦСК повинен підтримувати:

- адміністративні ролі (P\_АБ, P\_АС);
- користувальницькі ролі (P\_АР, P\_АРЧЗ, P\_АЦ, P\_ЗПП, P\_ЗАН, P\_ЗЗЯ).

Користувач ІТС ЦСК повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

### 5.3.16 КЗЗ з контролем цілісності (НЦ-1)

КЗЗ центрального сегменту ІТС ЦСК повинен реалізовувати механізми контролю цілісності підмножини своїх компонентів з метою виявлення фактів їх несанкціонованої модифікації.

Політика послуги має поширюватися на:

- ЗАЗ центральних серверів;
- МЕ;
- комутатори ЛОМ;
- мережні криптомодулі;
- криптомодулі;
- АПЗ КЗІ;
- ПЗ користувача ЦСК;
- ЗАЗ для РМ генерації ключів.

У разі виявлення порушення цілісності свого компоненту КЗЗ центрального сегменту ІТС ЦСК повинен повідомити користувача з роллю P\_АБ або P\_АС і перевести об'єкт, цілісність якого було порушено, до стану з якого повернути його до нормального функціонування може тільки користувач з роллю P\_АБ або P\_АС.

За допомогою організаційних заходів має бути забезпечено неможливість завантаження серверів та робочих місць зі складу комплексу технічних засобів центрального сегменту ІТС ЦСК із зовнішніх носіїв або через мережевий інтерфейс.

На етапі технічного проектування обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ центрального сегмента ІТС ЦСК і всі запити на доступ до захищених об'єктів контролюються ним, можуть бути уточнені.

### 5.3.17 КЗЗ з гарантованою цілісністю (НЦ-2)

КЗЗ центрального сегменту ІТС ЦСК повинен підтримувати домен для виконання підмножини своїх компонентів з метою захисту від зовнішніх впливів і несанкціонованої модифікації та/або втрати керування.

Політика послуги має поширюватися на:

- КЗЗ ОС центральних серверів;
- КЗЗ ОС серверів взаємодії;
- КЗЗ ОС сервера моніторингу та синхронізації часу;
- КЗЗ ОС РМ обслуговуючого персоналу;
- КЗЗ ОС РМ генерації ключів

та усі програмні засоби, що входять до складу КЗЗ центрального сегменту ІТС ЦСК та функціонують під їх керуванням.

За допомогою організаційних заходів має бути забезпечено неможливість завантаження серверів та робочих місць зі складу комплексу технічних засобів центрального сегменту ІТС ЦСК із зовнішніх носіїв або через мережевий інтерфейс.

На етапі технічного проектування обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ центрального сегмента ІТС ЦСК і всі запити на доступ до захищених об'єктів контролюються ним, можуть бути уточнені.

#### 5.3.18 Самотестування в реальному часі (НТ-3)

КЗЗ центрального сегмента ІТС ЦСК повинен перевіряти і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КЗЗ центрального сегмента ІТС ЦСК.

Процедурами, що мають використовуватися для оцінки правильності функціонування КЗЗ центрального сегмента ІТС ЦСК є:

- тестування на предмет вірусного зараження;
- перевірка коректності конфігураційних файлів окремих програмних засобів;
- тестування правильності криптографічних перетворень, що реалізовані у засобах КЗІ зі складу КЗЗ центрального сегмента ІТС ЦСК;
- діагностика функціонування мережних вузлів та перевірка функціонування спеціалізованих програмних сервісів.

КЗЗ центрального сегмента ІТС ЦСК має бути здатним виконувати набір тестів з метою оцінки правильності функціонування. Тести повинні виконуватися при запуску та за запитом користувача з роллю Р\_АБ, Р\_АС або іншого уповноваженого користувача.

Перелік процедур та тестів, що призначені для реалізації послуги може бути уточнений на етапі технічного проектування.

#### 5.3.19 Автентифікація вузла (НВ-1)

КЗЗ центрального сегмента ІТС ЦСК перед початком обміну повинен забезпечувати:

- взаємну ідентифікацію та автентифікацію апаратно-програмних засобів КЗІ (мережні криптомодулі, криптомодулі, АПЗ КЗІ) та програмних засобів, що встановлені на компонентах центрального сегмента ІТС ЦСК (центральної серверах, серверах взаємодії, РМ обслуговуючого персоналу).

Атрибутами доступу, що мають використовуватися при реалізації послуги повинні бути особистий і відкритий (у складі сертифіката) ключі електронного цифрового підпису компонентів КЗЗ ІТС ЦСК, що взаємодіють.

Підтвердження ідентичності має здійснюватися на основі затвердженого протоколу автентифікації, що використовує механізм ЕЦП.

#### 5.3.20 Автентифікація відправника з підтвердженням (НА-2)

КЗЗ центрального сегмента ІТС ЦСК повинен забезпечувати захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу (процесу), тобто той факт, що об'єкт був створений певним користувачем (процесом).

Політика послуги має відноситися до:

- користувачів з ролями: Р\_АЦ, Р\_АР, Р\_АРЧЗ, Р\_ЗПП, Р\_ЗЗЯ;
- процесів: ПК центральної серверів;
- об'єктів захисту: {Д\_СЕР}, {Д\_МЧ}, {Д\_ЗКСС}, {Д\_ЗКФС}.

Атрибутом, що дозволяє однозначно встановити, що об'єкти захисту до яких відноситься політика послуги, були створені одним з користувачів (процесів) до яких відноситься політика послуги має бути ЕЦП.

Атрибутами користувачів (процесів) на яких поширюється політика послуги має бути особистий ключ ЕЦП та сертифікат відкритого ключа.

Процедурою, що дозволяє однозначно встановити, що об'єкт захисту був створений певним користувачем (процесом), є перевірка ЕЦП від даних, що перевіряються за

криптографічним алгоритмом ЕЦП, що визначений ДСТУ 4145-2002. Для забезпечення можливості однозначного підтвердження належності об'єкта незалежною третьою стороною, у складі КЗЗ центрального сегмента ІТС ЦСК при формуванні та перевірці ЕЦП мають використовуватися надійні засоби ЕЦП та посилені сертифікати відкритих ключів.

У якості незалежної третьої сторони має виступати акредитований центр сертифікації ключів.

5.4 Вимоги до комплексної системи захисту інформації в частині захисту від витоку інформації технічними каналами та захисту від спеціальних впливів

5.4.1 Центральні сервери та криптомодулі повинні розміщуватись у екранованій шафі, яка відповідає вимогам Додатку 1 до Правил посиленої сертифікації.

5.4.2 Електроживлення центральних серверів та криптомодулів повинно здійснюватись через фільтри електроживлення, які відповідають вимогам Додатку 1 до Правил посиленої сертифікації.

5.4.3 Для з'єднання обладнання, яке знаходиться у екранованій шафі, з обладнанням, яке знаходиться за межами екранованої шафи, повинні використовуватись оптоволоконні лінії зв'язку.

## **6 ВИМОГИ ДО СКЛАДУ ПРОЕКТНОЇ ТА ЕКСПЛУАТАЦІЙНОЇ ДОКУМЕНТАЦІЇ**

6.1 Проектна документація на комплексну систему захисту інформації повинна включати:

- пояснювальну записку техноробочого проекту КСЗІ;
- план захисту інформації у ІТС ЦСК (сукупність документів), у якому повинні бути визначені:
  - перелік інформації, що підлягає автоматизованому обробленню у ІТС ЦСК та потребує захисту;
  - опис моделі загроз для інформації, оброблюваної у ІТС ЦСК;
  - опис політики безпеки інформації у ІТС ЦСК.

6.2 До складу документації техноробочого проекту повинні входити: основні технічні рішення щодо побудови КСЗІ в ІТС ЦСК; опис складу КЗЗ; опис функціонування механізмів захисту; способи реалізації послуг безпеки; основні правила експлуатації КЗЗ.

6.3 Склад експлуатаційної документації ІТС ЦСК:

- положення про службу захисту інформації;
- інструкція з безпечної інсталяції, генерації і запуску КЗЗ;
- порядок модернізації ІТС ЦСК;
- інструкція з забезпечення безперервного функціонування;
- інструкція з контролю за функціонуванням;
- інструкція про порядок реєстрації користувачів;
- інструкція про порядок забезпечення антивірусного захисту;
- настанови операторам;
- настанови адміністраторам;
- настанова адміністратору безпеки (відповідальному за захист).

6.4 Під час розроблення цих документів дозволяється поєднувати кілька з них у вигляді окремих розділів в одному документі.

6.5 Остаточний склад і зміст документації має бути уточнений на етапі техноробочого проекту.

## 7 ЕТАПИ ВИКОНАННЯ РОБІТ

7.1 Відповідно до вимог НД ТЗІ 3.7-003-2005 створення КСЗІ в ІТС ЦСК здійснюється поетапно. Узагальнені етапи виконання робіт зі створення КСЗІ в ІТС ЦСК наведені у таблиці 7.1.

Таблиця 7.1 – Етапи виконання робіт

Стадія	Етапи робіт	Результат роботи
1 Технічне завдання	1.1 Обстеження середовищ функціонування ІТС ЦСК. 1.2 Розробка та погодження технічного завдання на створення КСЗІ в ІТС ЦСК	1. Акт обстеження середовищ функціонування ІТС ЦСК. 2. Затверджене ТЗ на створення КСЗІ в ІТС ЦСК
2 Техноробочий проект	2.1 Розробка пропозицій до техноробочого проекту КСЗІ в ІТС ЦСК. 2.2 Розробка робочої та експлуатаційної документації на КСЗІ в ІТС ЦСК	1. Пояснювальна записка до техноробочого проекту. 2. Робоча та експлуатаційна документація на КСЗІ в ІТС ЦСК
3 Введення в дію та перевірка працездатності КСЗІ	3.1 Реалізація (впровадження) заходів щодо КСЗІ в ІТС ЦСК. 3.2 Розробка і затвердження "Програми і методики попередніх випробувань КСЗІ в ІТС ЦСК". 3.3 Проведення попередніх випробувань КСЗІ в ІТС ЦСК. 3.4 Дослідна експлуатація КСЗІ в ІТС ЦСК. 3.5 Корегування експлуатаційної й супровідної документації КСЗІ в ІТС ЦСК	1. КЗЗ, реалізовані і інсталювані у ЦСК. 2. Програма і методика попередніх випробувань КСЗІ в ІТС ЦСК. 3. Акт та протокол попередніх випробувань КСЗІ в ІТС ЦСК. 4. Дороблена експлуатаційна та супровідна документація. 5. Документація до проведення Державної експертизи
4 Державна експертиза	4.1 Супровід експертних робіт	Атестат відповідності (за результатами державної експертизи) КСЗІ в ІТС ЦСК

## 8 ПОРЯДОК ВНЕСЕННЯ ЗМІН І ДОПОВНЕНЬ ДО ТЗ

Зміни і доповнення до ТЗ після його затвердження оформляються окремим доповненням, що затверджується в такому ж порядку, як і це ТЗ.

## **9 ПОРЯДОК ПРОВЕДЕННЯ ВИПРОБУВАНЬ КСЗІ**

9.1 Об'єктом випробувань є КСЗІ в ІТС ЦСК.

9.2 Метою випробувань є визначення відповідності досягнутого в КСЗІ рівня захищеності інформації вимогам ТЗ і визначення готовності до експлуатації.

9.3 Випробування КСЗІ в ІТС ЦСК здійснюється з врахуванням змісту етапів та черговості виконання робіт з побудови КСЗІ (п . 7).

9.4 Проводяться наступні види випробувань КСЗІ: попередні, дослідна експлуатація, державна експертиза. За результатами попередніх випробувань складається акт, у якому зазначаються результати випробувань і дається висновок щодо можливості впровадження КСЗІ в ІТС ЦСК у дослідну експлуатацію.

9.5 КСЗІ в ІТС ЦСК вводиться у дослідну експлуатацію згідно з наказом. Після завершення дослідної експлуатації складається акт, у якому наводяться результати дослідної експлуатації і дається висновок про можливість представлення КСЗІ в ІТС ЦСК на державну експертизу.

9.6 Державна експертиза КСЗІ в ІТС ЦСК здійснюється відповідно до "Положення про державну експертизу в сфері технічного захисту інформації", яке затверджено наказом Адміністрації Держспецзв'язку від 16.05.2007 р. №93 (із змінами затвердженими наказом Адміністрації Держспецзв'язку від 10.10.2012 р. №567).