Примірник № 4

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

О.М. Чаузов

«5» 11 2018 року

ЗАТВЕРДЖУЮ
Генеральний прокурор України

Ю.В. Луценко

«5» листопада 2018 року

РЕГЛАМЕНТ РОБОТИ

ЦЕНТРУ СЕРТИФІКАЦІЇ КЛЮЧІВ ГЕНЕРАЛЬНОЇ ПРОКУРАТУРИ УКРАЇНИ

Перший заступник
Генерального прокурора

Д.А. Сторожук

«30» жовтня 2018 року

Начальник Департаменту
інформаційних технологій,
документального та
матеріально-технічного
забезпечення

К.І. Моргун

«29» жовтня 2018 року

Київ
2018 рік

Зміст

Додатки:

Додаток № 1. Заява на проведення реєстрації.

Додаток № 2. Заява про зміну статусу посиленого сертифіката відкритого ключа.

Перелік скорочень

БД	база даних
ВПР	Відокремленний пункт реєстрації
ЕЦП	електронний цифровий підпис
ІТС	інформаційно-телекомунікаційна система
КЗІ	криптографічний захист інформації
КСЗІ	комплексна система захисту інформації
НКІ	носій ключової інформації
ПЗ	програмне забезпечення
ПТК	програмно-технічний комплекс
СВС	список відкликаних сертифікатів
СУБД	система управління базами даних
ТЗІ	технічний захист інформації
ЦЗО	Центральний засвідчувальний орган
ЦОД	центр обробки даних
ЦР	центр реєстрації
ЦСК	центр сертифікації ключів

Загальні положення

Статус Регламенту

Даний Регламент є нормативним документом, що визначає організаційні, технічні та інші умови діяльності Центру сертифікації ключів Генеральної прокуратури України (далі – ЦСК або Центр) під час надання послуг електронного цифрового підпису, встановлює порядок роботи та процедури центру сертифікації ключів з надання послуг електронного цифрового підпису (далі – ЕЦП).

Норми цього Регламенту поширюються на всіх суб'єктів відносин, що в ньому визначені. Чітке дотримання та виконання умов Регламенту для всіх сторін, що визначаються ним як суб'єкти відносин, є обов'язковим.

Будь-яка зацікавлена особа може ознайомитися з положеннями Регламенту на електронному інформаційному ресурсі, в приміщенні ЦСК та його відокремлених пунктів.

Регламент розроблений у відповідності до:

- Закону України «Про електронний цифровий підпис» від 22 травня 2003 року №852-IV;
- Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу, затвердженого постановою Кабінету Міністрів України від 26 травня 2004 року № 680;
- Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності, затвердженому постановою Кабінету Міністрів України від 28 жовтня 2004 року № 1452;
- Порядку акредитації центру сертифікації ключів, затвердженому постановою Кабінету Міністрів України від 13 липня 2004 року № 903;
- Правил посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 року № 3 (у редакції наказу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 10 травня 2006 року № 50) та зареєстрованих в Міністерстві юстиції України 17 травня 2006 року за № 568/12442.

Порядок затвердження і внесення змін та доповнень до Регламенту

Регламент затверджується Генеральним прокурором України за погодженням з Адміністрацією Державної служби спеціального зв'язку та захисту інформації України.

Внесення змін та доповнень до цього Регламенту здійснюється у порядку, встановленому для його затвердження у відповідності до чинного законодавства України.

Про внесення змін та доповнень до цього Регламенту, ЦСК повідомляє Підписувачів та інших зацікавлених осіб шляхом розміщення зазначених змін та доповнень на електронному інформаційному ресурсі ЦСК.
Зміни та доповнення до Регламенту, що не пов'язані зі зміною чинного законодавства України, набувають чинності через 10 (десять) календарних днів з моменту розміщення зазначених змін і доповнень на електронному інформаційному ресурсі ЦСК.
Зміни та доповнення, внесені до Регламенту у зв'язку зі зміною законодавства України, набувають чинності одночасно із набранням чинності змін до відповідних нормативно-правових актів.

Суб'єкти відносин

Суб'єктами відносин, що визначаються положеннями цього Регламенту є:

Центр сертифікації ключів Генеральної прокуратури України – підрозділ Генеральної прокуратури України, що надає послуги електронного цифрового підпису, забезпечує функціонування та розвиток Центру, виконання вимог законодоавства до акредитованих центрів сертифікації ключів і у сфері захисту персональних даних та такий, що засвідчив свій відкритий ключ у Центральному засвідчувальному органі (ЦЗО) України.

Відокремлений пункт реєстрації – підрозділ регіонального органу Генеральної прокуратури України, який здійснює надання послуг електронного цифрового підпису з реєстрації та обслуговування Підписувачів на відповідній території.

Заявник – посадова особа, яка звертається до Центру з метою формування сертифіката.

Підписувач – особа, яка на законних підставах володіє особистим ключем та від свого імені накладає електронний цифровий підпис під час створення електронного документа.

Підписувачами можуть бути працівники органів прокуратури України або посадові особи інших органів державної влади (далі – державні органи), які звернулись у встановленому Регламентом порядку до ЦСК чи його відокремлених пунктів реєстрації з метою отримання послуги ЕЦП для доступу до інформаційно-телекомунікаційних систем, держателем яких є Генеральна прокуратура України.

Підписувач здійснює використання особистого ключа відповідно положень цього Регламенту. Норми даного Регламенту є обов'язковими для Підписувача та ЦСК з моменту подачі Підписувачем заяви до ЦСК на отримання посиленого сертифікату відкритого ключа.

Визначення термінів

У цьому Регламенті терміни вживаються у такому значенні:

абонент – посадова особа, яка на законних підставах отримує від ЦСК послуги ЕЦП;

автентифікація – процес, у тому числі електронний, який дає змогу підтвердити належність ідентифікаційних даних заявника;

автоматизована система – організаційно-технічна система ЦСК, що забезпечує обслуговування сертифікатів та об'єднує програмно-технічний комплекс, фізичне середовище, обслуговуючий персонал, а також інформацію, що обробляється в ЦСК;

акредитація – процедура документального засвідчення компетентності ЦСК здійснювати діяльність, пов'язану з обслуговуванням посилених сертифікатів ключів;

блокування сертифіката ключа – тимчасове зупинення чинності сертифіката ключа;

відкритий ключ – параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання ЕЦП;

відокремлений пункт реєстрації – підрозділ ЦСК, який здійснює реєстрацію підписувачів;

електронний підпис – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних;

ЕЦП – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. ЕЦП накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа;

засвідчення чинності відкритого ключа – процедура формування сертифіката відкритого ключа;

засіб ЕЦП – програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки ЕЦП;

захищений носій – носій (smart card, touch-memory тощо), що призначений для зберігання особистого ключа та має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на нього даних від несанкціонованого доступу;

заявник – посадова особа, яка звертається у встановленому цим Регламентом порядку до ЦСК чи його відокремлених пунктів з метою отримання послуги ЕЦП (формування посиленого сертифіката ключа);

ідентифікація особи – встановлення тотожності посадової особи на підставі ідентифікаційних даних;

компрометація особистого ключа – будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа, у тому числі втрата, крадіжка, несанкціоноване копіювання особистого ключа або пароля доступу до нього;

користувач – посадова особа, яка перевіряє ЕЦП, накладений підписувачем на електронний документ;

надійний засіб ЕЦП – засіб електронного цифрового підпису, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації;

особистий ключ – параметр криптографічного алгоритму формування ЕЦП, доступний тільки підписувачу;

підписувач – посадова особа, яка на законних підставах володіє особистим ключем та від свого імені накладає ЕЦП під час створення електронного документа;

повторне формування сертифіката – формування нового сертифіката ЦСК для підписувача, який є власником чинного сертифіката, сформованого даним центром сертифікації ключів;

посилений сертифікат відкритого ключа (далі – сертифікат) – документ, виданий ЦСК, який засвідчує чинність і належність відкритого ключа підписувачу (відповідно до наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18 грудня 2012 року № 739, складається з сертифікату для ЕЦП та сертифікату шифрування);

послуги ЕЦП – надання у користування надійних засобів ЕЦП, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги, визначені Законом України «Про електронний цифровий підпис» від 22 травня 2003 року № 852-IV;

програмно-технічний комплекс – апаратні, апаратно-програмні та програмні засоби центру, що забезпечують виконання функцій, пов'язаних з наданням послуг ЕЦП;

реєстрація – встановлення підписувача та перевірка наданих даних, що включаються у сертифікат;

розпізнавальне ім'я – сукупність реквізитів підписувача, що забезпечують можливість однозначного визначення належності сертифіката цьому підписувачу серед інших сертифікатів, сформованих у ЦСК;

розповсюдження сертифіката ключа – надання сертифіката ключа підписувачу – власнику особистого ключа або, у разі його згоди, іншим користувачам;

розповсюдження інформації про статус сертифіката – надання вільного доступу до інформації про статус сертифіката у реальному часі у вигляді інформації про статус сертифіката, що оновлюється за визначеним періодом часу або у разі необхідності;

сертифікат відкритого ключа (далі – сертифікат ключа, сертифікат) – документ, виданий ЦСК, який засвідчує чинність і належність відкритого ключа підписувачу. Сертифікати ключів можуть використовуватися для ідентифікації особи підписувача;

сертифікація – формування сертифіката, заснованого на перевірених при реєстрації даних, накладання на сертифікат ЕЦП за допомогою особистого ключа центру;

спеціальне приміщення – приміщення, яке відповідає вимогам, що наведені у додатку до пункту 4.1.1 Правил посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 року № 3 (у редакції наказу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 10 травня 2006 року № 50);

список відкликаних сертифікатів – перелік блокованих та скасованих сертифікатів, що формується та розповсюджується центром;

статус сертифіката – стан сертифіката ключа (чинний, блокований, скасований) на конкретний момент;

управління статусом сертифіката – зміна статусу сертифіката на підставі відповідних запитів та за умовами, визначеними Законом України «Про електронний цифровий підпис» від 22 травня 2003 року № 852-IV;

центр реєстрації – окремий підрозділ центру сертифікації ключів, який відповідає за реєстрацію заяв на сертифікат, про блокування, скасування та відновлення сертифікатів від підписувачів;

Інші терміни застосовуються у значеннях, наведених у Законі України «Про електронний цифровий підпис» від 22 травня 2003 року № 852-IV, Порядку акредитації центру сертифікації ключів, затвердженому постановою Кабінету

Міністрів України від 13 липня 2004 року № 903, інших нормативно-правових актах з питань криптографічного та технічного захисту інформації.

1. Загальні відомості про ЦСК

1.1. Ідентифікаційні дані ЦСК

Повне найменування юридичної особи: Генеральна прокуратура України.

Скорочене найменування юридичної особи: ГПУ.

Повне найменування Центру: Центр сертифікації ключів Генеральної прокуратури України.

Скорочене найменування Центру: ЦСК ГПУ.

ЦСК підпорядкований управлінню інформаційних технологій Департаменту інформаційних технологій, документального та матеріально-технічного забезпечення і розміщується за адресою: Україна, 01011, м. Київ, вул. Різницька, 13/15.

Телефон: +38 (044) 200-75-84.

Код ЄДРПОУ: 00034051.

Електронна поштова скринька (e-mail): csk@ca.gp.gov.ua

Електронна адреса інформаційного ресурсу (web-сайту) Центру: https://ca.gp.gov.ua

1.2. Сфера та підстави діяльності ЦСК

ЦСК здійснює свою діяльність у сфері надання послуг ЕЦП органам прокуратури та іншим державним органам для доступу до інформаційно-телекомунікаційних систем, держателем яких є Генеральна прокуратура України, у тому числі системи електронного документообігу.

Діяльність ЦСК не поширюється на відносини, що виникають під час використання інших видів електронного підпису, в тому числі переведеного у цифрову форму зображення власноручного підпису.

1.3. Послуги ЕЦП, що надаються ЦСК

Під послугами ЕЦП розуміється надання у користування засобів ЕЦП, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги, визначені Законом України від 22.05.2003 р. N 852-IV «Про електронний цифровий підпис».

Перелік послуг ЕЦП, що надаються ЦСК:

1) обслуговування посилених сертифікатів відкритих ключів (далі – сертифікатів) Підписувачів ЦСК, що включає:
   - реєстрацію Підписувачів;
   - сертифікацію відкритих ключів Підписувачів;
   - розповсюдження сертифікатів;
   - управління статусом сертифікатів та розповсюдження інформації про статус сертифікатів;
   - надання послуг фіксування часу;
   - надання Підписувачам ЦСК допомоги в генерації відкритих та особистих ключів;
2) надання Підписувачам ЦСК:
   - засобів ЕЦП та шифрування даних;
   - консультаційні послуги у сфері ЕЦП.

Надання вищезазначених послуг здійснюється ЦСК у відповідності до цього Регламенту.

1.4. Сфери використання сертифікатів

Сертифікати відкритого ключа, що формуються Центром використовуються для перевірки та підтвердження ЕЦП, який задовольняє вимогам щодо підпису, застосованого до даних в електронній формі, у той же спосіб, як власноручні підписи задовольняють вимогам стосовно документа на папері.

ЦСК здійснює обслуговування сертифікатів ключів, сформованих для посадових осіб оранів прокуртаури України та інших посадових осіб державних органів для доступу до ІТС, держателем яких є Генеральна прокуратура України, у тому числі до системи електронного документообігу.

Виданий ЦСК сертифікат використовується для засвідчення чинності і належності відкритого ключа Підписувачу, автентифікації в електронних системах та системах електронного документообігу.

Особисті ключі ЕЦП і відповідні їм сертифікати, що формуються ЦСК, і за правовим статусом прирівнюються до власноручного підпису та печатки і можуть використовуватися в усіх сферах, де використовується власноручний підпис посадових осіб.

ЦСК має право встановлювати обмеження сфери використання сформованих ним сертифікатів ключів. Інформація щодо обмеження сфери використання

застосовується у відповідно до вимог законодавства та доводиться до Підписувача (заявника) та зазначається у сформованому ЦСК сертифікаті ключа.

1.5. Відокремлені пункти реєстрації

Відокремлені пункти реєстрації (далі – ВПР) є відокремленими регіональними підрозділами при органах прокуратури регіонального рівня, що реалізують функції ЦСК з реєстрації Підписувачів та їх подальшого обслуговування на відповідній території, крім формування сертифікатів та СВС.

Відокремлені пункти діють на підставі цього Регламенту.

Керівництво ВПР здійснює віддалений адміністратор реєстрації ВПР.

Безпосереднє управління ВПР здійснюється ЦСК.

2. Права та обов'язки ЦСК та Підписувачів

2.1. Центр сертифікації ключів

2.1.1. ЦСК має право:

- надавати послуги ЕЦП в обсягах, передбачених чинним законодавством;
- під час реєстрації вимагати від Підписувача надавати повну та дійсну інформацію необхідну для формування сертифіката, а також здійснювати перевірку наданої інформації;
- скасовувати, блокувати, поновлював
- ти сертифікати Підписувача у порядку визначеному цим Регламентом;
- вимагати від Підписувача дотримуватись вимог цього Регламенту та умов надання послуг;
- при виникненні необхідності зміни даних, зазначених у сертифікаті, здійснювати переформування сертифіката підписувачу із використанням попередньо засвідченого відкритого ключа підписувача у разі якщо відповідний йому особистий ключ не був скомпрометований та з дотриманням вимог щодо недопущення перевищення часу чинності особистого ключа та відповідного йому відкритого ключа більше двох років;
- припинити надання Підписувачу послуг ЕЦП у разі порушення умов цього Регламенту або вимог законодавства в сфері ЕЦП та захисту інформації.

2.1.2. ЦСК зобов'язаний:

- використовувати особистий ключ Центру, відповідний засвідченому в ЦЗО відкритому ключу (шляхом формування сертифіката), виключно для формування сертифікатів Підписувачів та списків відкликаних сертифікатів (СВС);
- забезпечити можливість цілодобового доступу Підписувачів до даних про статус сертифікату ЦСК, нормативних документів з питань надання послуг ЕЦП, до сертифікатів ключів Підписувачів через загальнодоступні телекомунікаційні ресурси (спеціальні відомчі інформаційні системи);
- забезпечувати захист інформації в ІТС Центру шляхом використання комплексної системи захисту інформації (КСЗІ), яка має атестат відповідності нормативним документам із захисту інформації;
- забезпечувати захист персональних даних, отриманих від Підписувача, згідно діючого законодавства;
- забезпечувати реєстрацію та облік Підписувачів за заявами відповідно до порядку реєстрації, визначеному у даному Регламенті;

- ознайомлювати Підписувача із умовами обслуговування сертифікатів перед наданням послуг ЕЦП через електронний інформаційний ресурс або в інший спосіб;
- встановлювати відповідно до законодавства осіб, які звернулись до ЦСК з метою формування сертифіката ключа;
- перевіряти дані, обов'язкові для формування сертифікату, і дані, які вносяться до нього на вимогу Підписувача;
- забезпечувати формування сертифікатів зареєстрованого Підписувача відповідно до порядку, визначеного у даному Регламенті;
- формувати сертифікат ключа згідно із законом та у форматі, визначеному законодавством;
- забезпечувати цілісність та автентичність сформованих сертифікатів;
- забезпечувати унікальність розпізнавального імені та реєстраційного номера сертифіката Підписувача, що формуються ЦСК;
- встановлювати належність відкритого ключа та відповідного особистого ключа Підписувачу під час формування сертифіката;
- інформувати Підписувачів про необхідність здійснення перевірки чинності сертифіката з використанням інформації про його статус та врахування всіх визначених у сертифікаті обмежень щодо його використання;
- своєчасно попереджувати Підписувача та додавати до сертифіката Підписувача інформацію про обмеження використання ЕЦП;
- перевіряти законність звернень про скасування, блокування та поновлення сертифікатів та зберігати документи, на підставі яких були скасовані, блоковані та поновлені сертифікати;
- скасовувати сертифікат за заявою на скасування, що надходить від Підписувача, або за іншими умовами, які визначені чинним законодавством, та протягом 2 годин занести відомості про скасований сертифікат в СВС із зазначенням дати та часу занесення та причини скасування;
- блокувати сертифікат за заявою на блокування, що надходить від його власника, або за іншими умовами, які визначені чинним законодавством, в усній формі чи у електронному вигляді, та протягом 2 годин занести відомості про блокований сертифікат у СВС із зазначенням дати та часу занесення;
- поновлювати сертифікат за заявою на поновлення, що надходить від його власника, або за іншими умовами, які визначені чинним законодавством, не пізніше одного робочого дня, наступного за робочим днем, протягом якого була подана заява, та виключити відомості про блокований сертифікат зі СВС;
- вести електронний перелік чинних, скасованих і блокованих сертифікатів ключів;

- забезпечити зберігання сформованих сертифікатів протягом строку, передбаченого законодавством для зберігання відповідних документів на папері;
- забезпечувати резервування усіх сформованих сертифікатів;
- цілодобово приймати заяви про скасування, блокування та поновлення сертифікатів ключів;
- публікувати СВС на електронному інформаційному ресурсі ЦСК із періодичністю не менш ніж один раз у 2 години;
- встановлювати за київським часом, синхронізованим з Всесвітнім координованим часом (UTC) з точністю до однієї секунди, час формування, скасування, блокування та поновлення сертифікатів ключів;
- забезпечувати протоколювання всіх подій, пов'язаних із формуванням, переформуванням, блокуванням, поновленням та скасуванням сертифікатів ключів, виданих ЦСК, із забезпеченням захисту протоколів від несанкціонованого доступу;
- при повторному формуванні сертифіката ключа здійснювати перевірку стосовно того, що інформація, яка надавалася раніше заявником під час реєстрації, дійсна;
- надавати консультації з питань, пов'язаних з ЕЦП;
- використовувати ПТК ЦСК, засоби КЗІ, у тому числі засоби ЕЦП, що відповідають вимогам нормативних документів у галузі криптографічного та технічного захисту інформації та мають позитивний експертній висновок у галузі КЗІ та атестат відповідності КСЗІ ЦСК;
- розташовувати засоби ПТК, які забезпечують роботу з особистим ключем ЦСК у спеціальних приміщеннях, здійснювати їх охорону для запобігання безконтрольного проникнення у спеціальні приміщення (серверну) ЦСК сторонніх осіб;
- під час генерації ключів підписувачам вжити заходів конфіденційності;
- не допускати зберігання особистих ключів підписувачів та ознайомлення з ними в ЦСК;
- вести облік засобів КЗІ, ключових документів, програмно-апаратних та апаратних носіїв особистих ключів підписувачів, надійних засобів ЕЦП у журналі обліку, видачі засобів КЗІ та носіїв ключової інформації до них;
- зберігати та вести облік документів (засвідчених в установчому порядку копій оригіналів документів), що використовуються під час реєстрації.

2.2. Підписувач

2.2.1. Підписувач (заявник) має право:

- своєчасно отримувати якісні послуги ЕЦП;
- одержувати сертифікати ключів ЦСК;
- одержувати список відкликаних сертифікатів, сформований ЦСК;
- застосовувати сертифікат ЦСК для перевірки справжності ЕЦП сертифікатів, сформованих ЦСК (у тому числі через ВПР);
- застосовувати СВС, сформований ЦСК, та протокол інтерактивного визначення статусу сертифіката (OCSP) для перевірки статусу власного сертифіката та сертифікатів інших Підписувачів;
- ознайомитись з інформацією щодо діяльності ЦСК, його ЦР та надання послуг ЕЦП;
- вимагати скасування, блокування або поновлення свого сертифіката ключа;
- вимагати від ЦСК чи ЦР усунення порушень умов даного Регламенту;
- вимагати від ЦСК чи ЦР виконання вимог із захисту інформації при використанні персональних даних (конфіденційності);
- подавати заяви, скарги, претензії.

2.2.2. Підписувач (заявник) зобов'язаний:

- ознайомитись та дотримуватись правил надання послуг ЕЦП, визначених даним Регламентом;
- надавати повну та дійсну інформацію під час реєстрації, необхідну для формування сертифіката ключа;
- використовувати особистий ключ відповідно до призначення ключа, зазначеного у сертифікаті відкритого ключа, а також додержуватися інших вимог щодо його використання, визначених ЦСК у цьому Регламенті;
- використовувати надійні засоби ЕЦП для генерації особистих та відкритих ключів, формування та перевірки ЕЦП;
- негайно інформувати ЦСК про наступні події, що трапилися до закінчення строку чинності сертифіката: втрату або компрометацію особистого ключа; виявлену неточність або зміни даних, зазначених у сертифікаті;
- не використовувати особистий ключ в разі його компрометації;
- зберігати в таємниці особистий ключ та вживати всі можливі заходи для запобігання його втрати, розкриття, модифікації та несанкціонованого використання іншими особами;

- не розголошувати та не повідомляти іншим особам пароль доступу до особистого ключа та фразу-пароль для блокування сертифікату за телефоном;
- не використовувати особистий ключ, відповідний до сертифікату, заява на скасування чи блокування якого подана до ЦСК, протягом часу з моменту подання заяви і до моменту офіційного повідомлення про скасування сертифікату;
- не використовувати особистий ключ, відповідний до сертифіката, що скасований або блокований;
- не застосовувати особистий ключ, якщо стало відомо, що цей ключ використовується або використовувався раніше іншими особами;
- в разі компрометації паролю захисту особистого ключа, негайно змінити пароль захисту, якщо є впевненість, що доступ до особистого ключа інших осіб був неможливий, у зворотному випадку вважати особистий ключ скомпрометованим і виконати процедуру скасування сертифікату;
- використовувати сертифікати для перевіряння ЕЦП, а також свій особистий ключ для формування ЕЦП тільки після перевірки чинності відповідного сертифіката, з використанням інформації про статус сертифіката.

2.3. Відповідальність Сторін

У разі невиконання своїх обов'язків згідно з чинним законодавством ЦСК, ЦР, ВПР та Підписувач, несуть визначену чинним законодавством відповідальність.

Сторони не відповідають за невиконання або неналежне виконання своїх обов'язків за даним Регламентом, а також за збитки, які виникли у зв'язку з цим, у випадках, якщо це є наслідком попереднього невиконання або неналежного виконання іншою стороною своїх обов'язків.

ЦСК не несе відповідальності за майнову та моральну шкоду, що була спричинена Підписувачу неналежною роботою клієнтського програмного забезпечення (ПЗ) ЦСК у разі, якщо неналежна робота зазначеного ПЗ була викликана неналежним захистом робочої станції, де Підписувач застосовує ПЗ ЕЦП (наприклад, «мережевими атаками», дією «вірусних програм» та іншим неякісним або не ліцензованим програмним забезпеченням Підписувача).

ЦСК не несе відповідальності за майнову та моральну шкоду, що може бути спричинена Підписувачу та (або) третім особам у разі невиконання або неналежного виконання Підписувачем цього Регламенту.

3. Умови, процедури та механізми надання ЦСК послуг Підписувачам

Всі процедури по обслуговуванню Підписувачів здійснюються після їх ознайомлення з наступними положеннями цього Регламенту:

- права та обов'язки Підписувача і ЦСК та їх відповідальність;
- порядок ідентифікації та реєстрації Підписувача;
- порядок генерації ключів ЕЦП;
- порядок формування сертифікатів;
- сфери використання посиленого сертифіката та обмеження щодо його використання;
- порядок перевірки чинності посиленого сертифіката,
- порядок блокування, скасування та поновлення сертифіката, який викладено в цьому розділі.

3.1. Порядок ідентифікації та реєстрації Підписувачів (заявників)

Під реєстрацією Підписувача розуміється внесення інформації про Підписувача до реєстру Підписувачів ЦСК.

Проведення реєстрації здійснюється в ЦР ЦСК у робочий час згідно з розпорядком роботи ЦСК.

Для проведення реєстрації особа подає до ЦСК заяву про проведення реєстрації та комплект документів за переліком та у порядку, що визначені у цьому Регламенті та порядку, затвердженому постановою Кабінету Міністрів України від 28.10.2004 №1452.

Для проведення реєстрації особа (заявник), яка бажає стати Підписувачем ЦСК, повинна надати до відповідного ЦР наступні документи:

- заяву на проведення реєстрації, та формування посиленого сертифікату відкритого ключа ЕЦП (додаток № 1 до Реламенту);
- оригінал паспорта або паспорта заявника виготовленого у формі ID-картки, що містить безконтактний електронний носій (також надаються засвідчені підписом власника копії 1–2 сторінок паспорта і сторінки з актуальнною реєстрацією (3–6 за наявності відміток) або лицьового та зворотного боку ID-картки та копія паперового витягу з Єдиного державного демографічного реєстру щодо реєстрації місця проживання);
- оригінал картки фізичної особи — платника податків з реєстраційним номером облікової картки платника податків (РНОКПП) та її копію завсідчену підписом власника (у разі якщо через релігійні переконання посадова особа відмовилась від РНОКПП - не подається, однак надається засвідчена підписом власника копія відповідної сторінки паспорта з відміткою про це);

- оригінал службового посвідчення;
- копію наказу або витяг з наказу або довідку кадрового підрозділу про призначення на посаду (перебування на посаді), що завірена належним чином. Вказаний документ має бути видано/посвідчено не раніше 5 днів до звернення до ЦР.

Копії документів (заяви, копії паспортів тощо) засвідчуються підписом Підписувача (заявника) та звіряються уповноваженою особою ЦСК, якій надаються копії разом з оригіналами. Використання факсимільного підпису під час засвідчення документів не допускається.

До розгляду не приймаються документи, які мають підчистки, дописки, закреслені слова, інші незастережні виправлення або написи олівцем, а також мають пошкодження, внаслідок чого їх текст неможливо прочитати.

Бланки реєстраційних документів (заява на реєстрацію тощо) встановленої форми розміщуються на інформаційному ресурсі ЦСК.

3.1.1. Процедура проведення реєстрації Підписувача

Особа, що звертається до ЦСК для формування сертифіката, подає документи оператору реєстрації ЦР.

Оператор реєстрації виконує процедуру ідентифікації особи, яка проходить процедуру реєстрації, шляхом установлення особи за паспортом.

При ідентифікації посадової особи з'ясовують:

- прізвище, ім'я та по батькові;
- дату народження;
- серію і номер паспорта (або іншого документа, який засвідчує особу), дату видачі та орган, що його видав;
- реєстраційний номер облікової картки платника податків (РНОКПП) або відмітку в паспорті.

Після позитивної ідентифікації оператор реєстрації приймає та розглядає документи, надані особою.

Оператор реєстрації ЦР приймає рішення про відмову в реєстрації за результатом розгляду поданих документів у разі:

- відсутності всіх необхідних для реєстрації документів;
- подання заявником неналежно засвідчених копій документів чи документів, які мають підчистки, дописки, закреслені слова, інші незастережні виправлення або написи олівцем, а також мають пошкодження, внаслідок чого їх текст неможливо прочитати;

- невідповідності даних, що визначені в поданих документах, фактичним даним Підписувача (заявника);
- відсутності у посадової особи іншого державного органу підстав для доступу до ІТС, держателем яких є Генеральна прокуратура України.

У разі відмови в реєстрації заява на реєстрацію разом з додатками повертається заявнику з позначкою оператора реєстрації ЦР.

При ухваленні позитивного рішення оператор реєстрації ЦР виконує реєстраційні дії щодо занесення реєстраційної інформації до електронного реєстру абонентів ЦСК, робить копії документів (за необхідності) та формує з них справу Підписувача.

Справі Підписувача надається номер, яким вона підписується та за яким реєструється в «Журнал обліку справ підписувачів ЦСК».

Справи зберігаються в металевих шафах, що забезпечують надійний захист від несанкціонованого доступу, в ЦР.

Оператор реєстрації проводить інформування Підписувача щодо порядку надання послуг ЕЦП, правил поводження з особистими ключами, особливостей і обмежень використання сертифікату.

Реєстрація заявника є підставою для генерації ключів та формування сертифіката ключа підписувача.

Адміністратор реєстрації, як і оператор реєстрації, може проводити процедури з ідентифікації та реєстрації заявника (Підписувача).

3.2. Порядок генерації ключів Підписувача

Для використання ЕЦП відповідно асиметричного алгоритму, визначеному ДСТУ 4145-2002, Підписувач повинен згенерувати пару ключів – відкритий та особистий.

Процедура генерації ключів ЕЦП проходить два етапа:
- генерація стартових ключів;
- генерація робочих ключів.

За введеними під час реєстрації даними оператор реєстрації генерує стартові ключі за допомогою ПЗ. При цьому ключова пара в захищеному вигляді зберігається на НКІ, що видається в користування Підписувачу центром реєстрації ключів або надається самим Заявником. Так ключовий контейнер може зберігатися у шифрованому вигляді як файл або зберігатися на апаратному захищеному НКІ.

Пароль доступу до ключа у шифрованому файловому контейнері або апаратному захищеному НКІ, вводиться оператором реєстрації та повідомляється Підписувачу.

Запит на формування стартового сертифікату засвідчується ЕЦП оператора реєстрації та відправляється електронними засобами до ЦСК. Стартовий сертифікат відкритого ключа формується ЦСК в автоматичному режимі, відправляється до ЦР та записується ПЗ разом із ланцюжком сертифікатів ЦСК до файлового контейнера Підписувача або апаратному захищеному НКІ. Термін дії стартового сертифіката складає сім днів.

Після формування стартового сертифікату оператором реєстрації чи адміністратором реєстрації на вимогу Підписувача виготовляє дві копії стартового сертифіката у вигляді документа у паперовій формі. Копії сертифікатів засвідчуються власноручним підписом Підписувача, а також власноручним підписом оператора реєстрації чи адміністратора реєстрації, а Підписувач на другій копії сертифіката ставить відмітку про отримання такої копії.

Оператор реєстрації чи адміністратор реєстрації видає НКІ з файловим ключовим контейнером чи апаратний захищений НКІ, Підписувачу.

Підписувач підключає свій НКІ до відокремленого комп'ютеру, що не підключений до мережі. За допомогою ПЗ генерації ключів Підписувач генерує робочу ключову пару. Під час генерації особистий ключ зберігається на НКІ Підписувача. Одночасно Підписувач вводить новий пароль доступу до файлового контейнеру чи апаратного захищеного НКІ.

Запит на робочий сертифікат підписаний стартовим ключем, Підписувач записує на технологічний носій ЦР та передає його адміністратору реєстрації.

Строк дії особистого ключа Підписувача

Строк дії особистого ключа Підписувача становить один рік. Початком строку дії особистого ключа Підписувача є дата та час початку дії сертифікату, зазначені у сертифікаті.

3.3. Порядок формування сертифікатів та надання їх Підписувачам

Формування сертифіката Підписувача проводиться в ЦСК за запитом, який надходить від адміністратора реєстрації ЦР.

Формування сертифіката може бути первинним (під час першого звернення Заявника до ЦСК), та повторним. Повторне формування сертифіката проводиться в таких випадках:

- закінчення строку чинності сертифіката ключа;

- скасування сертифіката за заявою власника;
- зміна даних, що вносяться до сертифікату ключа;
- компрометація особистого ключа.

3.3.1. Порядок первинного формування сертифіката

Процедура формування сертифіката відкритого ключа Підписувача проводиться після успішного завершення процедур реєстрації та генерації робочих ключів.

Адміністратор реєстрації перевіряє коректність даних Підписувача, що внесені в запит на формування сертифікату.

Після позитивної перевірки поданого запиту з відкритим ключем, адміністратор реєстрації за допомогою ПЗ засвідчує запит власним ключем ЕЦП та відправляє до ЦСК для формування сертифіката.

ПТК відправляє запит внутрішньою електронною поштою та отримує з ЦСК електронну квитанцію про отримання. При цьому статус запиту на формування сертифікату в електронному реєстрі ЦР змінюється на «Прийнятий ЦСК». Якщо квитанція про отримання не надійшла та статус залишився «Відправлений» протягом 15 хв., адміністратор реєстрації повторює відправлення запиту до ЦСК.

Після того, як запит на формування сертифіката засвідчується ПЗ адміністратора сертифікації, сервер ЦСК формує сертифікат та засвідчує його особистим ключем ЦСК.

Після формування сертифікат публікується в LDAP-каталог та відсилається до ЦР, з якого надійшов запит, внутрішньою електронною поштою у вигляді квитанції.

Сертифікат в електронній формі записується на НКІ Підписувача на робочий станції генерації ключів, якщо введення в дію ключів ЕЦП Підписувача здійснюється в ЦР.

Якщо введення в дію ключів ЕЦП Підписувача здійснюється на робочому місці Підписувача, то отримання сертифікату з LDAP-каталогу та запис його до НКІ здійснює прикладне ПЗ користувача при першому використанню ключів.

Введення в дію ключів ЕЦП Підписувача можливе протягом строку дії стартового сертифіката, яка спливає о 0 годин 00 хвилин сьомого дня з моменту його генерації. Після спливу даного часу, процедуру генерації ключів Підписувача необхідно повторити.

3.3.2. Порядок повторного формування сертифіката

Повторне формування сертифіката не потребує проведення реєстраційних дій, крім випадку зміни даних, відображених у сертифікаті ключа.

У випадку зміни даних реєстрація проводиться відповідно до п.3.1 – подається заява, але до неї додаються тільки документи, які містять відомості, в яких відбулися зміни.

Крім того, надається НКІ, якщо такий раніше видавався Підписувачеві у користування даним ЦР.

3.3.3. Особливості використання сертифікатів

Строк чинності сертифіката Підписувача не може перевищувати двох років. Початком строку чинності сертифіката Підписувача є дата та час початку дії сертифіката, що в ньому зазначений.

3.4. Порядок блокування, поновлення та скасування сертифікатів

3.4.1. Причини, за яких Підписувач зобов'язаний скасувати сертифікат

Підписувач зобов'язаний виконати дії зі скасування свого сертифіката у разі:

- компрометації особистого ключа;
- зміни відомостей, зазначених у сертифікаті.

У випадках:

- смерті Підписувача або оголошення його померлим за рішенням суду;
- визнання Підписувача недієздатним за рішенням суду;
- звільнення з посади у відповідному органі;
- припинення діяльності відповідного органу чи його підроздліу

керівництво установи, до якого належить Підписувач, зобов'язаний сповістити ЦСК про ці події письмово та протягом семи днів надати до Центру завірені копії документів, що підтверджують цю подію. ЦСК блокує сертифікат Підписувача при надходженні відповідного письмового сповіщення та скасовує його після отримання документального підтвердження.

Центр автоматично скасовує сертифікат при закінченні строку його чинності або при надходженні в Центр інформації про припинення діляьності відповідного органу, у якому працював Підписувач, про компрометацію особистого ключа Підписувача чи надання Підписувачем недостовірних даних, якщо достовірність цієї інформації підтверджена.

Компрометація ключа Підписувача – це:

- факт або обґрунтована підозра того, що особистий ключ Підписувача став відомий або доступний до використання іншим особам;

- факт втрати Підписувачем можливості подальшого використання особистого ключа із будь-яких обставин (зокрема: фізичне пошкодження або втрата носія, неможливість відтворити пароль захисту).

У випадку компрометації ключа Підписувач зобов'язаний терміново сповістити про цей факт ЦСК та виконати дії згідно пункту 3.4.3.

Сертифікат Підписувача буде скасовано у разі надання до ЦСК третьою особою, загубленого/вилученого НКІ Підписувача та підтвердження його справжності (співпадання внутрішнього ідентифікаційного номера НКІ чи особистого ключа Підписувача).

Зміна будь-якого з реквізитів, що зазначені в сертифікаті, потребує його скасування.

Зокрема, до таких причин належать:

- переведення на іншу посаду або звільнення з роботи власника сертифікату;
- зміна прізвища, ім'я по батькові;
- виявлення помилок у реквізитах тощо.

За виникнення будь-яких причин та обставин, зазначених вище, Підписувач зобов'язаний невідкладно заблокувати сертифікат згідно пункту 3.4.3 та протягом терміну дії блокування виконати операції зі скасування сертифікату згідно пункту 3.4.6.

Дозволяється виконувати безпосередньо скасування сертифікату (обминаючи фазу його блокування).

Документи, що були підставою для скасування, блокування або поновлення сертифіката ключа, фіксуються та зберігаються у ЦСК.

3.4.2. Порядок блокування сертифікатів

Блокування тимчасово припиняє дію сертифіката. Після блокування сертифіката Підписувач зобов'язаний або поновити сертифікат згідно пункту 3.4.8, або виконати скасування сертифікату згідно пункту 3.4.6 цього Регламенту. Для здійснення блокування сертифіката, Підписувач подає заяву на блокування до ЦСК (додаток № 2 до Реламенту).

Блокування сертифіката здійснюється ЦСК на підставі заяви, що надходить установленим порядком в ЦР чи ВПР або церговому адміністратору реєстрації в усній або паперовій формі.

Часом блокування сертифіката вважається час внесення інформації про зміну статусу сертифіката до СВС.

3.4.3. Блокування сертифіката за заявою в усній формі

Заява на блокування в усній формі подається в черговому адміністратору реєстрації за телефоном.

Підписувач повинен повідомити відповідній посадовій особі ЦСК наступну інформацію:

- своє прізвище, ім'я та по батькові;
- ключову фразу-пароль.

Заява в усній формі приймається тільки при збігу даних Підписувача та парольної фрази, переданих в заяві, з інформацією, що знаходиться в реєстрі Підписувачів ЦСК.

Приймання і обробка усної заяви здійснюється цілодобово черговим адміністратором реєстрації або у робочий час відповідною особою ЦР чи ВПР. Обробка усної заяви на блокування сертифіката здійснюється безпосередньо після приймання заяви.

Черговий адміністратор реєстрації після перевірки повідомлених даних за допомогою ПТК формує запит на блокування сертифікат та передає його до ЦСК.

3.4.4. Блокування сертифіката за заявою в паперовій формі

Заява в паперовій формі подається в ЦР за відповідною формою (додаток № 2 до Реламенту).

Заява на блокування сертифіката засвідчується власноручним підписом власника сертифіката.

Подача заяви на блокування сертифіката в ЦР чи ВПР та її розгляд здійснюється тільки в робочий час, відповідно до розпорядку роботи ЦР чи ВПР.

Під час приймання заяви оператор реєстрації чи адміністратор реєстрації ЦСК проводить ідентифікацію Підписувача шляхом установлення особи за паспортом та звірення паспортних даних зі збереженими в реєстрі користувачів.

За умови позитивного результату ідентифікації оператор реєстрації передає заяву адміністратору реєстрації. Адміністратор реєстрації за допомогою ПЗ формує запит на блокування сертифікату з вказанням терміну блокування та передає його до ЦСК.

Обробка заяви в паперовій формі на блокування сертифіката здійснюється на протязі не більш ніж двох годин з моменту подачі заяви.

Адміністратор реєстрації, як і оператор реєстрації, може проводити процедури з ідентифікації та реєстрації заяви.

3.4.5. Блокування сертифіката за зверненням керівництва установи до якої належить Підписувач

Звернення керівнитва установи, до якої належить Підписувач, подається письмово в ЦР у довільній формі.

Звернення про блокування сертифіката виконується на фірмовому бланку та повино бути підписане власноручним підписом керівника такого підрозділу з зазначенням обставин, які викликають необіхність блокування, та долученням належним чином засвідчених копій відповідних документів.

Такими обставинами можуть бути:

- тимчасове відсторонення від посади чи виконання службових обов'язків;
- затримання та обрання запобіжного заходу у вигляді тримання під вартою чи цілодобового домашнього арешту;
- тривале відрядження чи його продовження без можливості Підписувачу самостійно звернутись до ЦР;
- тривала хвороба чи стаціонарне лікування;
- інші причини, які обмежують використання Підписувачем особистого ключа та не дають йому самостійно здійснити блокування сертифіката.

Подача звернення про блокування сертифіката в ЦР та його розгляд здійснюється тільки в робочий час, відповідно до розпорядку роботи ЦР.

Під час отримиання звернення адміністратор реєстрації ЦР перевіряє повноваження керівника та проводить ідентифікацію Підписувача шляхом звірення паспортних даних зі збереженими в реєстрі користувачів.

За умови позитивного результату ідентифікації адміністратор реєстрації за допомогою ПТК формує запит на блокування сертифікату з вказанням терміну блокування та передає його до ЦСК.

Обробка такого звернення на блокування сертифіката здійснюється протяом не більш ніж двох годин з моменту подачі.

3.4.6. Порядок скасування сертифікатів

Операція «Скасування» припиняє дію сертифікату. **Скасовані сертифікати поновленню не підлягають.**

Для скасування сертифіката Підписувач подає заяву на скасування до ЦР (додаток № 2 до Реламенту).

Скасування сертифіката здійснюється ЦСК на підставі заяви, що надходить установленим порядком в ЦР чи ВПР або церговому адміністратору реєстрації в усній або паперовій формі.

Заява на скасування сертифіката подається в ЦР чи ВПР за відповідною формою, яка доступна на інформаційному ресурсі ЦСК, і засвідчується підписом власника сертифіката.

Часом блокування сертифіката вважається час внесення інформації про зміну статусу сертифіката до СВС.

3.4.7. Скасування сертифіката за заявою в усній формі

Заява на блокування в усній формі подається в черговому адміністратору реєстрації ЦСК, ЦР за телефоном.

Підписувач повинен повідомити відповідній посадовій особі ЦСК наступну інформацію:

- своє прізвище, ім'я та по батькові;
- ключову фразу-пароль.

Заява в усній формі приймається тільки при збігу даних Підписувача та парольної фрази, переданих в заяві, з інформацією, що знаходиться в реєстрі Підписувачів ЦСК.

Приймання і обробка усної заяви здійснюється цілодобово черговим адміністратором реєстрації або у робочий час відповідною особою ЦР чи ВПР. Обробка усної заяви на скасування сертифіката здійснюється безпосередньо після приймання заяви.

Черговий адміністратор реєстрації після перевірки повідомлених даних за допомогою ПТК формує запит на скасування сертифікат та передає його до ЦСК.

3.4.8. Скасування сертифіката за заявою в паперовій формі

Заява в паперовій формі подається в ЦР чи ВПР за відповідною формою (додаток № 2 до Реламенту).

Заява на скасування сертифіката засвідчується власноручним підписом власника сертифіката.

Подача заяви на скасування сертифіката в ЦР чи ВПР та її розгляд здійснюється тільки в робочий час, відповідно до розпорядку роботи ЦР чи ВПР.

Під час приймання заяви оператор реєстрації чи адміністратор реєстрації ЦСК проводить ідентифікацію Підписувача шляхом установлення особи за паспортом та звірення паспортних даних зі збереженими в реєстрі користувачів.

За умови позитивного результату ідентифікації оператор реєстрації передає заяву адміністратору реєстрації. Адміністратор реєстрації за допомогою ПЗ формує

запит на скасування сертифікату з вказанням часу скасування та передає його до ЦСК.

Обробка заяви в паперовій формі на скасування сертифіката здійснюється на протязі не більш ніж двох годин з моменту подачі заяви.

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

Часом скасування сертифіката вважається час зміни статусу сертифіката та занесення до СВС.

Адміністратор реєстрації, як і оператор реєстрації, може проводити процедури з ідентифікації та реєстрації заяви.

3.4.9. Скасування сертифіката за зверненням керівнитва установи до якого належить Підписувач

Звернення керівнитва установи, до якої належить Підписувач, подається письмово в ЦР чи ВПР у довільній формі.

Звернення про скасування сертифіката виконується на фірмовому бланку та повино бути підписане власноручним підписом керівника такого підрозділу з зазначенням обставин, які викликають необіхність скасування сертифіката, та долученням належним чином засвідчених копій відповідних документів.

Такими обставинами можуть бути:

- смерть Підписувача;
- набрання законної сили рішенням суду про оголошення його померлим, визнання його безвісно відсутнім, недієздатним, обмеження його цивільної дієздатності;
- припинення діяльності відповідного органу чи його підрозділу;
- тривале відсторонення від посади чи виконання службових обов'язків;
- звільнення після затримання, обрання запобіжного заходу у вигляді тримання під вартою чи цілодобового домашнього арешту, засудження до покарання, повязаного з позбавленням/обмеженям волі;
- тривале закордонне відрядження чи його продовження без можливості Підписувачу самостійно звернутись до ЦР чи ВПР;
- інші причини, які унеможливлюють використання Підписувачем особистого ключа та не дають йому самостійно здійснити скасування сертифіката.

Подача звернення про скасування сертифіката в ЦР чи ВПР та його розгляд здійснюється тільки в робочий час, відповідно до розпорядку роботи ЦР чи ВПР.

Під час отримиання звернення адміністратор реєстрації ЦР ч ВПР перевіряє повноваження керівника та проводить ідентифікацію Підписувача шляхом

звірення паспортних даних зі збереженими в реєстрі користувачів. У випадку надання ЦР чи ВПР Підписувачу у користування носія ключової інформації такий носій має бути повернутий до ЦР чи ВПР.

За умови позитивного результату ідентифікації адміністратор реєстрації за допомогою ПТК формує запит на скасування сертифікату та передає його до ЦСК.

Обробка такого звернення на скасування сертифіката здійснюється протяом не більш ніж двох годин з моменту подачі.

3.4.10. Порядок поновлення чинності сертифікатів

Поновлення чинності сертифікату ключа можливе лише для сертифікатів, що заблоковані. Скасовані сертифікати поновленню не підлягають.

Поновлення чинності сертифіката здійснюється ЦСК на підставі заяви, що Підписувач особисто подає в ЦР у паперовій формі у випадку, якщо блокування відбувалось за заявою Підписувача (додаток № 2 до Реламенту).

Поновлення чинності сертифіката здійснюється ЦСК на підставі заяви, що надходить установленим порядком в ЦР чи ВПР або черговому адміністратору реєстрації в усній або паперовій формі .

3.4.11. Поновлення чинності сертифіката за заявою в усній формі

Заява на поновлення чинності в усній формі подається в черговому адміністратору реєстрації за телефоном.

Підписувач повинен повідомити відповідній посадовій особі ЦСК наступну інформацію:

- своє прізвище, ім'я та по батькові;
- ключову фразу-пароль.

Заява в усній формі приймається тільки при збігу даних Підписувача та парольної фрази, переданих в заяві, з інформацією, що знаходиться в реєстрі Підписувачів ЦСК.

Приймання і обробка усної заяви здійснюється цілодобово черговим адміністратором реєстрації або у робочий час відповідною особою ЦР чи ВПР. Обробка усної заяви на поновлення чинності сертифіката здійснюється безпосередньо після приймання заяви.

Черговий адміністратор реєстрації після перевірки повідомлених даних за допомогою ПТК формує запит на відновлення чинності сертифіката та передає його до ЦСК.

3.4.12. Поновлення чинності сертифіката за заявою в паперовій формі

Заява в паперовій формі подається в ЦР за відповідною формою (додаток № 2 до Реламенту).

Заява на поновлення чинності сертифіката засвідчується власноручним підписом власника сертифіката.

Подача заяви на поновлення чинності сертифіката в ЦР чи ВПР та її розгляд здійснюється тільки в робочий час, відповідно до розпорядку роботи ЦР чи ВПР.

Під час приймання заяви оператор реєстрації чи адміністратор реєстрації ЦСК проводить ідентифікацію Підписувача шляхом установлення особи за паспортом та звірення паспортних даних зі збереженими в реєстрі користувачів.

За умови позитивного результату ідентифікації оператор реєстрації передає заяву адміністратору реєстрації. Адміністратор реєстрації за допомогою ПЗ формує запит на поновлення чинності сертифікату з вказанням терміну поновлення та передає його до ЦСК.

Обробка заяви в паперовій формі на поновлення чинності сертифіката здійснюється на протязі не більш ніж двох годин з моменту подачі заяви.

Адміністратор реєстрації, як і оператор реєстрації, може проводити процедури з ідентифікації та реєстрації заяви.

3.4.13. Поновлення чинності сертифіката за зверненням керівництва установи до якої належить Підписувач

Поновлення чинності сертифіката здійснюється ЦСК на підставі звернення від керівнитва підрозділу, до якого належить Підписувач, з зазначенням обставин, які викликають необіхність поновлення сертиіфката, та долученням належним чином засвідчених копій відповідних документів.

Подача заяви чи звернення на поновлення чинності сертифіката в ЦР чи ВПР та її розгляд здійснюється тільки в робочий час, відповідно до розпорядку роботи ЦР чи ВПР.

Під час приймання заяви оператор реєстрації чи адміністратор реєстрації ЦСК проводить ідентифікацію Підписувача шляхом установлення особи за паспортом та звірення паспортних даних зі збереженими в реєстрі користувачів.

За умови позитивного результату ідентифікації оператор реєстрації передає заяву адміністратору реєстрації. Адміністратор реєстрації за допомогою ПТК формує запит на поновлення сертифікату та передає його до ЦСК.

Обробка заяви на поновлення чинності сертифіката про поновлення повинні здійснюватись протяом не більше ніж двох годин з моменту подачі заяви чи звернення.

Адміністратор реєстрації, як і оператор реєстрації, може проводити процедури з ідентифікації та реєстрації заяви чи звернення.

Часом поновлення чинності сертифіката вважається час виключення сертифіката Підписувача зі СВС.

3.5. Порядок надання Центром інформації про статус сертифіката

При використанні Підписувачем особистого ключа для формування ЕЦП, він повинен попередньо перевірити чинність відповідного даному ключу сертифіката. Те ж саме стосується й сертифікатів, які Підписувач або інший користувач використовує для перевірки ЕЦП та позначки часу.

Для перевірки статусу сертифікатів використовуються такі механізми:

- подання до ЦСК запитів та отримання відповідей за протоколом OCSP;
- перевірка наявності сертифіката у поточному списку відкликаних сертифікатів ЦСК.

3.5.1. Отримання статусу сертифікату за допомогою OCSP

Взаємодія з ЦСК за протоколом OCSP дозволяє отримувати інформацію про статус сертифіката в реальному часі. Обмін з Центром таким чином здійснюється ПЗ посадових осіб ЦСК або прикладним ПЗ, що надається Підписувачам, наприклад прикладним застосуванням «Персональний сервіс ЕЦП».

OCSP-сервер, який функціонує в складі ПТК ЦСК, має власний ключ ЕЦП та відповідний йому сертифікат, доступ до якого надається через web-сайт Центру.

Для перевірки відповідей OCSP-серверу, під час введення в дію сертифікату Підписувача, ПЗ записує до особистого контейнеру Підписувача ланцюжок сертифікатів, включаючи сертифікати ЦСК та OCSP-серверу. Крім того ПЗ може отримувати сертифікати з LDAP-каталогу ЦСК.

ПЗ Підписувача відправляє запит до OCSP-серверу автоматично кожний раз як проводиться автентифікація користувача, накладення чи перевірка ЕЦП.

Відповідь від OCSP-серверу приймається і обробляється прикладним ПЗ Підписувача автоматично. Вона містить інформацію про статус сертифікату, відносно якого проводився запит, чи є він діючим, блокованим чи скасованим. У залежності від статусу ПЗ дозволяє або забороняє вхід до системи та/або накладення ЕЦП, або повідомляє про результат перевірки ЕЦП.

3.5.2. Отримання статусу сертифіката за допомогою СВС

СВС утримують перелік сертифікатів, що мають статус блокованих та скасованих. СВС формуються Центром, засвідчуються ЕЦП ЦСК та публікуються в LDAP-каталозі та на Web-сайті ЦСК. Період публікації складає дві години.

Перевірка статусу сертифікату за допомогою СВС є альтернативою перевірці за протоколом OCSP.

Перевірка статусу за СВС виконується ПЗ посадових осіб та прикладним ПЗ Підписувачів.

При наявності підключення до Internet на робочому місці Підписувача ПЗ автоматично перевіряє актуальність СВС та у випадку необхідності завантажує оновлений з LDAP-каталогу чи Web-сайту ЦСК.

У випадку відсутності на робочому місці Підписувача підключення до Internet, відповідальність за наявність у файловому сховищі актуального СВС покладається на Підписувача, який використовує ключі ЕЦП.

Використання ЕЦП без перевірки статусу сертифікатів за актуальним СВС чи за OCSP забороняється.

СВС ЦСК оновлюється при кожному доданні або виключенні з нього інформації про зміну статусу сертифікату.

4. Порядок розповсюдження (публікації) інформації ЦСК

4.1. Інформаційний ресурс ЦСК

Інформаційний ресурс ЦСК призначений для розміщення на ньому відкритої інформації, яка структурно поділяється на:

- довідкову інформацію (розпорядок роботи ЦСК, положення Регламенту, нормативні документи, форми заяв тощо);
- сертифікат ЦСК;
- сертифікати серверів ЦСК;
- СВС та дельта-СВС (містять інформацію про статуси сертифікатів ЦСК та Підписувачів, що відкликані).

Електронна адреса (DNS-ім'я) електронного інформаційного ресурсу: https://ca.gp.gov.ua.

Технічною основою інформаційного ресурсу ЦСК є web-сервер, що входить до складу ПТК ЦСК.

Сертифікат ЦСК, сертифікати функціональних серверів ЦСК (OCSP, TSP), СВС та сертифікати розміщуються:

- у складі web-сторінок на web-сервері ЦСК;
- у інформаційному дереві LDAP-каталогу на LDAP-сервері.

Сертифікати Підписувачів розміщуються в LDAP-каталозі та доступні прикладному ПЗ після авторизації.

Доступ до web-серверу здійснюється за DNS-ім'ям https://ca.gp.gov.ua за протоколом HTTP(S) (номер TCP-порту 80, 443).

4.2. Порядок публікації сертифікатів

На інформаційному ресурсі ЦСК виконується публікація сертифікатів:

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

Після формування сертифікату ЦСК та серверів ЦСК, вони автоматично публікуються в LDAP-каталозі. Інформаційний ресурс отримує сертифікати з LDAP при кожному зверненні з відповідної web-сторінки.

Сертифікати Підписувачів, враховуючи їх відомчу приналежність, на інформаційному ресурсі ЦСК не публікуються. Вони доступні для Підписувачів через прикладне ПЗ відомчої інформаційної системи, яка отримує їх після автентифікації з LDAP-каталогу.

4.3. Порядок розповсюдження інформації про статус сертифікатів ключів

Для розповсюдження інформації про статус сертифікатів ключів підписувачів використовується механізм списку відкликаних сертифікатів та механізм визначення статусу сертифіката ключа в режимі реального часу за протоколом OCSP, згідно Вимог до протоколу визначення статусу сертифіката, затверджених наказом Міністерства юстиції України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.08.2012 року № 1236/5/453 «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису», зареєстрованим в Міністерстві юстиції України 20.08.2012 року за № 1398/21710».

ЦСК надає всім користувачам послугу інтерактивного визначення статусу сертифіката. Послуга надається шляхом відправлення запиту за протоколом HTTP на OCSP-сервер ЦСК.

4.4. Порядок публікації СВС

Публікація СВС Підписувачів у LDAP-каталозі здійснюється одразу після його випуску.

Інформаційний ресурс Центру сертифікації ключів отримує СВС із LDAP при кожному зверненні до відповідної web-сторінки.

СВС випускається кожні дві години та містить інформацію про всі відкликані (заблоковані, поновлені) сертифікати, які були сформовані на особистому ключі, що відповідає діючому сертифікату ЦСК.

4.5. Закінчення строку чинності сертифіката ключа підписувача

Строк дії особистого та відкритого ключа дорівнює строку чинності відповідного сертифіката ключа.

Після закінчення строку чинності сертифіката ключа він вилучається з інформаційного ресурсу ЦСК та переміщується до архіву.

ЦСК зберігає сертифікат та пов'язані з ним СВС безстроково. За запитом користувачів ЦСК надає доступ до необхідного сертифіката та пов'язаних з ним СВС з архівних записів ЦСК.

4.6. Порядок надання послуги фіксування часу

ЦСК надає всім користувачам послугу фіксування часу. Послуга надається шляхом відправлення запиту за протоколом HTTP на TSP-сервер ЦСК, згідно Вимог до протоколу фіксування часу, затверджених наказом Міністерства юстиції

України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.08.2012 року № 1236/5/453 «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису», зареєстрованим в Міністерстві юстиції України 20.08.2012 року за № 1398/21710». Послуга фіксування часу надається цілодобово.

5. Управління та операційний контроль

5.1. Фізичне середовище

Компоненти ПТК ЦСК розміщуються у наступних приміщеннях: спеціальному приміщенні (серверне приміщення захищеного (екранованого) основного ЦОД та захищеного (екранованого) резервного ЦОД), які у якому знаходяться шафи з обладнанням ЦСК, та робочих приміщеннях ЦСК.

Приміщення відповідають вимогам техніки безпеки та протипожежної безпеки, комплектуються необхідними засобами енергозабезпечення, охоронної та протипожежної сигналізації, відеоспостереження (за необхідності), допоміжними технічними засобами (механічний замок у робочому приміщенні ЦСК, механічний замок та електронний кодовий замок у спеціальному приміщенні ЦСК), системами життєзабезпечення (кондиціонерами).

Пропускний і внутрішній режими визначаються внутрішніми документами Генеральної прокуратури України і передбачають порядок допуску співробітників і представників інших організацій на територію ЦСК, порядок внесення і винесення матеріальних цінностей, а також виконання особами, що перебувають на території ЦСК, встановлених вимог режиму й розпорядку робочого дня.

Відповідальність за організацію охорони, стан перепускного й внутрішнього режиму ЦСК в цілому покладається на СЗІ.

Загальне керівництво й контроль за організацією охорони, станом перепускного й внутрішнього режиму здійснює начальник СЗІ ЦСК та відповідним підрозділом Міністерства внутрішніх справ з забезпечення охорони органів прокуратури.

Спеціальні приміщення ЦСК відповідають вимогам до спеціальних приміщень, які визначено у Правилах посиленої сертифікації, за виключенням вимог щодо захисту від витоку та деструктивного впливу зовнішніх електромагнітних полів, а ПТК, який використовується для обслуговування сертифікатів підписувачів, має експертний висновок в галузі КЗІ та відповідає вимогам нормативних документів в сфері ТЗІ стосовно створення КСЗІ.

У спеціальних приміщеннях ЦСК розміщені:

- основного і резервного захищеного (екранованого) ЦОД, які забезпечують виконання вимог Правил посиленої сертифікації щодо захисту від витоку та деструктивного впливу зовнішніх електромагнітних полів:
  - шафи, в яких розміщується обладнання ЦСК і;
- робоче місце адміністратора сертифікації;
- робоче місце адміністратора безпеки;
- робоче місце системного адміністратора.

Захищений (екранована) основний і резервний ЦОД мають механічний замок, ключ від якого є лише у системного адміністратора (дублікат ключа зберігається в сейфі начальника ЦСК), забезпечує можливість її опломбування, сигналізації та контролю доступа.

5.2. Механізми контролю доступу до спеціального приміщення

Допуск у спеціальне приміщення у режимі штатної роботи ЦСК мають:

- начальник ЦСК та його заступник;
- адміністратор безпеки;
- системний адміністратор;
- адміністратор сертифікації.

Якщо ЦСК знаходиться у режимі штатної роботи, допуск в спеціальне приміщення ЦСК дозволений тільки в супроводі адміністратора безпеки, начальника ЦСК або його заступника.

Допуск у спеціальне приміщення ЦСК інших осіб, окрім визначених вище, може здійснюватися коли виконуються усі наступні умови:

- відвідування здійснюється з письмового дозволу начальника ЦСК або його заступника;
- склад відвідувачів, час відвідування та план робіт, що будуть виконуватися у спеціальному приміщенні ЦСК відвідувачами задокументовані та узгоджені з адміністратором безпеки;
- протягом усього часу знаходження відвідувачів у спеціальному приміщенні ЦСК дії відвідувачів контролюються адміністратором безпеки;
- під час відвідування не здійснюється штатна робота ЦСК.

Факти допуску у спеціальне приміщення ЦСК інших осіб, окрім персоналу ЦСК, повинні бути запротокольовані (з зазначенням мети і часу відвідування, складу відвідувачів) та засвідчені підписом адміністратора безпеки або начальника ЦСК.

Двері спеціального приміщення ЦСК постійно замкнені на електронний кодовий замок і можуть відкриватися лише тільки для санкціонованого проходу персоналу, що має право допуску у нього. Кодова комбінація електронного замка спеціального приміщення ЦСК змінюється у разі підозри її розголошення негайно або періодично не рідше одного разу в квартал. Опечатаний начальником ЦСК непрозорий конверт із аркушем паперу, на якому записане значенням кодової комбінації електронного замка спеціального приміщення ЦСК, зберігаються у сейфі керівника ЦСК та/або його заступника.

6. Організаційна структура ЦСК

До складу ЦСК входять:

- керівник ЦСК;
- заступник керівника ЦСК – адміністратор сертифікації;
- адміністратор безпеки;
- адміністратор сертифікації;
- адміністратор реєстрації;
- системний адміністратор;
- оператор реєстрації.
- служба захисту інформації ЦСК;
- чергові адмінісратори реєстрації;
- відокремлені пункти реєстрації.

До складу ЦСК можуть входити й інші підрозділи, що забезпечують його роботу.

6.1.1. Керівник ЦСК

Функції та завдання керівника ЦСК:

- здійснює загальне керівництво діяльністю ЦСК, забезпечує ефективне використання і збереження майна ЦСК, організацію діловодства, виконання завдань, передбачених Регламентом ЦСК;
- розглядає документи, що надійшли до ЦСК, у межах компетенції підписує, затверджує та візує службову документацію;
- контролює роботу відокремлених пунктів реєстрації ЦСК (далі – ВПР ЦСК);
- визначає систему організаційних і технічних заходів збереження конфіденційної інформації ЦСК та Генеральної прокуратури України;
- подає звіти про роботу ЦСК до ЦЗО та Державної служби спеціального зв'язку та захисту інформації України (відповідно до вимог нормативної документації);
- вживає заходів щодо підвищення ефективності роботи посадових осіб ЦСК та ВПР ЦСК;
- організовує впровадження нових форм і методів управління ЦСК та ВПР ЦСК, створення організаційних і адміністративних умов для ефективної праці у ЦСК;
- організовує створення безпечних і сприятливих умов праці;
- відповідно до вимог цього Регламенту звертається до державних органів, підприємств, установ, організацій незалежно від форми власності та фізичних осіб, підписує від імені Генеральної прокуратури України,

направляє та отримує у встановленому порядку листи, заяви, скарги, запити, відповіді на них та інші документи, що стосуються діяльності ЦСК;
- у встановленому порядку забезпечує підготовку організаційно-розпорядчих документів з питань, що належать до компетенції ЦСК;
- у встановленому порядку ініціює питання про необхідність застосування до посадових осіб ЦСК заходів дисциплінарного впливу;
- за дорученням керівництва Генеральної прокуратури України представляє в органах державної влади, громадських, наукових, міжнародних та інших організаціях Генеральну прокуратуру України з питань діяльності ЦСК;
- вносить на розгляд керівництва Генеральної прокуратури України або керівникам самостійних структурних підрозділів питання, пов'язані з діяльністю ЦСК або його відокремлених пунктів;
- доводить до відома розробників програмно-технічного комплексу (ПТК) та постачальників іншого програмного та апаратного забезпечення, що застосовується в ЦСК, пропозиції та зауваження щодо роботи зазначених компонентів ЦСК;
- здійснює оперативне управління майном ЦСК.

6.1.2. Заступник керівника ЦСК – адміністратор сертифікації

- формує за допомогою особистого ключа ЦСК сертифікати підписувачів, та списківи відкликаних сертифікатів (далі – СВС) та позначок часу;
- формує електронні заяви на блокування, поновлення та скасування сертифікатів ключів у випадках, передбачених Регламентом;
- зберігає резервну копію особистого ключа ЦСК, резервні копії особистих ключів функціональних серверів;
- контролює своєчасність і коректність процесу формування СВС та розміщення їх на інформаційному ресурсі ЦСК;
- подає до ЦЗО дані, які необхідні для формування сертифіката та засвідчення відкритого ключа ЦСК;
- бере участь у резервному копіюванні особистого ключа ЦСК та особистих ключів функціональних серверів ЦСК, відновленні цих ключів, знищенні особистих ключів та їх резервних копій.

6.1.3. Адміністратор сертифікації

Функції та завдання адміністратора сертифікації:
- формує за допомогою особистого ключа ЦСК сертифікати підписувачів, та списківи відкликаних сертифікатів (далі – СВС) та позначок часу;
- формує електронні заяви на блокування, поновлення та скасування сертифікатів ключів у випадках, передбачених Регламентом;

- зберігає резервну копію особистого ключа ЦСК, резервні копії особистих ключів функціональних серверів;
- контролює своєчасність і коректність процесу формування СВС та розміщення їх на інформаційному ресурсі ЦСК;
- подає до ЦЗО дані, які необхідні для формування сертифіката та засвідчення відкритого ключа ЦСК;
- бере участь у резервному копіюванні особистого ключа ЦСК та особистих ключів функціональних серверів ЦСК, відновленні цих ключів, знищенні особистих ключів та їх резервних копій.

6.1.4. Адміністратор безпеки

Функції та завдання адміністратора безпеки:

- забезпечує повноту та якість виконання організаційно-технічних заходів із захисту інформації;
- забезпечує функціонування комплексної системи захисту інформації (далі – КСЗІ);
- розробляє проекти розпорядчих документів щодо забезпечення захисту інформації в ЦСК, здійснює контроль за їх виконанням;
- своєчасно реагує на спроби несанкціонованого доступу до ресурсів програмно-технічного комплексу ЦСК (далі – ПТК ЦСК), спроби порушення правил експлуатації засобів захисту інформації;
- бере участь у процедурах генерації особистого ключа ЦСК та особистих ключів функціональних серверів, резервного копіювання цих ключів та їх знищенні;
- бере участь у відновленні особистого ключа ЦСК та особистих ключів функціональних серверів;
- зберігає резервну копію особистого ключа ЦСК;
- здійснює контроль за зберіганням резервних копій особистих ключів функціональних серверів;
- здійснює генерацію, контроль за зберіганням та використанням особистих ключів посадових осіб ЦСК і їх своєчасним та надійним знищенням;
- засвідчує електронні запити на формування сертифікатів відкритих ключів посадових осіб ЦСК;
- формує електронні заяви на блокування, поновлення та скасування сертифікатів відкритих ключів посадових осіб ЦСК у випадках, передбачених Регламентом ЦСК;
- здійснює контроль за процесом резервування сертифікатів ключів та списків відкликаних сертифікатів, а також інших важливих ресурсів;

- передає резервну копію бази даних сертифікатів ключів та СВС на зберігання до відокремленого сховища;
- організовує розмежування доступу до ресурсів ПТК ЦСК, зокрема розподілення між посадовими особами паролів, ключів, сертифікатів тощо;
- забезпечує спостереження за функціонуванням КСЗІ (реєстрація та аудит подій у ПТК ЦСК, моніторинг подій тощо);
- забезпечує організацію та проведення заходів із модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов або аварій;
- організовує зберігання та обіг у межах ІТС ЦСК засобів криптографічного захисту інформації (далі – КЗІ);
- здійснює контроль за веденням журналів аудиту подій, що реєструються засобами ПТК ЦСК;
- здійснює контроль за зберіганням архівних і резервних копій реєстрів сертифікатів, журналів аудиту та конфігурацій програмного забезпечення та обладнання;
- здійснює контроль за прийманням та здаванням чергування системним адміністратором і черговими адміністраторами реєстрації;
- веде журнали, що стосуються заходів із забезпечення захисту інформації;
- у встановленому порядку бере участь у проведенні службового розслідування;
- контролює дотримання посадовими особами політики безпеки;
- готує пропозиції щодо забезпечення ПТК ІТС ЦСК (КСЗІ) необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою з метою підвищення рівня захисту інформації;
- узгоджує умови включення до складу ПТК ІТС ЦСК нових компонентів та подає керівництву пропозиції щодо заборони їхнього включення, якщо вони порушують прийняту політику безпеки або рівень захищеності ресурсів;
- надає пропозиції керівництву щодо покращення умов праці.

6.1.5. Системний адміністратор

Функції та завдання системного адміністратора:

- організовує експлуатацію та технічне обслуговування ІТС ЦСК;
- веде моніторинг функціонування ІТС ЦСК;
- відновлює ІТС ЦСК після збоїв та відмов;
- підтримує електронний інформаційний ресурс ЦСК;
- бере приймає участь у забезпеченні функціонування КСЗІ;
- формує та веде резервні копії конфігурацій (конфігураційних файлів) загальносистемного та спеціального програмного забезпечення ПТК ЦСК;

- здійснює контроль архівації та резервування бази даних сформованих сертифікатів та СВС;
- адмініструє антивірусне ПЗ, забезпечує актуальність антивірусних баз;
- здійснює технічну підтримку підписувачів ЦСК каналами зв'язку;
- веде формуляр ІТС ЦСК;
- веде журнали, що стосуються експлуатації ІТС ЦСК;
- контролює дотримання посадовими особами політики безпеки та технології обробки інформації;
- забезпечує безперебійне функціонування ІТС ЦСК та доступність для користувачів інформаційного ресурсу ЦСК, а також відповідає за збереження апаратури та майна ІТС ЦСК;
- отримує під час приймання чергування від чергового адміністратора реєстрації вичерпні відомості про стан процесу обробки інформації, апаратних та програмних засобів ІТС та КСЗІ;
- звітує адміністратору безпеки про стан процесу обробки інформації, апаратних та програмних засобів ІТС та КСЗІ;
- готує пропозиції щодо забезпечення ПТК ІТС ЦСК необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою з метою підвищення рівня захисту інформації;
- бере приймає участь в інвентаризації апаратури та майна ЦСК;
- доводить до відома розробників пропозиції та зауваження у роботі апаратних, програмних та апаратно-програмних засобів.

6.1.6. Адміністратор реєстрації

Функції та завдання адміністратора реєстрації:

- перевіряють дані, обов'язкові для формування сертифіката, а також дані, які вносяться у сертифікат на вимогу підписувача;
- формують електронні заяви на формування, скасування, блокування та поновлення сертифікатів ключів на підставі письмових заяв підписувачів;
- надають допомогу підписувачам під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення, а також вживають заходів щодо забезпечення безпеки інформації під час генерації ключової інформації;
- перевіряють законність звернень про блокування, поновлення та скасування сертифікатів за процедурою, визначеною Регламентом ЦСК;
- забезпечують документально підтверджену законність заяв на зміну статусу сертифіката підписувача, які були ним сформовані та засвідчені особистим ЕЦП;

- формують запити на формування стартових та робочих сертифікатів відкритих ключів підписувачів, засвідчують коректність включених у них даних шляхом накладення на запит власного ЕЦП;
- забезпечують відповідність даних, включених у запит на формування сертифіката, який підписаний його ЕЦП, даним, що подані заявником у письмовій заяві та визначених Регламентом ЦСК документах;
- видають сертифікати відкритих ключів підписувачів за допомогою ПТК;
- формують електронні заяви на блокування та скасування сертифікатів ключів у випадках, передбачених Регламентом ЦСК;
- надають підписувачам консультації щодо умов та порядку надання послуг ЕЦП;
- зберігають власні НКІ з особистим ключем;
- реєструють внесення змін у реєстр користувачів з дозволу керівника ЦСК або особи, що його заміщує;
- перевіряють повноту комплекту документів відповідно переліку, визначеного Регламентом ЦСК, та коректність засвідчення копій документів, якими підписувач підтверджує дані для внесення у сертифікат;
- передають особові справи підписувачів до архіву;
- вирішують спірні питання, що виникають під час роботи оператора реєстрації з підписувачами;
- перевіряють роботу операторів реєстрації та адміністраторів реєстрації ВПР;
- перевіряють повноту та правильність наданої заявниками інформації, за потреби вимагають від заявників надання додаткових документів;
- відмовляють заявнику в реєстрації та формуванні, скасуванні, блокуванні та відновленні сертифікатів ключів, якщо форма та зміст відповідної заяви не відповідають вимогам Регламенту ЦСК або якщо ці заяви подає не уповноважена на це особа;
- відмовляють підписувачу в прийомі заяви на блокування сертифіката за телефоном, якщо деякі з названих даних не співпадають з тими, що містяться в реєстрі користувачів

6.1.7. Оператор реєстрації

Функції та завдання чергового адміністратора реєстрації:

- встановлює осіб, які звернулися до ЦСК із метою формування сертифіката;
- перевіряє дані, обов'язкові для формування сертифіката, а також дані, які вносяться у сертифікат на вимогу підписувача;
- перевіряє документи, надані заявниками для ідентифікації їх особи;
- перевіряє повноту комплекту документів відповідно переліку, визначеного Регламентом ЦСК, відповідність їх оформлення вимогам Регламенту ЦСК, а

також коректність засвідчення копій документів, якими заявник підтверджує дані для внесення в сертифікат;

- вимагає від заявників додаткову інформацію в документальній формі, якщо така інформація необхідна для їх реєстрації;
- заповнює електронні форми з даними підписувача, перевіряє точність занесення даних, формує особову справу підписувача;
- формує запити на формування стартових та робочих сертифікатів відкритих ключів підписувачів, засвідчує коректність включених у них даних шляхом накладення на запит власного ЕЦП;
- отримує від підписувачів письмові заяви на формування, скасування, блокування та поновлення сертифікатів ключів;
- перевіряє законність звернень про блокування, поновлення та скасування сертифікатів;
- формує електронні заяви на блокування, поновлення та скасування сертифікатів ключів у випадках, передбачених Регламентом ЦСК;
- надає допомогу підписувачам під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення та вживає заходів щодо забезпечення безпеки інформації під час генерації ключової інформації;
- фотографує заявника (у разі необхідності);
- надає підписувачам консультації щодо умов та порядку надання послуг ЕЦП;
- доводить до відома адміністратора реєстрації інформацію про всі спірні питання, які виникли при реєстрації заявників.

6.1.8. Чергові адміністратори реєстрації ЦСК

- забезпечують чергування у встановленому порядку;
- забезпечують безперебійне приймання звернень підписувачів ЦСК, автентифікацію підписувача, що звертається за блокуванням сертифіката (за процедурою, визначеною Регламентом ЦСК);
- формують електронні заяви на блокування сертифікатів ключів на підставі усних заяв підписувачів, отриманих по телефону;
- перевіряють законність звернень про блокування за процедурою, визначеною Регламентом ЦСК;
- відмовляють підписувачу в прийомі заяви на блокування сертифіката телефоном, якщо деякі з названих даних не співпадають з тими, що є в реєстрі користувачів;
- забезпечують коректне та своєчасне формування запиту на блокування сертифікату підписувача, який звернувся з цією вимогою до ЦСК;

- надають підписувачам консультації щодо умов та порядку надання послуг ЕЦП, а також технічну підтримку підписувачів ЦСК каналами зв'язку;
- забезпечують зберігання носія з особистим ключем, запобігання доступу до нього інших осіб;
- доводять до керівника ЦСК або особи що, його заміщує, про всі факти блокування сертифікатів, що сталися протягом його чергування або за вихідні дні (з часу останньої денної зміни);
- ведуть постійний моніторинг функціонування ІТС ЦСК;
- відновлюють ІТС ЦСК після збоїв та відмов;
- підтримують електронний інформаційний ресурс ЦСК;
- забезпечують безперебійне функціонування ІТС ЦСК та доступність для користувачів інформаційного ресурсу ЦСК, а також відповідають за збереження апаратури та майна ЦСК під час їх чергування;
- ведуть журнали, що стосуються експлуатації ІТС ЦСК;
- звітують адміністратору безпеки про стан процесу обробки інформації, апаратних та програмних засобів ІТС та КСЗІ;
- доводять до відома системного адміністратора ЦСК пропозиції та зауваження щодо роботи апаратних, програмних та апаратно-програмних засобів;
- готують пропозиції щодо забезпечення ПТК ІТС ЦСК необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою з метою підвищення рівня захисту інформації;
- отримують під час приймання чергування від системного адміністратора ЦСК чи іншого чергового адміністратора реєстрації ЦСК вичерпні відомості про стан процесу обробки інформації, апаратних та програмних засобів ІТС та КСЗІ

6.1.9. Посадові особи ЦСК (керівник, заступник керівника – адміністратор сертифікації, адміністратор безпеки, адміністратори реєстрації, системний адміністратор, оператор реєстрації, чергові адміністратори реєстрації)

- зберігають конфіденційні відомості ЦСК та Генеральної прокуратури України;
- негайно доповідають про факти спроб несанкціонованого доступу до інформації, що обробляється в ІТС ЦСК;
- дотримуються правил безпеки під час експлуатації персональних робочих станцій та електрообладнання

6.1.10. Служба захисту інформації

До складу служби захисту інформації входять:

- начальник служби захисту інформації;
- адміністратор безпеки;
- системний адміністратор.

Функції та завдання служби захисту інформації:

- 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 ПТК ЦСК, порушення правил експлуатації засобів захисту інформації;
- контроль за зберіганням особистого ключа ЦСК та його резервної копії, особистих ключів посадових осіб ЦСК;
- участь у знищенні особистого ключа ЦСК, контроль за правильним і своєчасним знищенням посадовими особами особистих ключів;
- ведення контролю за процесом резервування реєстру сертифікатів ключів та списків відкликаних сертифікатів, а також інших важливих ресурсів;
- організація розмежування доступу до ресурсів програмно-технічного комплексу ЦСК, зокрема розподілення між посадовими особами паролів, ключів, сертифікатів тощо;
- забезпечення спостереження (реєстрація та аудит подій в програмно-технічному комплексі ЦСК, моніторинг подій тощо) за функціонуванням комплексної системи захисту інформації;
- забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов та аварій ПТК.

6.1.11. Відокремлені пункти реєстрації

Відокремлені пункти реєстрації створюються при необхідності провадження сервісу ЦСК у територіально відокремлених районах.

До складу ВПР входять:

- віддалений адміністратор реєстрації;
- оператори реєстрації.

Керівництво ВПР здійснює віддалений адміністратор реєстрації.

ВПР підпорядковується керівнику ЦСК.

Функції та завдання ВПР:

- встановлення осіб, які звернулися до ЦСК з метою формування сертифіката;
- перевірка даних, обов'язкових для формування сертифіката, а також даних, які вносяться у сертифікат на вимогу Підписувача;

- проведення реєстрації Підписувачів;
- отримання від Підписувачів заявок на формування, скасування, блокування та поновлення сертифікатів ключів;
- надання допомоги Підписувачам під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення та вживання заходів щодо забезпечення безпеки інформації під час генерації;
- перевірка законності звернень про блокування, поновлення та скасування сертифікатів;
- надання Підписувачам консультацій щодо умов та порядку надання послуг електронного цифрового підпису.

7. Опис процедур та механізмів, пов'язаних з функціонуванням ЦСК

7.1. Управління ключами ЦСК

7.1.1. Порядок генерації особистого ключа ЦСК

Генерація особистого ключа ЦСК виконується на Сервері застосувань ЦСК (основному) всередині екранованого серверного приміщення ЦСК не менш, ніж трьома посадовими особами за допомогою надійних засобів ЕЦП. Обов'язково приймають участь у генерації керівник ЦСК та адміністратор безпеки. Крім них здійснювати генерацію можуть адміністратор сертифікації та системний адміністратор.

Після генерації особистого ключа ЦСК виконується генерація особистих ключів посадових осіб ЦСК, що приймають участь у генерації особистого ключа ЦСК.

Перед виконанням генерації посадова особа підключає особистий НКІ. Під час генерації особистого ключа відповідної посадової особи вона вводить свої ідентифікаційні дані та дані, що заносяться до сертифікату, у програмну форму на сервері застосувань ЦСК. Контроль за коректністю вводу здійснює адміністратор безпеки. Контроль за вводом даних адміністратора безпеки здійснює керівник ЦСК. Після вводу даних програмний комплекс вимог ввести пароль доступу до файлового контейнеру, в якому зберігається особистий ключ. Введення паролю необхідно проводити так, щоб жодна інша особа не могла побачити який пароль було введено.

Після генерації особистий ключ зберігається в файловому контейнері на особистому НКІ.

Після генерації особистих ключів всім посадовим особам, які проводять генерацію, програмний комплекс автоматично генерує ключ шифрування файлового контейнеру для захисту особистого ключа ЦСК.

Особистий ключ ЦСК шифрується за допомогою згенерованого ключа захисту та поміщується в файловий контейнер. Файловий контейнер записується на файлову систему Серверу застосувань ЦСК.

Ключ захисту особистого ключа ЦСК в свою чергу шифрується за допомогою ключа, що створюється поєднанням двох ключів симетричного алгоритму шифрування, що належать до кожної посадової особи та зберігаються в файловому контейнері. Для всіх варіантів поєднань пар особистих ключів шифрування посадових осіб, які проводили генерацію, проводиться шифрування ключа захисту. Всі варіанти зашифрованого ключа захисту записуються у файл-список доступу, що зберігається на файлову систему Серверу застосувань.

Для використання особистого ключа ЦСК необхідно одночасне використання будь-яких двох з особистих ключів посадових осіб, сумісне використання яких дозволяє розшифрування ключа захисту особистого ключа ЦСК. Тобто використання особистого ключа ЦСК можливе тільки при участі двох осіб з числа тих, які проводили його генерацію.

7.1.2. Порядок резервного копіювання особистого ключа ЦСК

Після генерації всіх ключів проводиться резервне копіювання особистого ключа ЦСК. Створюється не менше двох копій особистого ключа ЦСК на зовнішніх НКІ.

НКІ перед створенням резервних копій реєструється адміністратором безпеки в «Журналі обліку засобів КЗІ» для активних НКІ або в «Журналі обліку носіїв конфіденційної інформації» для НКІ.

Копіювання здійснюється засобами операційної системи адміністратором безпеки в присутності адміністратора сертифікації та/або керівника ЦСК. На кожен НКІ копіюється файловий контейнер з особистим ключем ЦСК та файл-список доступу.

Кожен НКІ з копією особистого ключа ЦСК поміщується в конверт, який запечатується та підписується адміністратором безпеки та адміністратором сертифікації.

Одна копія ключа ЦСК зберігається в сейфі адміністратора безпеки, інша(і) – в сейфі адміністратора сертифікації.

Адміністратор безпеки реєструє факти генерації, резервного копіювання, відновлення та знищення особистого ключа ЦСК та посадових осіб ЦСК в «Журналі реєстрації генерацій, резервного копіювання, відновлення та знищення ключових даних» з розписом всіх осіб, які приймали участь в даній операції.

7.1.3. Порядок формування запиту на сертифікат ЦСК

Термін дії особистого ключа ЦСК становить не більше 5 (п'яти) років. Початком строку дії особистого ключа ЦСК вважається дата його генерації.

Після генерації особистого ключа ЦСК здійснюється формування самопідписаного запиту на формування сертифіката ЦСК, який є запитом на формування сертифіката у Центральному засвідчувальному органі.

Формування запиту виконується на сервері застосувань ЦСК, на якому проводилась генерація.

В процесі формування запиту, інформація, що вноситься в сертифікат ЦСК вводиться з консолі серверу адміністратором сертифікації, при цьому адміністратор безпеки контролює відсутність помилок.

Запит записується на сервері застосувань на CD-носій та передається керівником ЦСК до Центрального засвідчу вального органу.

7.1.4. Порядок використання (введення) особистого ключа ЦСК

Введення особистого ключа ЦСК виконується на сервері застосувань ЦСК (основному та резервному), розташованих в серверному приміщенні.

Файловий контейнер копіюється з НКІ на файлову систему серверу, в каталог, що обрано в конфігурації серверу.

Для запуску серверу необхідно підключення НКІ з особистими ключами ЕЦП двох з посадових осіб, які виконували генерацію особистого ключа НКІ. Після успішної автентифікації на сервері цих осіб за допомогою їх власних ключів шифрування проводиться розшифрування файлового контейнеру з особистим ключем ЦСК. Ключ завантажується в пам'ять серверу і може бути використаний за призначенням.

7.1.5. Порядок планової зміни ключів ЦСК

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

Процедура планової зміни ключів ЦСК здійснюється в наступному порядку:

1. Програмний комплекс резервного серверу застосувань зупиняється та сервер відключається від ПТК ЦСК.

2. Старий особистий ключ ЦСК на резервному сервері застосувань знищується надійним чином.

3. На резервному сервері застосувань проводиться генерація нового ключа ЦСК визначеними особами.

4. Керівник ЦСК ініціює процес засвідчення чинності відкритого ключа ЦСК в ЦЗО шляхом передачі запиту на формування сертифікату.

5. Після отримання засвідченого сертифікату від Центрального засвідчувального органу новий сертифікат ЦСК публікується на інформаційному ресурсі ЦСК.

6. Старий особистий ключ, що зберігається в основному сервері застосувань, знищується надійним чином.

7. Проводиться запуск основного серверу застосувань ЦСК з новим особистим ключем ЦСК

8. Резервний сервер підключається до ПТК ЦСК, запускається в штатний режим роботи з новим особистим ключем ЦСК.

9. Проводиться знищення надійним чином всіх резервних копій старого особистого ключа ЦСК.

10. Сертифікати серверів ЦСК (OCSP, TSP), що були засвідчені старим особистим ключем ЦСК скасовуються.

11. Сертифікати Підписувачів, що були засвідчені старим особистим ключем ЦСК скасовуються.

12. Проводиться знищення надійним чином резервних копій ключів серверів ЦСК, що відповідають скасованим сертифікатам.

Після публікації нового сертифіката ЦСК у LDAP-каталозі та на інформаційному ресурсі ЦСК, сертифікат, відповідний старому ключу ЦСК, скасовується та вноситься у список відкликаних сертифікатів.

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

7.1.6. Порядок позапланової зміни ключів ЦСК

У випадку компрометації особистого ключа ЦСК виконується позапланова зміна ключів.

Сертифікат ЦСК негайно скасовується шляхом подання керівником ЦСК письмової заяви до ЦЗО.

Сертифікати серверів ЦСК та Підписувачів ЦСК, що були засвідчені скомпрометованим ключем скасовуються.

Надання послуг ЦСК Підписувачам припиняється до моменту формування ЦЗО нового сертифікату ЦСК.

Подальші дії відповідають порядку планової зміни ключів.
Список відкликаних сертифікатів підписується новим особистим ключем ЦСК.

ЦСК офіційно оповіщає Підписувачів про факт позапланової зміни ключів ЦСК.

Після одержання офіційного повідомлення про факт позапланової зміни ключів ЦСК Підписувачам необхідно виконати процедуру одержання нових ключів і сертифікатів відповідно до цього Регламенту.

7.1.7. Порядок ведення журналів аудиту

Всі події що виникають у ПТК ЦСК (генерація ключів, обробка запитів на створення, блокування скасування, поновлення, формування сертифікатів,

формування СВС, та інші події) записуються до журналів аудиту. Всі складові частини ПТК ЦСК (програмні комплекси серверів ЦСК, АРМів посадових осіб, операційні системи серверів) ведуть власні журнали аудиту. Журнали аудиту зберігаються на файловій системі відповідного серверу чи робочої станції.

Журнали аудиту мають право переглядати керівник ЦСК, адміністратор безпеки, та системний адміністратор. Періодичність перегляду журналів відповідними посадовими особами визначається їх посадовими інструкціями.

Доступ до перегляду журналів аудиту забезпечується штатними засобами розподілу доступу ОС та спеціальним прикладним ПЗ.

7.1.8. Порядок архівного зберігання документованої інформації

Архівному зберіганню в ЦСК підлягають наступні дані та документи:

- надані Підписувачами документи (копії документів), що використовуються під час реєстрації;
- заяви на формування сертифікатів Підписувачів;
- заяви на скасування сертифікатів Підписувачів;
- заяви на блокування сертифікатів Підписувачів;
- заяви на поновлення сертифікатів Підписувачів;
- сертифікати ЦСК;
- сертифікати серверів ЦСК;
- сертифікати посадових осіб ЦСК;
- сертифікати Підписувачів;
- службові документи ЦСК, у тому числі журнали аудиту програмно-технічного комплексу тощо;
- дані про надані послуги фіксування часу та електронні позначки часу передані користувачам.

Документи на паперових носіях, зберігаються в порядку, встановленому відомчими правилами ведення діловодства.

Сертифікати ЦСК, серверів ЦСК, Підписувачів та списки відкликаних сертифікатів зберігаються постійно.

Архівні копії журналів аудиту зберігаються не менше, ніж два роки.

Для перевірки електронних документів, підписаних особистими ключами Підписувачів, що не є чинними, ЦСК надає можливість доступу до відповідних сертифікатів відкритих ключів через власний інформаційний ресурс. Додатково забезпечується можливість перевірки статусу сертифікату на момент накладання ЕЦП.

Знищення архівних документів здійснюється комісією, сформованою із посадових осіб ЦСК при безпосередній участі керівника ЦСК та адміністратора безпеки.

Засоби СУБД, що входять до складу сервера ЦСК виконують автоматичне резервне копіювання БД. Автоматичне резервне копіювання засобами СУБД виконується на накопичувач на жорстких магнітних дисках. Між основним та резервним серверами ЦСК виконується автоматична реплікація БД.

Резервне копіювання даних в ЦСК а також зберігання копій здійснюється у відповідності до Регламенту резервного копіювання даних ЦСК.

Резервна копія бази сертифікатів та списків відкликаних сертифікатів на носії запечатується в конверт, що опечатується керівником ЦСК та передається на зберігання до сейфу сховища ДСК-діловодства.

Факт передачі резервної копії на зберігання реєструється у «Журналі реєстрації резервного копіювання БД та журналів аудита», зокрема її номер, дата та час передачі.

Відповідальність за контроль автоматичного резервного копіювання та виконання резервного копіювання журналу моніторингу ПТК ЦСК покладається на системного адміністратора. Адміністратор безпеки періодично контролює процес створення та зберігання резервних копій.

7.1.9. Порядок синхронізації часу у ПТК ЦСК

Для синхронізації системних годинників технічних засобів, що входять до складу ПТК ЦСК застосовується централізований сервер точного часу ЦСК, який постійно отримує точний час за протоколом NTP з серверів точного часу ЦЗО.

На всіх робочих станціях та серверах що входять до складу ПТК ЦСК встановлюється клієнт синхронізації часу. Клієнт синхронізації часу за заданим інтервалом здійснює зчитування значення часу з сервера синхронізації та у відповідності до цього значення встановлює системний годинник.

7.2. Забезпечення захисту особистого ключа ЦСК

7.2.1. Порядок захисту та доступу до особистого ключа ЦСК

Шифрування даних підпису власного особистого ключа ЦСК виконується за допомогою спеціального секретного ключа шифрування даних, який розподіляється між трьома і більше відповідальними особами ЦСК. Порядок розподілу цього ключа забезпечує:

- жодна відповідальна особа одноосібно не може забезпечити розшифровування особистого ключа ЦСК;

- особистий ключ ЦСК може бути розшифрований тільки за умови пред'явлення будь-якими двома відповідальними особами частин спеціального секретного ключа, що належать їм.

Особистий ключ ЦСК застосовується лише у захищеній (екранованій) шафі в спеціальному приміщенні ЦСК.

Зберігання особистих ключів відповідальних осіб ЦСК і підписувачів виконується виключно на носіях, що належать їм. Будь-які інші варіанти збереження вказаних особистих ключів виключені.

7.2.2. Порядок резервного копіювання особистого ключа ЦСК, порядок доступу та використання резервної копії особистого ключа ЦСК

Резервування виконується тільки під час генерування ключів ЦСК на знімний носій інформації.

Резервна копія особистого ключа ЦСК може бути застосована лише з дозволу начальника ЦСК за умов, коли особистий ключ ЦСК було знищено з причин, не пов'язаних з його компрометацією.

Застосування резервної копії особистого ключа ЦСК здійснюється у такому ж порядку, як і використання особистого ключа ЦСК. Про факти використання резервної копії особистого ключа ЦСК повинен бути поінформований адміністратор безпеки.

Адміністратор сертифікації ЦСК повинен зберігати основні та частину резервних НКІ з ключами ЦСК у сейфі на своєму основному робочому місці, іншу частину резервних НКІ з ключами ЦСК – на резервному робочому місці. Він несе особисту відповідальність за надійне зберігання цих НКІ та нерозголошення значень паролів доступу і розблокування.

7.2.3. Умови зберігання ключів ЦСК

Особистий ключ розміщується у зашифрованому вигляді в базі даних ПТК ЦСК на сервері застосувань ЦСК або на захищеному зйомному носії ключової інформації та постійно знаходиться у захищеній (екранованій) шафі, яка відповідає вимогам Правил посиленої сертифікації.

Особистий ключ послуг фіксування часу постійно знаходиться у робочому стані на сервері ЦСК. Системний адміністратор несе відповідальність за недопущення компрометації особистого ключа послуг фіксування часу, його несанкціонованого використання або модифікації.

Відповідальні особи ЦСК повинні зберігати НКІ зі своїми особистими ключами у неробочий час і в робочий час, якщо вони не використовуються в роботі, у спосіб,

який виключає можливість несанкціонованого доступу до НКІ, і несуть особисту відповідальність за надійне зберігання НКІ та нерозголошення паролів доступу і розблокування. Відповідальні особи ЦСК повинні зберігати основний пристрій НКІ на своєму основному робочому місці, а резервний пристрій НКІ – на резервному робочому місці.

Перелік змін до Регламенту

Додаток №1 до Регламенту роботи
Центру сертифікації ключів
Генеральної прокуратури України

РЕЄСТРАЦІЙНА КАРТКА

Заповнюється українською мовою та приймається до розгляду,
якщо немає виправлень, дописок чи необумовлених зауважень (заповнення олівцем не допускається)

Заява на проведення реєстрації			
Дані підписувача для формування посиленого сертифікатів відкритих ключів:			
Прізвище:			
Ім'я:			
По батькові:			
Найменування підрозділу:			
*Посада:**			
*Роль в ЄРДР:***			
Реєстраційний номер облікової картки платника податків:		*серія та номер паспорту або номер паспорту (ID-картки):*	
Засоби зв'язку (заповнюються обов'язково)			
Телефон службовий		*Мобільний (+380)*	
Фраза для блокування сертифікату:			
Фраза для розблокування сертифікату:			
*Згода підписувача на оброблення персональних даних ****		***ТАК*** ☐	***НІ*** ☐

** – вказується посада (індекс підрозділу), відповідно до наказу про призначення .*

*** - відповідно до ст. 3 КПК України.*

**** – підписувач надає ЦСК ГПУ згоду на оброблення (збирання, накопичення, зберігання) своїх персональних даних, зазначених у цій заяві, та інших документах (заявах), які передбачені Регламентом ЦСК ГПУ, та необхідні для реєстрації його як підписувача і формування посиленого сертифіката ключа.*

Підписавши цю заяву користувач засвідчує повне розуміння Регламенту ЦСК ГПУ, значень термінів і всіх умов. Підписавши цю Реєстраційну картку, Ви підтверджуєте достовірність та правильність зазначеної в ній інформації, погоджуєтесь на формування посиленого сертифіката ключа за вказаними даними та зобов'язуєтесь негайно повідомляти про зміну даних, зазначених у цій Реєстраційній картці.

Дата	***Підпис***	***Прізвище, ініціали***
«____» _____ 20___ р.	_____	_____

Обліковий номер Реєстраційної картки	

Адміністратор реєстрації _____ / _____ / _____

дата *підпис* *ПІБ*

Додаток №2 до Регламенту роботи
Центру сертифікації ключів
Генеральної прокуратури України

ЗАЯВА
(про зміну статусу посиленого сертифіката відкритого ключа)

Заповнюється українською мовою та приймається до розгляду,
якщо немає виправлень, дописок чи необумовлених зауважень (заповнення олівцем не допускається)

Дані підписувача, які були зазначені при реєстрації сертифіката:			
Прізвище:			
Ім'я:			
По батькові:			
Реєстраційний номер облікової картки платника податків:		*серія та номер паспорту або номер паспорту (ID-картки):*	

Зміна статусу посиленого сертифіката (оберіть один із варіантів)

Скасувати		**Заблокувати**		**Поновити**	

Причина скасування посиленого сертифіката *(заповнюється обов'язково у разі необхідності скасування посиленого сертифіката)*

Підписавши цю Заяву, Ви підтверджуєте достовірність та правильність зазначеної вище інформації.

Дата	***Підпис***	***Прізвище, ініціали***
«____» _____ 20____ р.	_____	_____

Адміністратор реєстрації _____ / _____ / _____
дата *підпис* *ПІБ*