

**Товариство з обмеженою відповідальністю  
«Український сертифікаційний центр»**

**ПОГОДЖЕНО**

Перший заступник Голови Державної служби спеціального зв'язку та захисту інформації України

\_\_\_\_\_ О.І. Сиров  
“ \_\_\_ ” \_\_\_\_\_ 2008 р.

**ЗАТВЕРДЖУЮ**

Директор  
Товариства з обмеженою відповідальністю  
«Український сертифікаційний центр»

\_\_\_\_\_ О.С. Шаталов  
“ \_\_\_ ” \_\_\_\_\_ 2008 р.

**Регламент  
роботи акредитованого центру сертифікації ключів  
товариства з обмеженою відповідальністю  
«Український сертифікаційний центр»**

На 24 аркушах

Київ 2008

<b>Вступ</b> .....	4
1. Загальні положення.....	4
1.1. Терміни та визначення .....	4
1.2. Регламент ЦСК.....	4
1.3. Поширення дії Регламенту.....	5
1.4. Порядок ознайомлення із положеннями Регламенту .....	5
1.5. Порядок внесення змін до Регламенту .....	5
1.6. Ідентифікаційні дані ЦСК .....	6
2. Діяльність ЦСК .....	6
3. Обслуговування та використання сертифікатів, суб'єкти та відносини між ними .....	6
3.1. Обслуговування сертифікатів .....	6
3.2. Використання сертифікатів.....	7
3.3. Обмеження щодо використання сертифікатів .....	7
4. Порядок доступу до відкритої інформації (розповсюдження інформації).....	7
4.1. Адреса загальнодоступного ресурсу.....	7
4.2. Перелік інформації, розміщеної на даному ресурсі: .....	7
4.3. Порядок публікації кореневого та службових сертифікатів ЦСК. ....	7
4.4. Порядок публікації сертифікатів ключів підписувачів .....	8
4.5. Порядок публікації списку відкликаних сертифікатів .....	8
5. Порядок автентифікації та авторизації заявника .....	8
5.1. Вимоги щодо встановлення особи заявника під час реєстрації .....	8
5.1.1. Загальні положення .....	8
5.1.2. Встановлення юридичної особи.....	8
5.1.3. Встановлення фізичної особи.....	9
5.2. Захист персональних даних підписувачів .....	10
5.3. Підтвердження володіння заявником особистим ключем .....	11
5.4. Автентифікація підписувача при зміні статусу сертифіката.....	11
6. Порядок генерації ключів підписувачів.....	11
6.1. Генерація ключів на особистому обладнанні. ....	11
6.2. Генерація ключів на робочій станції ЦСК.....	11
7. Створення та зміна статусу сертифіката підписувача .....	12
7.1. Порядок створення сертифікатів відкритих ключів підписувачів, визнання сертифіката його власником.....	12
7.2. Повторне формування сертифіката ключа .....	13
7.3. Використання сертифіката та особистого ключа підписувача.....	13
7.3.1. Права та обов'язки підписувача.....	13
7.3.2. Підписувачі мають право:.....	13
7.3.3. Обов'язки користувача .....	14
7.4. Порядок блокування сертифікатів ключів.....	14
7.4.1. Блокування сертифіката по телефону.....	14
7.4.2. Блокування сертифіката за заявою у електронній формі .....	14
7.4.3. Блокування сертифіката за заявою у письмовій формі.....	14
7.5. Порядок поновлення чинності сертифікатів ключів .....	15
7.6. Порядок скасування сертифікатів ключів .....	15
7.6.1. Скасування сертифіката за заявою у електронній формі .....	15
7.6.2. Скасування сертифіката за заявою у письмовій формі.....	15
7.7. Термін дії сертифікатів підписувачів.....	15
8. Управління та операційний контроль .....	16
8.1. Фізичне середовище .....	16
8.2. Процедурний контроль.....	17
8.2.1. Права ЦСК.....	17

---

8.2.2.	Зобов'язання ЦСК під час формування та обслуговування сертифікатів: .....	17
8.2.3.	ЦСК під час формування та обслуговування сертифікатів несе відповідальність за: .....	18
8.3.	Організаційна структура ЦСК, функціональні обов'язки та відповідальність.....	18
8.3.1.	Реєстраційний центр.....	18
8.3.2.	Сертифікаційний центр.....	18
8.3.2.1.	Обов'язки та відповідальність адміністратора сертифікації. ....	19
8.3.2.2.	Обов'язки та відповідальність оператора сертифікації: .....	19
8.3.3.	Служба захисту інформації .....	19
8.3.4.	Технічна служба .....	19
8.4.	Ведення журналів аудиту автоматизованої системи.....	20
8.5.	Ведення архівів .....	20
9.	Управління ключами.....	21
9.1.	Порядок генерації, захисту та доступу до особистого ключа ЦСК.....	21
9.2.	Резервування особистого ключа, порядок та умови зберігання, доступу та використання резервної копії.....	22
9.3.	Протоколювання операцій з особистим ключем ЦСК.....	23
10.	Термін дії особистого ключа ЦСК .....	23
10.1.	Порядок планової зміни ключів ЦСК .....	23
10.2.	Порядок позапланової зміни ключів ЦСК.....	23
11.	Порядок синхронізації часу у ПТК.....	24

## Вступ

Рішення у сфері використання технологій інфраструктури відкритих ключів (Public key infrastructure) повинні відповідати міжнародним стандартам ISO/IEC, IETF, ETSI. Згадані стандарти передбачають достатню гнучкість відносно технічних аспектів: протоколів, форматів даних, технологічних процедур. Для деяких параметрів об'єктів вони передбачають перелік альтернативних рішень. В той же час ряд специфічних аспектів не розглядаються, не враховуються і вимоги Українського законодавства. З метою забезпечення сумісності програмно-технічних рішень, які використовуються сертифікаційними центрами, з програмно-технічними рішеннями, що використовують користувачі, і розроблені технічні специфікації, засновані на міжнародних стандартах. Технічні специфікації визначають:

- перелік стандартів, яких необхідно дотримуватись при побудові програмного забезпечення сертифікаційного центру та користувача;
- обмеження можливих альтернативних реалізацій, що передбачені міжнародними стандартами;
- технічні вимоги до об'єктів, які не визначені міжнародними стандартами, але потрібні для забезпечення сумісності цих об'єктів.

Крім програмно-технічних рішень, що застосовані в сертифікаційному центрі, цей регламент визначає правила взаємодії сертифікаційного центру, підписувачів та користувачів, порядок і процедури обслуговування сертифікатів.

### 1. Загальні положення.

#### 1.1. Терміни та визначення

Розпізнавальне ім'я – сукупність реквізитів підписувача, що забезпечують можливість однозначного визначення належності сертифіката цьому підписувачу з поміж інших сертифікатів, сформованих в акредитованому центрі сертифікації ключів Товариства з обмеженою відповідальністю "Український сертифікаційний центр" (надалі – ЦСК);

Заява на формування (зміну статусу) сертифіката – заява фізичної чи юридичної особи (уповноваженої особи) у письмовій або електронній формі щодо формування (зміни статусу) сертифіката, яка надається до ЦСК (ВПР) відповідно до порядку, встановленого Регламентом;

ВПР - відокремлений пункт реєстрації, організаційна структура ЦСК.

Звернення підписувача – звернення підписувача або уповноваженої особи до ЦСК (ВПР), щодо реєстрації, формування або зміни статусу сертифіката;

Службовий ключ – особистий електронний ключ, спеціально сформований для посадової особи ЦСК або сервісу. Посадова особа ЦСК або сервіс використовують службовий ключ для реалізації функцій, пов'язаних із обслуговуванням посиленних сертифікатів.

Службовий сертифікат – сертифікат відкритого ключа, що відповідає службовому ключу.

Особистий ключ сертифікаційного центру – секретний ключ ЦСК який згенеровано відповідно до процедур на обладнанні ПТК і який має відповідний відкритий ключ з сертифікатом ЦЗО.

ПТК – програмно-технічний комплекс.

Інші терміни, що застосовуються у Регламенті, відповідають термінам, наведеним у Законах України «Про електронний цифровий підпис», «Про електронні документи та електронний документообіг», постанові Кабінету Міністрів України від 13.07.2004 № 903 «Про затвердження Порядку акредитації ЦСК сертифікації ключів» та політиці сертифікації.

#### 1.2. Регламент ЦСК

Регламент роботи ЦСК (надалі – Регламент) розроблений відповідно до Закону України «Про електронний цифровий підпис», Закону України «Про електронні документи та електронний документообіг», Порядку акредитації ЦСК сертифікації ключів, затвердженого постановою Кабінету Міністрів України від 13.07.2004 №903, Правил посиленої сертифікації, затверджених наказом ДСТСЗІ СБ України від 10.05.06 «Про внесення змін до Правил посиленої сертифікації», наказу ДСТСЗІ СБ України від 11.09.06 №99/166 «Про затвердження

Технічних специфікацій форматів представлення базових об'єктів національної системи електронного цифрового підпису».

Регламент визначає організаційні, технічні та інші умови діяльності ЦСК під час надання послуг електронного цифрового підпису (надалі – ЕЦП).

### 1.3. Поширення дії Регламенту

- регламент є обов'язковим для виконання ЦСК та ВПР;
- положення цього Регламенту обов'язкові для підписувачів та клієнтів ЦСК з моменту звернення для отримання посиленого сертифікату відкритого ключа.

### 1.4. Порядок ознайомлення із положеннями Регламенту

Користувачі послуг ЦСК ознайомлюються з положеннями Регламенту, що підтверджують відповідність його діяльності політиці сертифікації, безпосередньо в ЦСК чи ВПР та через загальнодоступний мережевий електронний інформаційний ресурс ЦСК, розташований за адресою: <http://www.ukrcc.com>.

### 1.5. Порядок внесення змін до Регламенту

ЦСК має право в односторонньому порядку вносити зміни та доповнення до Регламенту. Зміни до Регламенту погоджуються з контролюючим органом у встановленому порядку.

Зміни та доповнення до Регламенту, що не пов'язані зі зміною чинного законодавства України, набувають чинності через 10 (десять) календарних днів з моменту їх розміщення на електронному інформаційному ресурсі ЦСК.

Зміни та доповнення, внесені до Регламенту при зміні законодавства України, набувають чинності одночасно із набранням чинності відповідних нормативних актів.

## 1.6. Ідентифікаційні дані ЦСК

Країна	Україна
Назва області	Київська
Назва міста	Київ
Повне найменування організації	Товариство з обмеженою відповідальністю «Український сертифікаційний центр»
Скорочене найменування організації	ТОВ «Український сертифікаційний центр»
ЄДРПОУ	33406510
Місцезнаходження організації	04080, м. Київ, вул. Фрунзе, 102
Номери телефонів/факсів	телефон/факс (044) 206-72-31/206-72-32
Веб сайт ЦСК	<a href="http://www.ukrcc.com">http://www.ukrcc.com</a>
Електронна пошта	<a href="mailto:info@ukrcc.com">info@ukrcc.com</a>
Служба позначок часу (Timestamp)	timestamp.ukrcc.com:139
Служба стану сертифікату (OCSP)	ocsp.ukrcc.com:2560

## 2. Діяльність ЦСК

ЦСК здійснює свою діяльність відповідно до Закону України «Про електронний цифровий підпис» та надає послуги ЕЦП фізичними особам, підприємствам, установам та організаціям усіх форм власності, органам державної влади, органам місцевого самоврядування, іншим суб'єктам господарської діяльності.

ЦСК здійснює діяльність та надає послуги на підставі:

- Свідоцтва про Державну реєстрацію серія А01 №456704, дата проведення реєстрації 23.03.2009 р.
- Засвідчення чинності відкритого ключа в ЦЗО та свідоцтва про акредитацію.

## 3. Обслуговування та використання сертифікатів, суб'єкти та відносини між ними

### 3.1. Обслуговування сертифікатів

Перелік послуг ЕЦП, які надаються ЦСК, передбачені нормативно-правовими актами, у тому числі політикою сертифікації, це зокрема :

- обслуговування посилених сертифікатів відкритих ключів (далі – сертифікатів), реєстрація підписувачів, сертифікація відкритих ключів підписувачів, надання доступу до сертифікатів, управління статусом сертифікатів, надання інформації про статус сертифікатів;
- надання у користування засобів криптографічного захисту інформації, надійних засобів ЕЦП;
- консультації клієнтів при генерації відкритих та особистих ключів;
- надання послуг фіксування часу (позначки часу);
- консультації щодо застосування ЕЦП за зверненнями підписувачів, клієнтів ЦСК.

ЦСК здійснює надання зазначених послуг у відповідності з законодавством, Регламентом та на підставі укладених угод.

Для наближення до заявників послуг ЕЦП, ЦСК створює ВПР. ВПР діють на підставі Положення про відокремлений пункт реєстрації та цього Регламенту.

В ролі ВПР можуть виступати представництва (філії, підрозділи) ЦСК, які можуть відряджати адміністраторів реєстрації до клієнтів.

Перелік ВПР ЦСК та відомості про місця їх розташування публікуються на інформаційному ресурсі ЦСК. Для взаємодії з ЦСК, ВПР використовують програмні або програмно-технічні засоби, які надаються ЦСК.

ВПР виконує такі функції:

- встановлення особи заявника (підписувача) чи його довіреної особи, що звертаються для формування, блокування, поновлення або скасування сертифікатів ключів ЕЦП;
- отримує і перевіряє відомості та документи, що надаються заявниками (підписувачами) для формування або зміни статусу сертифіката;

- надсилає до ЦСК підписаний своїм ЕЦП запит на формування або зміну статусу сертифіката відповідно з результатами перевірки документів заявника (підписувача);
- передає до ЦСК відомості та документи, що надаються заявниками (підписувачами) для формування або зміни статусу сертифіката;
- веде реєстр заяв і звернень заявників (підписувачів);
- надає консультації заявникам (підписувачам) щодо використання ЕЦП.

### 3.2. Використання сертифікатів

У процесі електронного документообігу підписувачі та особи ВПР, які перевіряють електронний цифровий підпис підписувачів (надалі - користувачі), використовують сертифікати, сформовані ЦСК.

Користувачі можуть не мати угод на обслуговування з ЦСК.

Підписувачами можуть бути:

фізичні особи та фізичні особи юридичних осіб, у тому числі посадові особи органів державної влади, органів місцевого самоврядування, яким сформовані сертифікати ключів для застосування ЕЦП у електронному документообігу;

юридичні особи, у тому числі органи державної влади, органи місцевого самоврядування, яким сформовані сертифікати ключів для використання ЕЦП (у якості печатки при електронному документообігу).

### 3.3. Обмеження щодо використання сертифікатів

ЦСК не встановлює обмеження щодо використання сформованих ним сертифікатів.

## 4. Порядок доступу до відкритої інформації (розповсюдження інформації)

### 4.1. Адреса загальнодоступного ресурсу.

Доступ до відкритої інформації здійснюється через загальнодоступний ресурс ЦСК (web - сайт), який має адресу: <http://www.ukgcc.com>

### 4.2. Перелік інформації, розміщеної на даному ресурсі:

- чинний регламент роботи ЦСК;
- перелік послуг ЕЦП, що надаються ЦСК та порядок їх надання;
- адреса ЦСК та перелік ВПР з адресами;
- нормативно-правові акти України у сфері ЕЦП;
- перелік документів, необхідних для реєстрації заявника, та документів, за якими виконується автентифікація та авторизація заявника;
- типова угода про надання послуг ЕЦП;
- вартість послуг з обслуговування сертифіката;
- кореневий сертифікат ЦСК, виданий центральним засвідчувальним органом;
- службові сертифікати ЦСК;
- сертифікати клієнтів, сформовані ЦСК (за наданою власниками згодою на публікацію);
- чинний список відкликаних сертифікатів;
- режим роботи ЦСК;
- додаткова інформація.

### 4.3. Порядок публікації кореневого та службових сертифікатів ЦСК.

Після формування кореневої сертифікати та службові сертифікати ЦСК публікуються на інформаційному ресурсі. Службові ключі використовуються для надання таких послуг:

- сервера позначок часу (TSP-сервера);
- сервера визначення статусу сертифікатів ключів (OCSP-сервера).

#### 4.4. Порядок публікації сертифікатів ключів підписувачів

Сертифікати підписувачів на інформаційному ресурсі ЦСК публікуються за згодою власників сертифікатів. Інформація щодо можливості публікації сертифіката вноситься до реєстраційних даних під час реєстрації підписувача. Після формування сертифіката, за наявності згоди його власника, сертифікат публікується на інформаційному ресурсі ЦСК.

Отримати інформацію про стан сертифіката підписувачі та користувачі можуть за допомогою сервера визначення статусу сертифікатів ключів (OCSP-сервера), який розташований на інформаційному ресурсі ЦСК.

#### 4.5. Порядок публікації списку відкликаних сертифікатів

Список відкликаних сертифікатів на інформаційному ресурсі ЦСК публікується одразу після його формування.

ЦСК формує повний список відкликаних сертифікатів.

Оновлений список публікується протягом двох годин після отримання заявки на скасування, блокування або поновлення сертифіката.

Доступ до інформаційного ресурсу не обмежується. Термін зберігання списку відкликаних сертифікатів – необмежений.

### 5. Порядок автентифікації та авторизації заявника

#### 5.1. Вимоги щодо встановлення особи заявника під час реєстрації

##### 5.1.1. Загальні положення

До початку формування сертифікатів для юридичних осіб (ЕЦП використовується в якості печатки) або фізичних осіб (ЕЦП використовується як аналог власноручного підпису) ЦСК здійснює встановлення особи заявника (фізичної або юридичної особи). Встановлення особи заявника здійснюється за його особистої присутності або присутності його уповноваженого представника в ЦСК або ВПР.

Заявник (уповноважений представник) повинен ознайомитись з умовами обслуговування сертифікатів ключів, передбачених політикою сертифікації та цим Регламентом, зокрема:

- зобов'язаннями та відповідальністю ЦСК стосовно обслуговування сертифікатів ключів;
- зобов'язаннями та відповідальністю заявника (підписувача) при використанні сертифікату та зберіганні особистого ключа;
- умовами та порядком використання підписувачам свого сертифікату відкритого ключа;
- терміном зберігання даних про заявників (підписувачів), які отримує ЦСК при реєстрації;
- відомостями про надійні засоби ЕЦП, що можуть використовуватися для генерації ключів, формування та перевірки ЕЦП.

##### 5.1.2. Встановлення юридичної особи

Встановлення заявника – юридичної особи здійснюється за установчими документами юридичної особи або нотаріально засвідченими згідно із законодавством копіями таких документів. Крім цього, під час реєстрації встановлюється особа - представник юридичної особи та її повноваження.

Для реєстрації уповноважена особа заявника надає такі документи:

- заповнену та підписану Угоду про надання послуг ЕЦП - у двох примірниках або заповнену та підписану заявником Картку приєднання до електронної угоди про надання послуг ЕЦП - в одному примірнику;
- оригінал статуту юридичної особи (положення про установу) або його нотаріально засвідчену копію (виключно для ознайомлення);
- оригінал свідоцтва про державну реєстрацію або його нотаріально засвідчену копію;

- копії паспортів підписувачів чи представників юридичної особи (копії 1-4 сторінок), засвідчені заявником;
- копії довідки про присвоєння індивідуального податкового номера (ПН) підписувача юридичної особи, засвідчені заявником;
- копії документів про призначення на посаду підписувачів, представників юридичної особи, засвідчені заявником.

Копії оригіналів документів, які виконуються під час реєстрації заявників, засвідчуються підписом адміністратора реєстрації.

Для відокремлених підрозділів (філії, представництва) юридичних осіб:

- заповнену та підписану заявником Угоду про надання послуг ЕЦП - у двох примірниках або заповнену та підписану заявником Картку приєднання до електронної угоди про надання послуг ЕЦП - в одному примірнику;
- довідку управління статистики про внесення відомостей про відокремлений підрозділ до ЄДРПОУ;
- положення про установу або його нотаріально засвідчену копію (виключно для ознайомлення);
- копії паспортів підписувачів (копії 1-4 сторінок) чи представників юридичної особи, засвідчені заявником;
- копії довідок про присвоєння підписувачам та представникам юридичної особи ПН, засвідчені заявником;
- копії документів про призначення на посаду підписувачів та представників юридичної особи, засвідчені заявником;

Якщо заявником подається оригінал документу, копія такого документу може бути засвідчена підписом адміністратора реєстрації ЦСК.

Бланки угод про надання послуг ЕЦП та деяких реєстраційних документів встановленої форми (довіреність, тощо) розміщуються на інформаційному ресурсі ЦСК.

### 5.1.3. Встановлення фізичної особи

Встановлення фізичної особи здійснюється за її паспортом (або іншим документом, який засвідчує особу відповідно до законодавства України). Встановлення фізичної особи - підприємця здійснюється на підставі свідоцтва про державну реєстрацію або його копії, засвідченої у встановленому порядку, та документа, що посвідчує особу (паспорт).

У випадку, якщо під час реєстрації встановлюється підписувач - фізична особа як представник юридичної особи, заявником виступає юридична особа. Реєстрація заявника здійснюється відповідно до п. 5.1.2 Регламенту.

Під час реєстрації заявник – фізична особа - підприємець надає такі документи:

- заповнену та підписану заявником Угоду про надання послуг ЕЦП - у двох примірниках або заповнену та підписану заявником Картку приєднання до електронної угоди про надання послуг ЕЦП в одному примірнику;
- оригінал свідоцтва про державну реєстрацію фізичної особи – підприємця або його нотаріально засвідчену копію;
- паспорт або інший документ, який засвідчує особу відповідно до законодавства України;
- довідку про присвоєння ПН;
- заповнену та підписану заяву встановленого зразка для реєстрації на отримання сертифіката ключа, яка є копією електронної заяви на отримання посиленого сертифіката електронного цифрового підпису;

Якщо заявником подається оригінал документу, копія такого документу може бути засвідчена підписом адміністратора реєстрації ЦСК.

Бланки угод на надання послуг ЕЦП та деяких реєстраційних документів встановленої форми (довіреність, тощо), розміщуються на інформаційному ресурсі ЦСК.

Під час реєстрації заявник - фізична особа надає такі документи:

- заповнену та підписану заявником Угоду про надання послуг ЕЦП - у двох примірниках або заповнену та підписану заявником Картку приєднання до електронної угоди про надання послуг ЕЦП - в одному примірнику;
- паспорт або інший документ, який засвідчує особу відповідно до законодавства України;
- довідку про присвоєння ПІН;
- заповнену, перевірену та підписану заяву на реєстрацію для отримання сертифіката ключа встановленого зразку, яка є копією електронної заяви на отримання посиленого сертифіката електронного цифрового підпису;

Якщо заявником подається оригінал документу, копія такого документу може бути засвідчена підписом адміністратором реєстрації ЦСК.

Бланки угод на надання послуг ЕЦП та деяких реєстраційних документів встановленої форми (довіреність, тощо), розміщуються на інформаційному ресурсі ЦСК.

Заявника може представляти довірена особа – представник, якщо неможлива особиста присутність заявника при реєстрації. У цьому випадку заявник надає довіреність відповідного зразка. Встановлення представника здійснюється за його паспортом або іншими документами відповідно до законодавства.

Довіреність представника повинна засвідчуватися:

- для юридичних осіб – підписом керівника та відбитком печатки юридичної особи;
- для фізичних осіб-підприємців - підписом підприємця та відбитком його печатки або, у разі відсутності печатки, бути нотаріально засвідченою;
- для фізичних осіб – нотаріально засвідчена.

Адміністратор реєстрації встановлює особу заявника (його довірену особу), що проходить процедуру реєстрації.

Надані заявником (представником) документи розглядаються в його присутності.

Не приймаються до розгляду документи, які мають підчистки, помарки, дописки, закреслені слова, інші виправлення чи надписи олівцем, а також пошкоджені, внаслідок чого їх текст неможливо прочитати.

За результатами розгляду наданих документів адміністратор реєстрації приймає рішення про відмову у реєстрації у таких випадках:

- при відсутності всіх необхідних для реєстрації документів;
- при поданні неналежно засвідчених копій документів;
- при встановленні невідповідності фактичних даних тим, які зазначені у поданих на реєстрацію документах.

У разі відмови у реєстрації, адміністратор реєстрації повертає надані документи заявнику (представнику) з роз'ясненнями причини повернення.

У випадку чинності поданих документів заявника та встановлення повноважень (довіреної) особи, здійснюється реєстрація заявника.

Із документів, що були надані заявником під час реєстрації, формується справа підписувача. Необхідні ідентифікаційні дані підписувачів заносяться до бази даних ЦСК, а документи беруться на облік. Справа підписувача реєструється в журналі, який ведеться в паперовому або електронному вигляді.

Реєстрація заявника є підставою для генерації ключів заявника, створення запиту на сертифікацію та формування сертифікату ключа підписувача.

Після завершення реєстрації заявнику надаються:

- угода, підписана ЦСК;
- надійні засоби ЕЦП разом з інструкцією користувача (за відсутності їх у заявника);
- носій інформації, що містить особистий ключ підписувача (у випадку генерації ключів у ЦСК або ВПР).

## 5.2. Захист персональних даних підписувачів

Захист персональних даних підписувачів забезпечується шляхом застосування:

- організаційних заходів з обліку та зберігання справ підписувачів, зокрема формування справ підписувачів та їх облік, призначення відповідальної особи за зберігання справ підписувачів, обмеження доступу обслуговуючого персоналу до приміщення (шаф), де зберігаються справи підписувачів;
- організаційно-технічних та технічних заходів, реалізованих комплексною системою захисту інформації автоматизованої системи ЦСК (далі – КСЗІ), у тому числі: використанням надійних засобів ЕЦП, веденням журналів роботи системи у захищеному вигляді, розмежуванням та контролем за інформаційними потоками між внутрішньою локальною мережею ЦСК та підсистемою відкритого доступу, застосуванням антивірусних засобів, міжмережєвих екранів тощо.

### 5.3. Підтвердження володіння заявником особистим ключем

Запит на сертифікацію в електронному вигляді містить відкритий ключ, що надається на сертифікацію та засвідчується ЕЦП за допомогою відповідного йому особистого ключа. Належність заявнику особистого ключа, що відповідає відкритому ключу, наданому на сертифікацію, підтверджується шляхом перевірки в ЦСК ЕЦП запиту на формування сертифіката ключа.

### 5.4. Автентифікація підписувача при зміні статусу сертифіката

Залежно від способу звернення в ЦСК відносно блокування, скасування чи поновлення сертифіката ключа, передбачені різні форми автентифікації підписувача та перевірки законності такого звернення:

- у разі письмового звернення підписувача, чинність звернення встановлюється за власноручним підписом відповідальної особи та печатки юридичної особи (для юридичних осіб);
- у разі звернення шляхом направлення запиту в електронному вигляді на блокування або скасування сертифіката, чинність звернення встановлюється шляхом перевірки ЕЦП на запиті за допомогою чинного сертифіката підписувача;
- у разі звернення по телефону щодо блокування сертифіката ключа, чинність звернення встановлюється за паролем фразою, яка вказується підписувачем під час формування заявки на отримання посиленого сертифікату відкритого ключа.

## 6. Порядок генерації ключів підписувачів

Відкритий та особистий ключі підписувача можуть бути згенеровані за допомогою надійного засобу ЕЦП:

- самостійно, на особистому обладнанні;
- на робочій станції генерації ключів підписувачів в ЦСК або ВПР.

### 6.1. Генерація ключів на особистому обладнанні.

Для самостійної генерації відкритого та особистого ключів застосовуються надійні засоби ЕЦП, що надаються ЦСК. При цьому, генерація здійснюється з використанням технічних засобів заявника.

Згенерований особистий ключ підписувача захищається паролем та записується на носій ключової інформації. Відповідальність за забезпечення конфіденційності та цілісності особистого ключа несе заявник.

Надійні засоби ЕЦП, що надаються заявнику, формують відкритий ключ підписувача у відповідному форматі.

Передача підписувачем сформованого відкритого ключа до ЦСК або ВПР здійснюється на носії інформації ним особисто або довіреною особою заявника.

### 6.2. Генерація ключів на робочій станції ЦСК

Під час генерації ключів робоча станція від'єднується від комп'ютерної мережі шляхом зупинки мережевого з'єднання.

Ключі підписувача генеруються ним особисто на робочій станції адміністратора реєстрації, на якій встановлено надійний засіб ЕЦП.

По закінченні процедури генерації особистий ключ підписувача захищається паролем і записується на носій ключової інформації, який залишається у підписувача, а відкритий ключ залишається на робочій станції адміністратора реєстрації.

Особисті ключі підписувачів не зберігаються в ЦСК.

Після генерації та запису особистого ключа підписувача на носій ключової інформації він автоматично знищується на станції генерації ключів надійним способом.

Генерація ключів довіреною особою здійснюється на робочій станції генерації ключів. По закінченні процедури генерації особистий ключ підписувача захищається паролем та записується на носій ключової інформації. Носій ключової інформації та пароль до особистого ключа вкладаються у непрозорий конверт, який запечатується, скріплюється печаткою ТОВ "УСЦ", підписами довіреної особи та адміністратора реєстрації.

Довірена особа робить запис на бланку про отримання конверта з носієм особистого ключа, паролем до особистого ключа та інструкції про порядок зміни паролю до особистого ключа підписувача. Документ із записом зберігається разом з документами заявника. Після передачі конверта з носієм ключової інформації довіреній особі заявника, відповідальність за забезпечення конфіденційності та цілісності особистого ключа несе заявник.

У разі, якщо генерація ключів здійснювалась довіреною особою, заявник при отриманні від довіреної особи конверта з особистим ключем та паролем зобов'язаний виконати дії, наведені в інструкції, яка передається довіреній особі, а саме:

- перевірити цілісність конверта;
- якщо цілісність не порушена, то невідкладно, перед першим використанням особистого ключа для накладання підпису, підписувач зобов'язаний змінити пароль доступу до нього;
- у разі, якщо неможливо змінити пароль шляхом перезапису ключа на той самий носій ключової інформації (наприклад ключ записаний на CD-R), необхідно після зміни паролю зберегти особистий ключ на новому носії, а попередній носій особистого ключа знищити надійним способом, без можливості його відтворення;
- при порушенні цілісності конверта, заявник (підписувач) невідкладно зобов'язаний звернутись до ЦСК із заявою про скасування сертифіката відповідного ключа.

## 7. Створення та зміна статусу сертифіката підписувача

### 7.1. Порядок створення сертифікатів відкритих ключів підписувачів, визнання сертифіката його власником.

Підписувач на один і той самий момент часу може мати і використовувати лише один особистий ключ, якому відповідає відкритий ключ із чинним сертифікатом ключа. Це обмеження не стосується електронної печатки.

Формат сертифіката відповідає вимогам Закону України "Про електронний цифровий підпис" та визначається відповідними технічними специфікаціями форматів представлення базових об'єктів національної системи ЕЦП.

Сертифікат створюється за заявкою на створення сертифікату. Заявка подається адміністратором реєстрації до ЦСК електронною поштою або на електронному носії інформації. Заявка підписана особистим ЕЦП адміністратора реєстрації. Опрацювання заявки здійснюється протягом робочого дня з моменту надходження заявки до ЦСК.

Формат сертифіката визначений в Технічних специфікаціях форматів представлення базових об'єктів, затверджених спільним наказом Держзв'язку та ДСТСЗІ СБ України № 99/166 від 11.11.2006.

ЦСК забезпечує унікальність розпізнавального імені підписувача, що міститься в сертифікаті. Для фізичної особи обов'язковими реквізитами розпізнавального імені є прізвище, ім'я, по батькові та ПІН (серія та номер паспорта), а для юридичної особи – назва юридичної особи відповідно до статуту (положення) та ідентифікаційний код за ЄДРПОУ.

Сформований сертифікат, за бажанням заявника, адміністратор реєстрації:

- записує на носій інформації та передає заявнику;
- надає сертифікат - документ у паперовій формі, який засвідчуються печаткою ЦСК та власноручним підписом адміністратора реєстрації.

Сертифікат визначається прийнятим з моменту підпису власником паперового варіанту заявки на формування сертифікату, яка є копією електронного документу наданого для формування сертифікату.

На загальнодоступному ресурсі сертифікат публікується не пізніше, ніж за 15 хвилин після його створення.

Термін чинності сертифіката вказаний в сертифікаті.

## 7.2. Повторне формування сертифіката ключа

Повторне формування сертифіката ключа полягає у формуванні нового сертифіката підписувача у разі завчасного (протягом дії угоди) скасування чинного сертифіката. Сертифікат скасовується у випадку зміни відомостей про підписувача, зазначених у ньому, компрометації відповідного особистого ключа.

При повторному формуванні сертифіката, адміністратором реєстрації виконуються дії, зазначені в п. 6 та п. 7 цього Регламенту.

## 7.3. Використання сертифіката та особистого ключа підписувача.

### 7.3.1. Права та обов'язки підписувача

Під час звернення до ЦСК або ВІР для формування сертифіката, а також при використанні сертифіката та особистого ключа підписувачі зобов'язані:

- надавати повну та достовірну інформацію, необхідну для формування сертифіката під час реєстрації;
- зберігати особистий ключ в таємниці, вживати заходів щодо запобігання його втрати, розкриттю, перекручуванню та несанкціонованому використанню;
- не розголошувати та не повідомляти іншим особам пароль доступу до особистого ключа та ключову фразу для автентифікації по телефону;
- використовувати надійні засоби ЕЦП для генерації особистих та відкритих ключів, формування та перевірки ЕЦП;
- негайно інформувати ЦСК про події, що виникли до закінчення терміну чинності сертифіката: компрометація особистого ключа; компрометація паролю захисту особистого ключа; виявлення неточностей або зміна даних, зазначених у сертифікаті;
- не використовувати особистий ключ у разі його компрометації;
- не використовувати особистий ключ після подання заяви на скасування чи блокування сертифіката;
- не використовувати особистий ключ відповідного сертифіката, що скасований або заблокований.

### 7.3.2. Підписувачі мають право:

- отримувати сертифікат ЦСК;
- отримувати список відкликаних сертифікатів, який формує ЦСК;
- використовувати сертифікат ЦСК для перевірки справжності ЕЦП сертифікатів, які сформовані ЦСК;
- використовувати список відкликаних сертифікатів, сформований ЦСК, для перевірки як статусу власного сертифіката, так і сертифікатів інших підписувачів;
- генерувати на своєму робочому місці відкриті та особисті ключі;
- ознайомлюватися з інформацією про діяльність ЦСК та надання ним послуг ЕЦП;
- звертатися у ЦСК із заявами, скаргами чи претензіями;

- вимагати скасування, блокування або поновлення свого сертифіката ключа у випадках, передбачених Регламентом;
- оскаржувати дії або бездіяльність ЦСК у судовому порядку.

### 7.3.3. Обов'язки користувача

Перед використанням сертифіката користувач зобов'язаний:

- перевірити статус сертифіката за актуальним списком відкликаних сертифікатів або сервісом OCSP;
- перевірити автентичність і цілісність списку відкликаних сертифікатів,
- використовувати сертифікат ЦСК для перевірки справжності ЕЦП сертифікатів, які сформовані ЦСК;

Якщо одержати інформацію про поточний стан сертифіката тимчасово неможливо, користувач повинен тимчасово відмовитись від використання сертифіката.

### 7.4. Порядок блокування сертифікатів ключів

Блокування сертифікату ключа - це тимчасове припинення чинності сертифікату ключа.

Після блокування сертифікату ключа, заявник зобов'язаний протягом 90 календарних днів поновити чинність сертифікату або подати заяву про його скасування. У випадку, якщо протягом зазначеного терміну заявник не поновить чинність заблокованого сертифіката або не подасть заяви про його скасування, сертифікат ключа автоматично скасовується ЦСК.

Блокування сертифіката ключа здійснюється на підставі заяви заявника, яка подана в усній, письмовій формі, чи у вигляді електронного документа.

Часом блокування сертифікату ключа вважається час зміни його статусу на інформаційному ресурсі ЦСК.

Підписувач не має права використовувати особистий ключ для накладення ЕЦП, сертифікат ключа якого заблоковано або скасовано.

#### 7.4.1. Блокування сертифіката по телефону

Заява в усній формі подається заявником (підписувачем) до ЦСК засобами телефонного зв'язку за номером, який опублікований на власному інформаційному ресурсі ЦСК, при цьому заявник повинен повідомити оператору сертифікації таку інформацію:

- ідентифікаційні дані власника сертифіката;
- серійний номер сертифіката;
- ключову фразу голосової автентифікації.

Заява в усній формі приймається тільки у випадку позитивної автентифікації (збігу голосової фрази та ідентифікаційних даних підписувача з інформацією наданою в заяві на формування сертифікату).

Усна заява до ЦСК може бути подана цілодобово. Опрацювання усної заяви на блокування сертифікату та інформування власника сертифіката здійснюється протягом двох годин з моменту подання заяви до ЦСК.

#### 7.4.2. Блокування сертифіката за заявою у електронній формі

Електронна заява подається до ЦСК або ВПР за встановленою формою та засвідчується підписувачем своїм ЕЦП. Заяви приймаються на електронну адресу **status@ukrcc.com**.

Розгляд заяви на блокування сертифіката та інформування заявника здійснюється протягом двох годин з моменту надходження заяви до ЦСК.

#### 7.4.3. Блокування сертифіката за заявою у письмовій формі

Письмова заява подається до ЦСК або ВПР за встановленою формою та засвідчується власноручним підписом заявника.

У разі якщо власником сертифіката є юридична особа, підпис уповноваженого представника юридичної особи засвідчується печаткою.

Розгляд письмової заяви на блокування сертифіката до ЦСК та інформування заявника здійснюється протягом двох годин з моменту надходження заяви до ЦСК.

#### 7.5. Порядок поновлення чинності сертифікатів ключів

Поновлення чинності сертифіката ключа можливе лише для заблокованих сертифікатів ключів, термін блокування яких не скінчився.

Для поновлення чинності сертифіката ключа, заявник подає до ЦСК або ВПР письмову заяву встановленого зразка.

Опрацювання письмової заяви на поновлення чинності сертифіката, її розгляд та інформування заявника про поновлення, здійснюється протягом двох годин з моменту надходження заяви до ЦСК.

Часом поновлення чинності сертифіката ключа вважається час зміни його статусу на інформаційному ресурсі ЦСК.

#### 7.6. Порядок скасування сертифікатів ключів

Скасування припиняє чинність сертифіката ключа. Скасовані сертифікати ключів поновленню не підлягають.

##### 7.6.1. Скасування сертифіката за заявою у електронній формі

Електронна заява подається до ЦСК або ВПР за встановленою формою та засвідчується підписувачем своїм ЕЦП. Заяви приймаються на електронну адресу **status@ukrcc.com**.

Розгляд та опрацювання заяви на скасування сертифіката ключа та інформування заявника про блокування здійснюється протягом двох годин з моменту надходження заяви до ЦСК.

##### 7.6.2. Скасування сертифіката за заявою у письмовій формі

Для скасування сертифіката ключа заявник зобов'язаний подати до ЦСК або ВПР письмову заяву встановленого зразка, засвідчену його особистим підписом. Якщо заявником є юридична особа, заява засвідчується підписом уповноваженого представника та печаткою юридичної особи.

Розгляд та опрацювання заяви на скасування сертифіката ключа та інформування заявника про блокування здійснюється протягом двох годин з моменту надходження заяви до ЦСК.

Часом скасування сертифікату вважається час, який вказаний для скасованого сертифіката в списку відкликаних сертифікатів.

У випадку, якщо необхідне термінове скасування сертифіката ключа через об'єктивні обставини, з метою недопущення майнової шкоди, заявник (підписувач) має заблокувати сертифікат такого особистого ключа в усній формі та протягом терміну блокування подати заяву про скасування сертифіката ключа.

#### 7.7. Термін дії сертифікатів підписувачів

Максимальний термін дії сертифікатів ключів ЕЦП не більше, ніж 2(два) роки.

Після закінчення терміну дії сертифіката, він вилучається з інформаційного ресурсу ЦСК та переміщується в архів. ЦСК зберігає сертифікат та пов'язані з ним списки відкликаних сертифікатів без терміново.

Сертифікат, у якого закінчився термін дії, можна завантажити з інформаційного ресурсу за його серійним номером.

За запитом користувачів, ЦСК надає необхідний сертифікат та пов'язані з ним списки відкликаних сертифікатів з архівних записів у терміни, встановлені законодавством України для відповідей на звернення громадян.

## 8. Управління та операційний контроль

### 8.1. Фізичне середовище

ЦСК розташований у приміщенні на третьому поверсі нежилого будинку, який знаходиться під охороною, за адресою: 04080, м. Київ, вул. Фрунзе, 102.

Приміщення ЦСК складається із чотирьох зон:

- серверна кімната, в якій розташована екранована шафа;
- спеціальне приміщення,
- приміщення архіву,
- адміністративне приміщення.

Обладнання програмно-технічного комплексу, що забезпечує формування сертифікатів, управління статусом сертифікатів та зберігання особистих ключів ЦСК, розміщується в екранованій шафі, яка знаходиться в серверній кімнаті та в спеціальному приміщенні.

Всі приміщення розміщуються в зоні основної будівлі на третьому поверсі та обладнані системою контролю доступу, охороною та пожежною сигналізацією.

Серверна кімната забезпечує фізичний захист від несанкціонованого доступу до екранованої шафи, де встановлено відповідне обладнання. Екранована шафа забезпечує пасивний захист інформації від витоку каналами ПЕМВН, від порушення її цілісності внаслідок деструктивного впливу зовнішніх електромагнітних полів. Величина ефективності екранування екранованої шафи відповідає встановленим нормам.

Приміщення ЦСК та програмно-апаратний комплекс, який використовується для обслуговування сертифікатів, має експертний висновок та **ВІДПОВІДАЄ** вимогам нормативних документів систем технічного захисту інформації в Україні щодо захисту інформації.

Вхідні двері ЦСК стійкі до злому, обладнані трьома замками (двома механічними та одним магнітним).

Автоматизовані робочі місця адміністраторів та операторів ЦСК знаходяться у спеціальному приміщенні, доступ до якого обмежений. Робочі місця адміністраторів та операторів реєстрації знаходяться в контрольованій зоні.

Доступ до екранованої шафи ЦСК у режимі штатної роботи мають:

- керівник ЦСК;
- адміністратор безпеки;
- системний адміністратор;
- адміністратор БД.

Інші особи мають право доступу до екранованої шафи тільки в супроводі адміністратора безпеки або керівника ЦСК. Факти доступу до екранованої шафи фіксуються у журналі (з зазначенням ПІБ посадової особи, мети та часу доступу, списку відвідувачів) та засвідчуються підписом керівника ЦСК або адміністратора безпеки. Усі співробітники ЦСК, які мають право доступу до екранованої шафи, зобов'язані виконувати роботи тільки під час виконання своїх обов'язків.

Допуск у спеціальне приміщення у режимі штатної роботи ЦСК мають:

- керівник ЦСК;
- адміністратор безпеки;
- адміністратор сертифікації;
- оператор сертифікації;
- системний адміністратор;
- адміністратор БД;

Ключі від приміщень ЦСК мають відповідальні особи, які передають під охорону усі приміщення ЦСК. Дублікати ключів від робочих приміщень ЦСК зберігаються у сейфі адміністратора безпеки ЦСК.

В ЦСК відсутнє фізичне з'єднання внутрішньої локальної обчислювальної мережі із зовнішньої мережею (глобальною мережею), яка є доступною для користувачів. В ЦСК реалізовано адміністрування з метою розмежування доступу обслуговуючого персоналу до ресур-

сів системи. Доступ надається тільки після успішної авторизації обслуговуючого персоналу (можливість виконувати тільки ті функції, що доступні та асоційовані з їх ролями).

## 8.2. Процедурний контроль

### 8.2.1. Права ЦСК

ЦСК під час формування та обслуговування сертифікатів має право:

- надавати послуги ЕЦП та обслуговувати сертифікати ключів, відповідно до вимог законодавства України;
- вимагати, отримувати та перевіряти інформацію, необхідну для реєстрації заявника і формування сертифіката, безпосередньо у заявника (юридичної або фізичної особи) або її уповноваженого представника;
- не приймати запит в електронному вигляді на формування сертифіката у тому випадку, якщо формати вихідних даних, створені засобом криптографічного захисту інформації, яким користувався заявник для генерації ключів, не підтримуються ЦСК;
- блокувати, скасовувати, поновлювати сертифікати у порядку, встановленому політикою сертифікації та цим Регламентом;
- вимагати від підписувача (заявника) дотримання вимог Регламенту, умов угоди про надання послуг;
- припиняти надання послуг ЕЦП за умов порушення угоди про надання послуг ЕЦП або вимог цього Регламенту.

### 8.2.2. Зобов'язання ЦСК під час формування та обслуговування сертифікатів:

- під час реєстрації встановлювати заявника відповідно до вимог, визначених в цьому Регламенті та законодавстві України, у тому числі встановлювати належність відкритого ключа та відповідного особистого ключа заявнику, якщо генерація ключів здійснювалося не в ЦСК або ВПР;
- формувати посилений сертифікат відкритого ключа за форматом, що відповідає вимогам «Технічних специфікацій форматів представлення базових об'єктів», затверджених спільним наказом Держзв'язку та ДСТСЗІ СБ України № 99/166 від 11.11.2006, забезпечувати унікальність реєстраційного номера сертифіката, який формується ЦСК;
- підтримувати статус сформованого сертифіката протягом терміну його чинності;
- скасовувати та блокувати сертифікати у порядку, визначеному цим Регламентом, формувати списки відкликаних сертифікатів у форматі, відповідно до вимог Технічних специфікацій форматів представлення базових об'єктів, які затверджені спільним наказом Держзв'язку та ДСТСЗІ СБ України № 99/166 від 11.11.2006;
- поновлювати сертифікати відповідно до порядку, визначеному у цьому Регламенті;
- зберігати документи, на підставі яких були сформовані, скасовані, заблоковані та поновлені сертифікати;
- забезпечувати надійне збереження сформованих сертифікатів та документів, що надавалися заявником для реєстрації;
- публікувати список відкликаних сертифікатів на електронному інформаційному ресурсі;
- забезпечувати можливість цілодобового вільного доступу користувачів до сертифікатів підписувачів (за їх згодою), сертифікатів ЦСК, даних про статус сертифікатів, нормативних документів з надання послуг та використання ЕЦП;
- використовувати для надання послуг ЕЦП програмно-технічний комплекс, засоби криптографічного захисту інформації, в тому числі засоби ЕЦП, що мають позитивний експертний висновок за результатами державної експертизи у сфері КЗІ;
- надавати підписувачам надійні засоби ЕЦП для генерації особистих та відкритих ключів, формування та перевірки ЕЦП;

- забезпечувати розташування засобів програмно-технічного комплексу в спеціально обладнаних приміщеннях, їх охорону з метою запобігання незаконному проникненню в приміщення ЦСК сторонніх осіб;
- забезпечувати надійний захист персональних даних, отриманих від підписувача, та інформації в автоматизованих системах згідно з чинним законодавством;
- інформувати користувачів про необхідність перевірки чинності сертифіката за його статусом;
- цілодобово приймати заяви підписувачів про скасування, блокування та поновлення сертифікатів ключів.

8.2.3. ЦСК під час формування та обслуговування сертифікатів несе відповідальність за:

- внесення в сертифікат невірних відомостей, відмінних від вказаних у заяві (зверненні) на формування сертифіката;
- невірне встановлення заявника, наприклад, внаслідок технічних помилок, недотримання процедур перевірки документів тощо;
- несвоєчасну публікацію списків відкликаних сертифікатів;
- помилкове відкликання або блокування сертифікатів;
- компрометацію особистого ключа ЦСК;
- відмову та збої технічних і програмних засобів ПТК;
- помилкові та/або протиправні дії обслуговуючого персоналу ЦСК;
- захист персональних даних підписувачів.

8.3. Організаційна структура ЦСК, функціональні обов'язки та відповідальність.

ЦСК складається з таких підрозділів та служб:

- реєстраційний центр;
- сертифікаційний центр;
- служба захисту інформації;
- технічна служба;
- відокремлені пункти реєстрації (ВІР).

Реєстраційний та сертифікаційний центри, технічна служба та служба захисту інформації територіально розташовані у приміщеннях ЦСК.

8.3.1. Реєстраційний центр

До складу реєстраційного центру входить(ять) адміністратор(и) реєстрації.

Функціональні обов'язки та відповідальність адміністратора реєстрації.

Адміністратор реєстрації відповідає за:

- встановлення осіб, які звернулися до ЦСК для формування сертифіката;
- перевірку даних, обов'язкових для формування сертифіката, а також даних, які вносяться у сертифікат на вимогу підписувача;
- отримання від користувачів заявок на формування, скасування, блокування та поновлення сертифікатів ключів;
- надання консультацій підписувачам під час генерації ключів у разі отримання від них відповідного звернення та вживає заходи щодо забезпечення безпеки інформації під час генерації;
- забезпечення перевірки чинності звернень про блокування, поновлення та скасування сертифікатів;
- надає підписувачам консультації щодо умов та порядку надання послуг ЕЦП;
- інформує адміністратора безпеки про події, що впливають на безпеку функціонування акредитованого центру.

8.3.2. Сертифікаційний центр

До складу сертифікаційного центру входять адміністратори та оператори сертифікації.

#### 8.3.2.1. Обов'язки та відповідальність адміністратора сертифікації.

- подає до центрального засвідчувального органу (засвідчувального центру) даних, необхідних для формування сертифіката та засвідчення відкритого ключа ЦСК;
- використовує особистий ключ ЦСК під час формування сертифікатів ключів, списків відкликаних сертифікатів та позначки часу;
- забезпечує ведення, архівацію та відновлення еталонної бази даних сформованих сертифікатів;
- інформує адміністратора безпеки про події, що впливають на безпеку функціонування акредитованого центру;
- формує та скасовує службові сертифікати.

#### 8.3.2.2. Обов'язки та відповідальність оператора сертифікації:

- створює сертифікати клієнтів ЦСК на підставі зареєстрованої заявки;
- змінює статус сертифікатів;
- оновлює списки відкликаних сертифікатів.

#### 8.3.3. Служба захисту інформації

Склад служби захисту інформації визначає директор ЦСК своїм наказом. Службу захисту інформації очолює адміністратор безпеки.

Адміністратор безпеки відповідає за:

- забезпечення повноти та якісного виконання організаційно-технічних заходів із захисту інформації;
- розроблення розпорядчих документів, згідно з якими в ЦСК повинен забезпечуватися захист інформації, контроль за їх виконанням;
- своєчасне реагування на спроби несанкціонованого доступу до ресурсів програмно-технічного комплексу ЦСК, порушення правил експлуатації засобів захисту інформації;
- бере участь у генерації ключів ЦСК та посадових осіб;
- бере участь у формуванні сертифікатів для посадових осіб;
- контролює збереження особистого ключа ЦСК та його резервної копії, особистих ключів посадових осіб ЦСК;
- веде контроль за веденням журналів прийому-передачі ключів;
- бере участь у знищенні особистого ключа ЦСК, контролює правильність і своєчасне знищення посадовими особами особистих ключів;
- контролює процес резервування сертифікатів ключів та списків відкликаних сертифікатів, а також інших важливих ресурсів;
- організацію розмежування доступу до ресурсів програмно-технічного комплексу ЦСК, зокрема розподілення між посадовими особами паролів, ключів, сертифікатів тощо;
- спостерігає (реєстрація та аудит подій в програмно-технічному комплексі ЦСК, моніторинг подій тощо) за функціонуванням комплексної системи захисту інформації;
- забезпечує організацію та проведення заходів з модернізації, тестування, оперативного відновлення функціонування комплексної системи захисту інформації після збоїв, відмов, аварій програмно-технічного комплексу;
- ведення журналу обліку.

#### 8.3.4. Технічна служба

Технічну службу очолює системний адміністратор. Технічна служба забезпечує:

- організацію експлуатації та технічного обслуговування програмно-технічного комплексу ЦСК;
- здійснення адміністрування сервера бази даних програмно-технічного комплексу;
- підтримку електронного інформаційного ресурсу, публікацію сертифікатів та списку відкликаних сертифікатів;

- адміністрування засобів програмно-технічного комплексу;
- бере участь у впровадженні та забезпеченні функціонування комплексної системи захисту інформації;
- встановлення та налагодження програмного забезпечення системи резервного копіювання бази даних програмно-технічного комплексу;
- формування та ведення резервних копій загальносистемного та спеціального програмного забезпечення програмно-технічного комплексу;
- актуальність еталонних, архівних і резервних копій баз сертифікатів та їх зберігання;
- ведення, архівацію та відновлення еталонної бази даних сформованих сертифікатів.

#### 8.4. Ведення журналів аудиту автоматизованої системи

До подій, які повинні фіксуватися в журналах аудиту, відносяться:

- генерація ключів ЦСК;
- формування сертифікатів, списків відкликаних сертифікатів;
- зміна статусу посиленних сертифікатів відкритих ключів підписувачів;
- помилки, попередження та збої в роботі програмних засобів і серверів ЦСК;
- спроби автентифікації персоналу в програмно-технічному комплексі;
- резервування особистого ключа;
- знищення особистого ключа ЦСК.

Запис повинен містити такі дані:

- дата та час події;
- тип події;
- ідентифікатор суб'єкта, що ініціював подію;
- додаткову інформацію.

Повний доступ до журналу аудиту має виключно адміністратор безпеки. Адміністратор безпеки має право на читання (перегляд) змісту журналу, пошук подій, перевірку цілісності чинного журналу та виконувати копіювання інформації аудиту до файлів з використанням засобів захисту.

Для всіх користувачів чинний журнал аудиту відкрито виключно на запис.

Засобами програмно-технічного комплексу заборонено модифікацію окремих записів чинного журналу аудиту. Записи захищаються від несанкціонованого видалення засобами системи управління базою. Очищення журналів аудиту виконується адміністратором безпеки тільки після створення копії журналу в архіві.

Термін зберігання протокольних записів аудиту не обмежений, але звичайно становить 3 роки. Вся база даних ЦСК, разом із системними таблицями, копіюється стандартними засобами експорту даних із системи керування базами даних у вигляді бінарного файлу на жорсткий диск, а потім на оптичний диск один раз на добу. Адміністратор безпеки періодично, не рідше одного разу на добу, переглядає журнали аудиту з метою виявлення сукупності подій (серед зареєстрованих у журналі аудиту), які свідчать про ситуацію, яка призвела або може призвести до порушення безпеки технічних засобів ЦСК.

#### 8.5. Ведення архівів

Сертифікати підписувачів та списки відкликаних сертифікатів в архівному режимі зберігаються безтерміново. Документи, що надавалися заявником для реєстрації, зберігаються на протязі терміну позовної давності.

Архівному зберіганню підлягають такі документи ЦСК:

- сертифікати ЦСК;
- сертифікати підписувачів ЦСК;
- заявки на сертифікацію;
- документи, надані під час реєстрації;
- заяви на зміну статусу сертифікатів (скасування, блокування, поновлення);
- службові документи ЦСК;

– журнали аудиту ЦСК.

Засобами СКБД, що входять до складу програмно-технічного комплексу, виконується автоматичне резервне копіювання бази даних ЦСК. Копіювання даних здійснюється на накопичувач на жорстких магнітних дисках, а потім на оптичний носій.

Резервна копія бази даних зберігається у спеціальному приміщенні ТОВ «Український сертифікаційний центр» у сейфі №2. Після створення нової резервної копії, попередня резервна копія стає архівною.

Для зберігання носіїв з резервними та архівними копіями виділяється окреме сховище з двома екземплярами ключів і пристроями для опечатування замкових щілин. Один екземпляр ключа від сховища знаходиться в уповноваженій посадовій особі ЦСК, яка відповідає за створення та зберігання резервних та архівних копій, а другий – в опечатаному вигляді зберігається у сховищі адміністратора безпеки ЦСК або посадової особи, яка його заміщує.

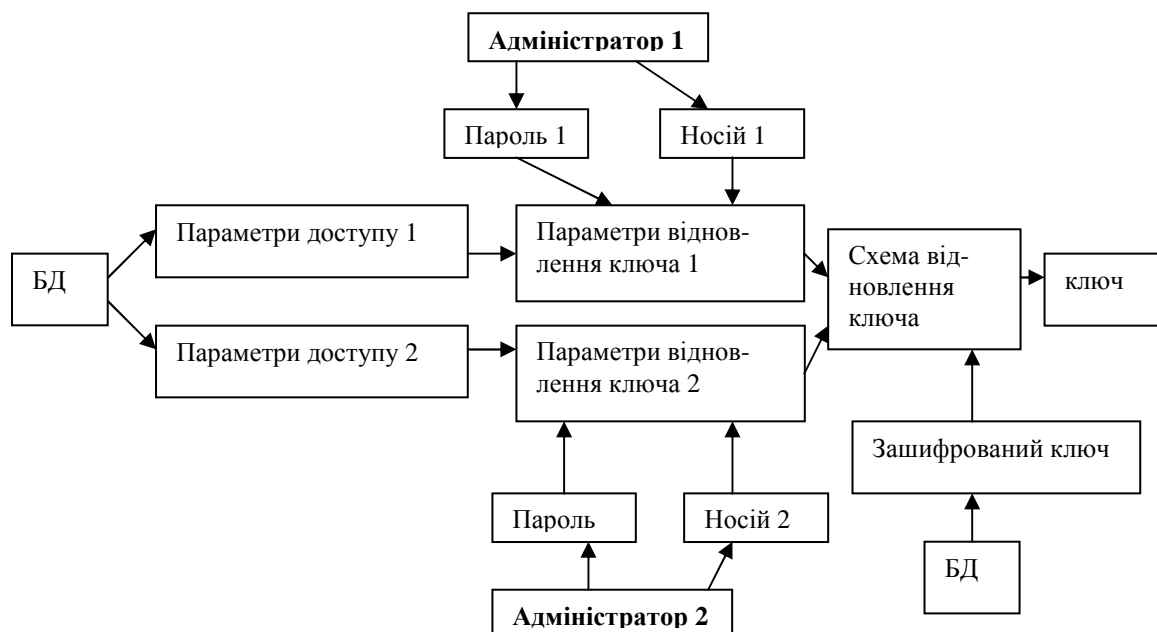
Архівні копії журналів аудиту ПТК ЦСК зберігаються не менше трьох років.

## 9. Управління ключами

### 9.1. Порядок генерації, захисту та доступу до особистого ключа ЦСК

Генерація особистого ключа здійснюється за допомогою надійних засобів ЕЦП, у спеціальному приміщенні, за участю двох адміністраторів сертифікації під контролем адміністратора безпеки. Обчислення ключів ЦСК сертифікації здійснюється наступною схемою: обчислення провадяться з використанням обчислених або вибраних параметрів. Після ініціалізації алгоритму генерується пара ключів. Відкритий ключ використовується при формуванні запиту на створення сертифікату відкритого ключа ЦСК в Центральний засвідчувальний орган. Особистий ключ шифрується з використанням випадкового ключа. Зашифрований особистий ключ записується до бази даних. Кожен адміністратор вводить свій пароль і для кожного адміністратора формується свій блок випадкових даних. За цими даними і ключем шифрування особистого ключа формується індивідуальна множина параметрів для кожного адміністратора. Ці параметри записуються до бази даних, де вони прив'язуються до зашифрованого особистого ключа.

Для використання особистого ключа сертифікату ЦСК, цей ключ відновлюють два адміністратори з числа тих, що мають доступ до цього ключа. Відповідний протокол зображено на наступній схемі – див. мал. 1



Мал. 1. Процедура використання особистого ключа УСЦ

Кожен з двох адміністраторів автентифікується системою та вводить свій пароль відновлення особистого ключа. З бази даних беруться відповідні параметри доступу та обчислюються індивідуальні параметри відновлення ключа для кожного з адміністраторів. За допомогою цих параметрів відновлюється ключ шифрування особистого ключа. З бази даних береться зашифрований ключ сертифіката ЦСК та розшифровується з використанням відновленого ключа шифрування особистого ключа.

Обмежені права на використання особистого ключа можуть надаватися операторам ЦСК. Оператори ЦСК сертифікації ключів можуть використовувати особистий ключ ЦСК для формування сертифікатів підписувачів і списку відкликаних сертифікатів та не мають права здійснювати резервування та знищення особистого ключа, формувати службові сертифікати. Схема роботи операторів з особистим ключем ЦСК подібна до схеми роботи адміністраторів.

Чинні адміністратори можуть допустити нового адміністратора. Для цього два адміністратори відновляють особистий ключ та новий адміністратор створює свої параметри доступу до ключа.

Відповідно до попереднього випадку, два адміністратори відновлюють особистий ключ, та створюють параметри доступу нового оператора сертифікації.

## 9.2. Резервування особистого ключа, порядок та умови зберігання, доступу та використання резервної копії.

Для відновлення працездатності ЦСК після аварії програмно-технічного комплексу необхідно, щонайменше, відновити такі критичні дані:

- Особистий ключ ЦСК (з метою забезпечення конфіденційності зберігається в зашифрованому вигляді);
- Параметри доступу адміністраторів до особистого ключа ЦСК;
- Сертифікат відкритого ключа ЦСК та ЦЗО;
- Службові сертифікати адміністраторів та операторів ЦСК;
- Сертифікати користувачів.

Паролі адміністраторів для відновлення особистого ключа разом з іншою ідентифікаційною інформацією (паролі доступу до операційних систем, систем управління базами даних, тощо) зберігаються в сейфі адміністратора безпеки ЦСК. Дані кожного адміністратора знаходяться в окремому конверті, на який накладено особистий підпис адміністратора.

Архів даних, який містить інформацію з якої відтворюється особистий ключ сертифікаційного центру в зашифрованому вигляді, створюється наступним чином:

- адміністратор бази даних засобами СКБД створює дамп даних;
- системний адміністратор створює архів дампа за допомогою архіватора з використанням паролю, який складається з двох частин та надається адміністратором безпеки. Пароль вводять призначені наказом співробітники ЦСК. Довжина частини паролю повинна мати не менше 16 символів. Повинні використовуватися букви (великі та малі), цифри та спеціальні символи. Архів записується в двох екземплярах на CD(DVD)-ROM. На носіях CD(DVD)-ROM робиться надпис з зазначенням номеру диску та дати запису на нього архіву.
- тимчасові копії оригінальних даних та архівів знищуються без можливості відтворення даних.
- частини паролю записуються (роздруковуються) на папері та запечатуються кожний окремо в непрозорі конверти. Кожний конверт нумерується.
- конверти та копії архіву на CD(DVD)-ROM зберігаються в сейфах окремих приміщень.

Всі події реєструються у журналі обліку резервних копій даних.

Архів створюється кожного разу після таких подій:

- завантаження ключів сертифікаційного центру;
- створення службових ключів та сертифікатів ЦСК;

- створення або видалення записів адміністраторів, операторів або сервісів ЦСК.

При створенні нового архіву попередній архів та конверти з паролями знищуються без можливості відтворення даних.

Складається акт про створення нового архіву даних та знищення попереднього архіву.

У випадку втрати чи пошкодження критичних даних та неможливості відновити їх стандартними засобами СКБД, дозволяється використати резервну копію критичних даних. Адміністратор сертифікації та системний адміністратор під контролем адміністратора безпеки вживають заходи щодо поновлення працездатності ЦСК, за необхідності, створюють нову базу даних. Запечатані конверти з ідентифікаційними даними та пенал з резервною копією критичних даних відкриваються в присутності адміністратора безпеки та адміністратора сертифікації ЦСК. Адміністратор сертифікації імпортує дані з файлів резервної копії до бази даних.

### 9.3. Протоколювання операцій з особистим ключем ЦСК

Будь-яка операція з особистим ключем ЦСК протоколюється в електронному або паперовому журналі із зазначенням дати та часу здійснення операції, посадової особи ЦСК, що виконала операцію, типу операції.

## 10. Термін дії особистого ключа ЦСК

Термін дії особистого ключа ЦСК становить не більше 5 (п'яти) років та вказаний в сертифікаті відкритого ключа, сформованого центральним засвідчувальним органом. Після закінчення терміну дії особистого ключа ЦСК особистий ключ та всі його резервні копії знищуються способом, що не дозволяє їх відновлення.

### 10.1. Порядок планової зміни ключів ЦСК

Планова зміна ключів ЦСК виконується не раніше, ніж через три роки та не пізніше, ніж через п'ять років після початку їх дії.

Процедура планової зміни ключів Центру здійснюється в такому порядку:

- посадові особи, призначені наказом директора ЦСК, в присутності адміністратора безпеки виконують генерацію нового особистого ключа ЦСК;
- адміністратор сертифікації ініціює процес засвідчення чинності відкритого ключа ЦСК в Центральному засвідчувальному органі шляхом передачі запиту на формування сертифіката;
- після отримання сертифіката від Центрального засвідчувального органу, новий сертифікат публікується на інформаційному ресурсі ЦСК.

Після публікації нового сертифіката на інформаційному ресурсі ЦСК (web-сторінці), старий особистий ключ знищується надійним способом.

Перевірка ЕЦП на документах, підписаних за допомогою старого особистого ключа, здійснюється шляхом застосування відповідного йому скасованого сертифіката ключа, який зберігається в інформаційному ресурсі ЦСК та в архіві Центрального засвідчувального органу.

### 10.2. Порядок позапланової зміни ключів ЦСК

У випадку компрометації або загрози компрометації особистого ключа ЦСК виконується позапланова зміна ключів.

Процедура позапланової зміни ключів ЦСК виконується в порядку, визначеному процедурою планової зміни ключів.

Після публікації нового сертифіката у загальнодоступному інформаційному ресурсі ЦСК (web-сторінці), старий особистий ключ знищується надійним способом.

Сертифікати ключів всіх підписувачів та сертифікат ключа ЦСК скасовуються шляхом занесення в список відкликаних сертифікатів.

Список відкликаних сертифікатів підписується новим особистим ключем ЦСК.

Центр офіційно сповіщає заявників про факт позапланової зміни ключів ЦСК.

Після одержання офіційного повідомлення про факт позапланової зміни ключів ЦСК, заявникам потрібно одержати нові ключі і сертифікати відповідно до положень цього Регламенту.

## 11. Порядок синхронізації часу у ПТК

Час ПТК синхронізується із Всесвітнім координованим часом (UTC) з точністю до однієї секунди. Порядок синхронізації виконувати таким чином:

Обидва сервери (сервер 1 та сервер 2) синхронізувати з зовнішніми серверами часу не нижче другого рівня (stratum 2) за протоколом NTP - у кількості не менш трьох. Перелік серверів часу складає системний адміністратор та затверджує адміністратор безпеки.

На серверах працюючих в кластері під керуванням операційної системи Red Hat встановити службу часу (NTP) та налаштувати синхронізацію наступним чином:

- Для першого серверу кластеру, серверами синхронізації часу призначити такі сервери:
  - сервер 1;
  - сервер 2;
  - другий сервер кластеру під керуванням Red Hat
- Для другого серверу кластеру серверами синхронізації часу призначити такі сервери:
  - сервер 1;
  - сервер 2;
  - перший сервер кластеру під керуванням Red Hat

Перевірка функціонування синхронізації часу здійснюється не рідше одного разу на тиждень.