ПОГОДЖЕНО

Голова Держспецзв'язку

_____ Л.О. Євдоченко

«7» липня 2015 року

ЗАТВЕРДЖЕНО

Наказ Державного підприємства
«Український інститут
інтелектуальної власності»
від «23» липня 2015 р. № 149

В.о. генерального директора

_____ Н.А. Полонська

Прим. № 3

АКРЕДИТОВАНИЙ ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ Державного підприємства "Український інститут інтелектуальної власності"

РЕГЛАМЕНТ РОБОТИ

(нова редакція)

Київ-2015

ЗМІСТ

С.

ВСТУП

Цей документ є внутрішнім нормативним документом, що визначає організаційно-методологічні та технологічні умови діяльності Акредитованого центру сертифікації ключів Державного підприємства "Український інститут інтелектуальної власності" (далі – АЦСК) під час надання послуг електронного цифрового підпису та є регламентом роботи АЦСК (далі – Регламент).

АЦСК Державного підприємства "Український інститут інтелектуальної власності" здійснює свою діяльність на підставі акредитації та засвідчення чинності свого відкритого ключа у центральному засвідчувальному органі.

Цей Регламент розроблено відповідно до вимог Правил посиленої сертифікації (далі – Правила посиленої сертифікації), затверджених наказом ДСТСЗІ СБ України від 13.01.2005 № 3 (у редакції наказу ДСТСЗІ СБ України від 10.05.2006 № 50).

1 СФЕРА ЗАСТОСУВАННЯ

1.1 Цей Регламент визначає організаційно-методологічні та технологічні умови діяльності Державного підприємства "Український інститут інтелектуальної власності" під час надання послуг електронного цифрового підпису (далі – ЕЦП).

1.2 Цей Регламент призначений для застосування суб'єктами, визначеними розділом 6 цього документу.

1.3 Вимоги даного Регламенту є обов'язковими для виконання всіма суб'єктами, які в ньому визначені, а також служать засобом офіційного повідомлення і інформування усіх суб'єктів у взаєминах, що виникають в процесі надання і використання послуг електронного цифрового підпису, що надаються АЦСК.

1.4 Будь-яка заінтересована особа може ознайомитися з положеннями Регламенту на електронному інформаційному ресурсі, в приміщеннях АЦСК та його відокремлених пунктах реєстрації.

1.5 Застосування положень Регламенту засноване на його добровільному визнанні взаємодіючими сторонами. Добровільне визнання цього Регламенту іншою стороною є підставою для укладення договору (угоди) про надання послуг і надання відповідних послуг.

2 НОРМАТИВНІ ПОСИЛАННЯ

У цьому документі є посилання на такі нормативно-правові документи:

- Закон України "Про електронний цифровий підпис";
- Закон України "Про електронні документи та електронний документообіг";
- Правила посиленої сертифікації, затверджені наказом ДСТСЗІ СБ України від 13.01.2005 № 3 (у редакції наказу ДСТСЗІ СБ України від 10.05.2006 № 50) (далі – Правила посиленої сертифікації);
- Положення про центральний засвідчувальний орган, затверджене постановою Кабінету Міністрів України від 28.10.2004 № 1451.
- Порядок засвідчення наявності електронного документа (електронних даних) на певний момент часу, затверджений постановою Кабінету Міністрів України від 24.05.2004 № 680.
- Порядок акредитації центру сертифікації ключів, затверджений постановою Кабінету Міністрів України від 13.07.2004 № 903.

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У цьому Регламенті використано терміни, встановлені в Законі України "Про електронний цифровий підпис" та Правилах посиленої сертифікації.

Нижче подано терміни, додатково використані у цьому Регламенті та визначення позначених ними понять:

3.1 відокремлений пункт реєстрації

Відособлений підрозділ АЦСК, який здійснює реєстрацію підписувачів.

3.2 заявник

Юридична (фізична особа – підприємець) або фізична особа, яка звернулась до АЦСК з метою отримання послуг ЕЦП.

3.3 підписувач (власник особистого ключа)

Особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, використовує цей особистий ключ за його призначенням, визначеним у сертифікаті відповідного відкритого ключа (накладає електронний цифровий підпис під час створення електронного документа / використовує особистий ключ у алгоритмі узгодження ключів при роботі з криптографічними повідомленнями). У разі, якщо в основних даних (реквізитах) підписувача, сформованих за зверненням заявника сертифіката, зазначаються реквізити заявника, заявник та підписувач є одним суб’єктом.

3.4 користувач

Особа, яка перевіряє електронний цифровий підпис, що накладений підписувачем на електронний документ, та яка під час перевірки покладається на належність і чинність сертифікату підписувача та дійсність інформації, зазначеної у цьому сертифікаті.

3.5 представник

Особа, уповноважена заявником на здійснення усіх дій щодо подання документів для формування та отримання сертифіката відкритого ключа для підписувача.

3.6 електронна печатка

Електронний цифровий підпис, спеціально призначений у випадках, коли згідно з законодавством необхідне засвідчення печаткою справжності підпису на документах та відповідності копій документів оригіналам.

4 ПОЗНАЧКИ ТА СКОРОЧЕННЯ

ВПР - відокремлений пункт реєстрації;
ЕЦП - електронний цифровий підпис;
НКІ - носій ключової інформації;
ПДВ - податок на додану вартість;
ПЗ - програмне забезпечення;
ПТК - програмно-технічний комплекс;
СЗІ - служба захисту інформації;
ЦЗО - центральний засвідчувальний орган;
АЦСК - акредитований центр сертифікації ключів Державного підприємства "Український інститут інтелектуальної власності";
CRL - список відкликаних сертифікатів;
TSP - Time Stamp Protocol;
OCSP - Online Certificate Status Protocol;
URL - unique resource locator (унікальна адреса інформаційного ресурсу в телекомунікаційній мережі).

5 ЗАГАЛЬНІ ПОЛОЖЕННЯ

5.1 Ідентифікаційні дані АЦСК

Країна	Україна
Назва міста	Київ
Повне найменування організації	Державне підприємство «Український інститут інтелектуальної власності»
Місцезнаходження АЦСК	01601, м. Київ-42, вул. Глазунова, 1
ЄДРПОУ	31032378
Підрозділ організації	Відділ інформаційної та внутрішньої безпеки
Повне найменування АЦСК	АЦСК Державного підприємства «Український інститут інтелектуальної власності»
Номери телефонів	+38 (044) 498-38-75, 494-06-20
Електронна пошта	info.acsk@ukrpatent.org
Електронна адреса	http://www.ukrpatent.org

5.2 Порядок публікації

Положення цього Регламенту розповсюджується:

- у електронній формі:
  - з веб-сайту АЦСК за адресою http://www.ukrpatent.org;
  - засобами електронної пошти від уповноваженої особи АЦСК;
- у паперовій формі:
  - через поштову адресу: 01601, м. Київ-42, вул. Глазунова, 1.

5.3 Порядок внесення змін та доповнень

Внесення змін та доповнень до цього Регламенту здійснюється АЦСК у відповідності до чинного законодавства України.

Про внесення змін та доповнень до цього Регламенту АЦСК повідомляє підписувачів та інших зацікавлених осіб офіційним повідомленням. Офіційне повідомлення здійснюється у спосіб, визначений у п. 5.2 "Порядок публікації".

Всі зміни та доповнення, внесені до цього 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 АЦСК.

Всі зміни та доповнення, внесені до цього Регламенту у зв'язку зі зміною чинного законодавства України, набувають чинності одночасно зі вступом в силу відповідних нормативно-правових актів.

Договори та інші правочини, умови яких суперечать змінам чи доповненням до цього документу, повинні бути переукладені протягом 10 (десяти) робочих днів з дня набрання чинності таких змін.

6 ПЕРЕЛІК СУБ'ЄКТІВ, ЗАДІЯНИХ В ОБСЛУГОВУВАННІ І ВИКОРИСТАННІ СЕРТИФІКАТІВ ВІДКРИТИХ КЛЮЧІВ, ТА ЇХ ФУНКЦІЇ

Суб'єктами правових відносин у сфері ЕЦП, що задіяні в обслуговуванні та використанні сертифікатів, є АЦСК, відокремлені пункти реєстрації АЦСК (далі – ВПР), заявники, підписувачі (власники особистих ключів та сертифікатів) та користувачі.

6.1 Функції, права та обов'язки АЦСК

6.1.1 АЦСК відповідно до покладених на нього завдань:

- формує, видає та обслуговує посилені сертифікати відкритих ключів (далі – сертифікати відкритих ключів, сертифікати ключів);
- приймає заяви про скасування, блокування та поновлення сертифікатів відкритих ключів;
- блокує, скасовує та поновлює сертифікати відкритих ключів підписувачів у випадках, передбачених законодавством;
- веде електронні реєстри сертифікатів відкритих ключів підписувачів, у тому числі блокованих і скасованих;
- зберігає сертифікати відкритих ключів підписувачів;
- забезпечує цілодобово доступ до сертифікатів відкритих ключів підписувачів та їх електронних реєстрів через загальнодоступні телекомунікаційні мережі;
- надає підписувачам консультації з питань, пов'язаних з використанням ЕЦП;
- розглядає заяви і скарги щодо неналежного функціонування АЦСК та організовує розслідування оскаржених дій.

6.1.2 Перелік послуг ЕЦП, що надаються АЦСК:

1) обслуговування сертифікатів відкритих ключів підписувачів, що включає:
- реєстрацію підписувачів;
- сертифікацію відкритих ключів підписувачів (шляхом формування відповідних сертифікатів відкритих ключів підписувачів);
- розповсюдження сертифікатів відкритих ключів підписувачів (за їх згодою);
- управління статусом сертифікатів відкритих ключів підписувачів та розповсюдження інформації про нього;

2) надання послуг фіксування часу;

3) надання підписувачам АЦСК допомоги в генерації відкритих та особистих ключів;

4) надання підписувачам АЦСК у користування надійних засобів ЕЦП;

5) консультаційні послуги у сфері ЕЦП.

Надання вищезазначених послуг здійснюється АЦСК у відповідності до цього документу та на підставі укладених договорів.

6.1.3 АЦСК має право:

- надавати послуги ЕЦП та обслуговувати сертифікати відкритих ключів підписувачів відповідно до вимог чинного законодавства та умов укладених договорів;
- отримувати інформацію, необхідну для реєстрації підписувача і формування сертифіката відкритого ключа, безпосередньо у юридичної (фізичної особи – підприємця) або фізичної особи чи у її уповноваженого представника та перевіряти її;
- встановлювати графіки прийому заявників (підписувачів) для надання їм планових консультацій щодо використання ЕЦП;
- припинити надання заявнику (підписувачу) послуг ЕЦП у разі несплати ним вартості послуг, порушення умов цього Регламенту та договору про надання послуг ЕЦП;
- не приймати запит на формування сертифіката у разі невиконання заявником вимог п. 10.1.2 цього Регламенту;
- вимагати від заявника (підписувача) дотримуватись цього Регламенту та умов договору про надання послуг ЕЦП;

- вимагати від заявника (підписувача) відшкодування згідно чинного законодавства майнової та моральної шкоди в разі, якщо така шкода була завдана АЦСК з вини заявника (підписувача);

- вимагати від заявника (підписувача) підписання Акту прийому-передачі наданих послуг;

- здійснювати аудіозапис всіх телефонних дзвінків до АЦСК, зокрема, для підтвердження факту здійснення голосової аутентифікації заявника при блокуванні його сертифікатів відкритих ключів.

6.1.4 АЦСК зобов'язаний:

- використовувати особистий ключ АЦСК, відповідний засвідченому в ЦЗО відкритому ключу (шляхом формування сертифіката), виключно для формування сертифікатів підписувачів та списків відкликаних сертифікатів;

- забезпечити можливість цілодобового вільного доступу заінтересованих осіб з використанням загальнодоступних телекомунікаційних мереж до сертифікатів підписувачів (за згодою заявників), даних про статус сертифікатів ключів, сертифікатів АЦСК, нормативних документів з питань надання послуг ЕЦП;

- забезпечувати захист інформації в інформаційно-телекомунікаційній системі АЦСК відповідно до чинного законодавства;

- забезпечувати захист персональних даних, отриманих від заявника (підписувача), згідно з чинним законодавством;

- при формуванні сертифікатів відкритих ключів дотримуватися вимог цього документу та умов договорів, укладених з заявниками;

- встановлювати під час формування сертифіката відкритого ключа належність відкритого ключа та відповідного особистого ключа підписувачу згідно вимог цього документу;

- встановлювати осіб, які звернулися до АЦСК з метою формування сертифікату відкритого ключа;

- своєчасно попереджувати підписувача та додавати в сертифікат відкритого ключа підписувача інформацію про обмеження використання ЕЦП, які встановлюються для забезпечення можливості відшкодування збитків сторін у разі заподіяння шкоди з боку АЦСК;

- своєчасно скасовувати, блокувати та поновлювати сертифікати відкритих ключів у випадках, передбачених Законом України "Про електронний цифровий підпис" та цим Регламентом;

- перевіряти законність звернень про скасування, блокування та поновлення сертифікатів відкритих ключів та зберігати документи, на підставі яких були скасовані, блоковані та поновлені сертифікати відкритих ключів;

- визначати та доводити до відома заявників (підписувачів) режим роботи АЦСК;

- вести електронний перелік чинних, скасованих, блокованих та поновлених сертифікатів відкритих ключів;

- забезпечувати зберігання сформованих сертифікатів відкритих ключів протягом строку, передбаченого чинним законодавством для зберігання відповідних документів на папері;

- надавати консультації з питань, пов'язаних з використанням ЕЦП;

- визначати працівників, відповідальних за взаємодію із заінтересованими особами щодо надання консультацій з питань надання послуг ЕЦП;

- забезпечити можливість приймання запитів, визначених цим Регламентом, від заявників (підписувачів) засобами телефонного зв’язку та з використанням загальнодоступних телекомунікаційних мереж;

- вести облік укладених договорів із заявниками, а також документів (засвідчених в установчому порядку копій оригіналів документів), що використовуються під час реєстрації та зберігати їх протягом встановленого законодавством часу;

- забезпечувати унікальність реєстраційного номера сертифіката підписувача, що формуються АЦСК;

- інформувати користувачів про необхідність здійснення перевірки чинності сертифіката з використанням інформації про його статус та врахування всіх визначених у сертифікаті обмежень щодо його використання;

- публікувати список відкликаних сертифікатів на електронному інформаційному ресурсі АЦСК;

- використовувати програмно-технічний комплекс (далі – ПТК) АЦСК, засоби криптографічного захисту інформації, у тому числі засоби ЕЦП, що відповідають вимогам нормативних документів у галузі криптографічного захисту інформації та мають позитивний експертний висновок у цій галузі, а також атестат відповідності комплексної системи захисту інформації АЦСК;

- розташовувати засоби ПТК, які забезпечують роботу з особистим ключем АЦСК у спеціальних приміщеннях (екранованих шафах), здійснювати їх охорону для запобігання безконтрольного проникнення у спеціальні приміщення (серверну) АЦСК сторонніх осіб;

- використовувати для надання послуг електронного цифрового підпису надійні засоби ЕЦП.

Зберігання особистих ключів підписувачів в АЦСК та ознайомлення з ними персоналу АЦСК забороняється.

6.1.5 ВПР АЦСК має право:

- надавати послуги ЕЦП відповідно до вимог чинного законодавства та умов укладених договорів;

- отримувати інформацію, необхідну для реєстрації заявника (підписувача) і формування сертифіката відкритого ключа, безпосередньо у юридичної (фізичної особи – підприємця) або фізичної особи чи у її уповноваженого представника та перевіряти її;

- вимагати від заявника (підписувача) дотримуватись цього Регламенту та умов договору про надання послуг ЕЦП.

6.1.6 ВПР АЦСК зобов’язаний:

- забезпечувати захист персональних даних, отриманих від заявника (підписувача), згідно з чинним законодавством;

- встановлювати осіб, які звернулися до АЦСК з метою формування сертифікату відкритого ключа;

- своєчасно попереджувати підписувача та додавати в сертифікат відкритого ключа підписувача інформацію про обмеження використання ЕЦП, які встановлюються для забезпечення можливості відшкодування збитків сторін у разі заподіяння шкоди з боку АЦСК;

- своєчасно подавати запит до АЦСК щодо скасування, блокування та поновлення сертифікатів відкритих ключів у випадках, передбачених Законом України "Про електронний цифровий підпис" та цим Регламентом;

- перевіряти законність звернень про скасування, блокування та поновлення сертифікатів відкритих ключів та зберігати документи, на підставі яких були скасовані, блоковані та поновлені сертифікати відкритих ключів;

- доводити до відома заявників (підписувачів) режим роботи ВПР АЦСК;

- надавати консультації з питань, пов'язаних з використанням ЕЦП;

- вести облік документів (засвідчених в установчому порядку копій оригіналів документів), що використовуються під час реєстрації заявників (підписувачів) та зберігати їх протягом встановленого законодавством часу;

- інформувати користувачів про необхідність здійснення перевірки чинності сертифіката з використанням інформації про його статус та врахування всіх визначених у сертифікаті обмежень щодо його використання;

- використовувати ПТК АЦСК, засоби криптографічного захисту інформації, у тому числі засоби ЕЦП, що відповідають вимогам нормативних документів у галузі криптографічного захисту інформації та мають позитивний експертний висновок у цій галузі, а також атестат відповідності комплексної системи захисту інформації АЦСК;

- інформувати АЦСК про всі випадки некоректної роботи програмно-технічних засобів АЦСК, випадки підозри на компрометацію ключів та криптографічних засобів, які використовуються в роботі ВПР та його клієнтів.

- прийняти необхідні дії щодо забезпечення функціонування робочих місць ВПР згідно інструкцій та рекомендацій АЦСК;

- використовувати для надання послуг електронного цифрового підпису надійні засоби ЕЦП.

6.2 Права та обов’язки заявника

6.2.1 Заявник має право:

- своєчасно отримувати якісні послуги ЕЦП;

- ознайомитись з інформацією щодо діяльності АЦСК та надання послуг ЕЦП;

- подавати заяви, скарги, претензії;

- вимагати від АЦСК усунення порушень умов даного Регламенту та договору про надання послуг АЦСК;

- вимагати від АЦСК виконання вимог конфіденційності;

- оскаржити дії чи бездіяльність АЦСК у судовому порядку.

6.2.2 Заявник зобов'язаний:

- ознайомлюватися та дотримуватись правил надання послуг, визначених цим документом та чинним законодовавством;

- надавати під час реєстрації повну та дійсну інформацію, необхідну для формування сертифіката(ів) підписувача(ів), які належать до заявника;

- ознайомлювати підписувачів, які належать до заявника, з Регламентом та вимагати від них виконання положень цього Регламенту та договору про надання послуг АЦСК;

- вимагати від підписувачів, які належать до заявника, негайно інформувати АЦСК про наступні події, що трапилися до закінчення строку чинності сертифіката: втрату або компрометацію особистого ключа; виявлену неточність або зміну даних, зазначених у сертифікаті;

- не розголошувати та не повідомляти іншим особам коди доступу до особистого ключа та ключову фразу для голосової аутентифікації;

- письмово сповіщати АЦСК стосовно всіх підписувачів, що належать до заявника, про факти смерті фізичної особи – підписувача або оголошення його померлим за рішенням суду, визнання підписувача недієздатним за рішенням суду, а також надавати завірені документальні підтвердження цих фактів у встановлені цим Регламентом строки;

- письмово інформувати АЦСК про припинення діяльності юридичної особи (фізичної особи – підприємця) – заявника (надати дані про підписувачів, що до нього належать) та надавати завірені встановленим чином документи, які це підтверджують.

6.3 Права та обов’язки підписувача

6.3.1 Підписувач використовує особистий ключ та сертифікат відкритого ключа ЕЦП при виконанні операцій, пов’язаних з накладанням та перевіркою ЕЦП на електронних документах. Підписувачі (користувачі) можуть використовувати надійні засоби ЕЦП, що розповсюджуються АЦСК, для перевірки ЕЦП підписувачів.

6.3.2 Підписувач має право:

- своєчасно отримувати якісні послуги ЕЦП;

- ознайомитись з інформацією щодо діяльності АЦСК та надання послуг ЕЦП;

- вимагати від АЦСК усунення порушень умов даного Регламенту та договору про надання послуг АЦСК;

- вимагати від АЦСК виконання вимог конфіденційності;

- одержувати сертифікат відкритого ключа АЦСК;

- одержувати список відкликаних сертифікатів відкритих ключів, що сформований АЦСК;

- застосовувати сертифікат АЦСК для перевірки дійсності ЕЦП сертифікатів відкритих ключів, сформованих АЦСК;

- застосовувати список відкликаних сертифікатів відкритих ключів, сформований АЦСК, як для перевірки статусу власного сертифіката відкритого ключа, так і сертифікатів відкритих ключів інших підписувачів або механізм визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP;

- вимагати скасування, блокування або поновлення свого сертифіката відкритого ключа;

- отримувати від АЦСК відповідне програмне забезпечення;

- подавати заяви, скарги, претензії;

- оскаржити дії чи бездіяльність АЦСК у судовому порядку.

6.3.3 Підписувач зобов'язаний:

- ознайомитись та дотримуватись правил надання послуг ЕЦП, визначених чинним законодавством та цим документом;

- надавати під час реєстрації повну та дійсну інформацію, необхідну для формування сертифіката відкритого ключа підписувача;

- зберігати в таємниці особистий ключ та вживати всі можливі заходи для запобігання його втрати, розкриття, компрометації та несанкціонованих модифікації або використання;

- не розголошувати та не повідомляти іншим особам коди доступу до особистого ключа та ключову фразу для голосової аутентифікації;

- використовувати особистий ключ виключно для мети, визначеної у сертифікаті відкритого ключа, та додержуватися інших обмежень щодо використання сертифіката відкритого ключа;

- використовувати виключно надійні засоби ЕЦП для генерації особистих та відкритих ключів, формування, накладання та перевірки ЕЦП;

- негайно інформувати АЦСК про наступні події, що трапилися до закінчення строку чинності сертифіката: компрометацію особистого ключа; компрометацію коду доступу до особистого ключа; виявлену неточність або зміну даних, зазначених у сертифікаті відкритого ключа;

- не використовувати особистий ключ в разі його компрометації;

- не використовувати особистий ключ відповідний до сертифіката, заява на скасування чи блокування якого подана до АЦСК, протягом часу з моменту подання заяви і до моменту офіційного повідомлення про поновлення сертифіката відкритого ключа;

- не використовувати особистий ключ, відповідний до сертифіката відкритого ключа, що скасований або блокований.

6.3.4 Користувачі можуть не мати договірних відносин з АЦСК, однак при цьому можуть використовувати загальнодоступну інформацію з електронного інформаційного ресурсу АЦСК, а також користуватися низкою послуг АЦСК, що не потребують автентифікації.

Користувачі для перевірки ЕЦП підписувачів повинні використовувати надійні засоби ЕЦП.

6.3.5 Користувач зобов'язаний:

- використовувати надійні засоби ЕЦП;

- підтверджувати ЕЦП з використанням чинних сертифікатів АЦСК;

- під час перевірки ЕЦП використовувати сертифікат, чинний на момент накладення ЕЦП.

6.4 Перелік посадових осіб АЦСК, що забезпечують його функціонування та обслуговування сертифікатів відкритих ключів, їх основні функції

До складу організаційної структури АЦСК входять наступні посадові особи та структурні одиниці:

- начальник АЦСК;

- адміністратор безпеки (який входить до складу Служби захисту інформації (далі – СЗІ));

- оператор реєстрації (у разі необхідності);

- адміністратор реєстрації;
- адміністратор сертифікації;
- системний адміністратор;
- Служба захисту інформації (штатна або позаштатна);
- ВПР (у разі створення).

Начальник АЦСК відповідає за керування АЦСК, вчасне та якісне виконання покладених на нього функціональних завдань.

Адміністратор безпеки відповідає за належне функціонування комплексної системи захисту інформації інформаційно-телекомунікаційної системи АЦСК та забезпечення захисту інформації з обмеженим доступом (зокрема, персональних даних підписувачів), що обробляється та зберігається в цій системі, здійснює контроль за генерацією ключових даних АЦСК, застосуванням та збереженням особистого ключа АЦСК та його резервної копії.

Оператор реєстрації відповідає за встановлення фізичної або юридичної особи (фізичної особи – підприємця) під час формування, блокування, поновлення або скасування сертифіката відкритого ключа.

Адміністратор реєстрації відповідає за встановлення фізичної або юридичної особи (фізичної особи – підприємця) під час формування, блокування, поновлення або скасування сертифіката відкритого ключа, генерацію ключових даних підписувачів, допомогу з генерації ключових даних підписувачів, оформлення договорів з заявниками щодо надання послуг ЕЦП та здійснення відповідних супутніх процедур, здійснює контроль за роботою оператора (операторів) реєстрації.

Адміністратор сертифікації відповідає за формування сертифікатів відкритих ключів, списків відкликаних сертифікатів, генерацію ключових даних АЦСК, збереження та використання особистого ключа АЦСК та його резервної копії, публікацію сертифікатів та списків відкликаних сертифікатів на інформаційному ресурсі АЦСК.

Системний адміністратор відповідає за функціонування інформаційно-телекомунікаційної системи АЦСК, забезпечує підтримку електронного інформаційного ресурсу АЦСК, створення резервних копій баз даних та відновлення даних, відповідає за забезпечення безпеки серверів АЦСК.

СЗІ АЦСК відповідає за організаційне забезпечення керування комплексною системою захисту інформації в автоматизованій системі АЦСК та здійснення контролю за її функціонуванням.

ВПР АЦСК здійснює представництво інтересів АЦСК ДП "УІПВ" у відповідному регіоні з питань надання послуг ЕЦП.

6.5 Розподіл прав і обов’язків

Розподіл прав і обов’язків у відносинах між суб’єктами правових відносин в сфері ЕЦП визначаються договорами про надання послуг ЕЦП та документами, на які зазначеними договорами здійснюються посилання.

6.6 Відповідальність

В разі невиконання своїх обов’язків за даним документом АЦСК або заявниками (далі разом – Сторони) повинні в повному обсязі відшкодувати збитки, заподіяні іншій стороні, у порядку, встановленому чинним законодавством.

Сторони несуть відповідальність за дії своїх співробітників, а також інших осіб, які мають або мали доступ (незалежно від того, був цей доступ санкціонований Стороною, або виник по її провині) до апаратних засобів, програмного, інформаційного забезпечення, криптографічних ключів та інших засобів ЕЦП, як за свої особисті.

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

АЦСК не несе відповідальності за майнову та моральну шкоду, що була спричинена підписувачу неналежною роботою програмного забезпечення АЦСК в разі, якщо неналежна

робота програмного забезпечення була викликана "мережевими атаками", дією "вірусних програм" або іншим неякісним (неліцензованим) програмним забезпеченням підписувача.

АЦСК не несе відповідальності за майнову та моральну шкоду, що може бути спричинена підписувачу та (або третім особам) в разі невиконання або неналежного виконання підписувачем вимог цього документу, умов договору про надання послуг ЕЦП або вимог чинного законодавства.

АЦСК не відповідає за невиконання або неналежне виконання своїх обов'язків за даним документом, а також за збитки, що виникли у зв'язку із цим, у випадках:

- якщо АЦСК обґрунтовано покладався на відомості, зазначені в заяві заявника на формування сертифіката відкритого ключа підписувача;
- підробки, підміни або іншого перекручування заявником або його уповноваженим представником відомостей, що містяться в заяві на формування сертифіката відкритого ключа підписувача або в інших документах, наданих АЦСК.

АЦСК відповідає за:

- збитки перед підписувачем у разі невиконання своїх зобов'язань, що можуть призвести до нелегитимності посиленого сертифіката відкритого ключа підписувача (зокрема, якщо під час формування посиленого сертифіката відкритого ключа підписувача використовувались ненадійні засоби ЕЦП, відсутнє свідоцтво про акредитацію тощо);
- надання користувачу недостовірної інформації про статус посиленого сертифіката ключа підписувача;
- збитки при використанні особистого ключа та сертифіката відкритого ключа підписувача тільки у випадку, якщо дані збитки виникли внаслідок компрометації особистого ключа АЦСК або внаслідок невідповідності відомостей у сертифікаті відкритого ключа відомостям, зазначеним у заяві підписувача.

Виплата пені і відшкодування збитків не звільняє Сторони від виконання своїх обов'язків за даним документом.

Відповідальність Сторін, яка не врегульована положеннями даного документу, регулюється чинним законодавством України.

Сторони звільняються від відповідальності за повне або часткове невиконання своїх зобов'язань, якщо таке невиконання сталося внаслідок настання форс-мажорних обставин, таких, як пожежа, повінь землетрус, інше стихійне лихо, військові дії, дія надзвичайного стану, блокада, громадські масові зворушення, страйків, диверсій, або інших обставин, які не залежать від волі Сторін, за умови, що дані обставини безпосередньо впливають на виконання їх зобов'язань, і їх неможливо було передбачити на момент укладання договору про надання послуг ЕЦП.

Сторона, що через зазначені вище обставини не може в повному обсязі виконувати свої зобов'язання, повинна в строк до 5-ти (п'яти) днів письмово сповістити про це іншу Сторону, а в строк до 10-ти (десяти) днів надати відповідні документи, які це підтверджують.

Несвоєчасне (пізніше 5-ти (п'яти) днів) повідомлення про існування обставин форс-мажору позбавляє відповідну Сторону права посилатися на них.

Достатнім доказом існування обставин форс-мажору є довідки компетентних органів влади.

У випадку, якщо вищезгадані обставини будуть діяти більше 3 (трьох) місяців, кожна зі Сторін може письмово сповістити іншу про повне або часткове припинення дії договору про надання послуг ЕЦП, що звільняє Сторони від взаємних зобов'язань, за винятком проведення взаєморозрахунків у частині вже виконаних Сторонами зобов'язань.

6.7 Порядок розв'язання спорів та вирішення конфліктних ситуацій

Будь-яка конфліктна ситуація вирішується шляхом переговорів із дотриманням претензійного порядку.

У разі виникнення непорозумінь щодо виконання вимог цього документу та умов договору про надання послуг ЕЦП, які не вирішено мирним шляхом, або інших спірних питань, Сторона, яка вважає, що її права порушуються, зобов'язана в місячний строк з

моменту, коли вона дізналась або повинна була дізнатись про таке порушення, направити іншій Стороні обґрунтовану претензію.

Претензія, направлена з порушенням зазначеного строку, не розглядається.

Термін розгляду претензії – 10 (десять) робочих днів з моменту її одержання.

Усі спірні ситуації, за якими не досягнуто згоди в претензійному порядку, вирішуються у господарському або загальному суді.

7 СФЕРА ВИКОРИСТАННЯ СЕРТИФІКАТІВ ВІДКРИТИХ КЛЮЧІВ

7.1 Сфера діяльності АЦСК

АЦСК надає послуги ЕЦП юридичним (фізичним особам – підприємцям) або фізичним особам, що заінтересовані у використанні таких послуг та є суб'єктами правових відносин у сфері надання послуг ЕЦП. Основним завданням АЦСК є обслуговування сертифікатів відкритих ключів підписувачів, виданих АЦСК.

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

7.2 Сфера використання сертифікатів відкритих ключів, сформованих АЦСК

Сертифікати відкритих ключів, які формуються АЦСК, призначені для забезпечення діяльності фізичних та юридичних осіб (фізичних осіб – підприємців), яка здійснюється з використанням електронних документів.

ЕЦП, який формується та перевіряється з використанням сертифікатів відкритих ключів, що формуються АЦСК, використовується фізичними та юридичними особами (фізичними особами – підприємцями) – суб'єктами електронного документообігу – для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Перелік сфер, у яких дозволяється використання сертифікатів:

- електронний цифровий підпис;
- неспростовність;

Відкритий ключ використовується в протоколах погодження ключа.

7.3 Обмеження щодо використання сертифікатів відкритих ключів, сформованих АЦСК

Обмеження щодо використання сформованих АЦСК сертифікатів ключів застосовуються у відповідності до положень цього Регламенту та діючого законодавства України.

АЦСК має право встановлювати обмеження сфери використання сформованих ним сертифікатів ключів. Інформація щодо обмеження сфери використання сертифікату ключа зазначається у сформованому сертифікаті ключа у вигляді уточненого призначення ключа.

8 ПОРЯДОК РОЗПОВСЮДЖЕННЯ (ПУБЛІКАЦІЇ) ІНФОРМАЦІЇ АЦСК

8.1 Перелік інформації, що публікується АЦСК на електронному інформаційному ресурсі.

На електронному інформаційному ресурсі АЦСК розміщується наступна інформація:

- положення чинного регламенту роботи АЦСК, засвідчені ЕЦП уповноваженої особи АЦСК;
- нормативно-правові акти України у сфері ЕЦП;
- довідково-методичні матеріали щодо порядку використання послуг ЕЦП;
- форми документів заявників;
- сертифікати відкритих ключів АЦСК;
- порядок перевірки чинності сертифікатів відкритих ключів, у тому числі умов перевірки статусу сертифіката;
- списки відкликаних сертифікатів відкритих ключів;
- списки чинних сертифікатів відкритих ключів підписувачів (за згодою заявника про опублікування сертифіката підписувача, що належить до заявника);
- контактна інформація АЦСК (фізична адреса, контактні телефони тощо), а також перелік ВПР (у разі наявності) з адресами та контактними телефонами.

Зазначені інформаційні об’єкти доступні цілодобово.

Електронна адреса (URL-адреса) електронного інформаційного ресурсу: http://www.ukrpatent.org.

Технічною основою інформаційного ресурсу АЦСК є веб-сервер, що входить до складу ПТК АЦСК.

Довідкова інформація (регламент роботи АЦСК, довідково-методичні матеріали щодо порядку використання послуг ЕЦП, контактна інформація тощо) розміщується на веб-сервері у вигляді набору веб-сторінок або електронних документів (з розширеннями .doc або .pdf).

Сертифікат відкритого ключа АЦСК, сертифікати відкритих ключів підписувачів, а також списки відкликаних сертифікатів розміщуються у складі веб-сторінок на веб-сервері. Доступ до веб-сервера здійснюється за DNS-ім’ям за протоколом HTTP.

Для розповсюдження інформації про статус сертифікатів ключів підписувачів використовується механізм списку відкликаних сертифікатів та механізм визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP.

АЦСК надає всім користувачам послугу інтерактивного визначення статусу сертифіката (в режимі реального часу). Послуга надається шляхом відправлення запиту за протоколом HTTP на OCSP-сервер АЦСК.

8.2 Час і порядок публікації сертифікатів та списків відкликаних сертифікатів

8.2.1 Інформація щодо формування сертифікатів відкритих ключів підписувачів та самі сертифікати відкритих ключів (за згоди їх власників на опублікування своїх сертифікатів) розміщуються на електронному інформаційному ресурсі АЦСК безпосередньо після їх формування.

8.2.2 Оновлення списків відкликаних сертифікатів відкритого ключа здійснюється на електронному інформаційному ресурсі АЦСК відповідно до п. 10.6.5 цього документу безпосередньо після обробки відповідного запиту на скасування, блокування чи поновлення свого сертифікату відкритого ключа.

9 ПОРЯДОК ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

9.1 Механізми підтвердження володіння підписувачем особистим ключем

Відкритий ключ підписувача подається на сертифікацію виключно у вигляді самопідписаного відповідним особистим ключем запиту формату PKCS#10. Належність підписувачу особистого ключа, що відповідає відкритому ключу, наданому на сертифікацію, підтверджується шляхом перевірки в АЦСК ЕЦП запиту на формування сертифіката ключа.

9.2 Умови встановлення юридичної (фізичної особи – підприємця) або фізичної особи

9.2.1 Встановлення юридичної особи (фізичної особи – підприємця) здійснюється за її установчими документами (положення, статут юридичної особи тощо) або копіями таких документів, які нотаріально посвідчені відповідно до чинного законодавства. Крім цього, встановлюється представник юридичної особи (фізичної особи – підприємця) та його повноваження за довіреністю (дорученням).

9.2.2 Встановлення фізичної особи здійснюється за паспортом (або іншим документом, який засвідчує особу відповідно до законодавства України).

9.2.3 Під процедурою реєстрації заявника розуміється встановлення фізичної особи, юридичної особи (фізичної особи – підприємця) та уповноваженого представника юридичної особи (фізичної особи – підприємця) за наданими документами та внесення відповідних відомостей щодо фізичних осіб, юридичних осіб (фізичних осіб – підприємців) до списку підписувачів АЦСК, який ведеться адміністратором реєстрації в електронному вигляді.

9.2.4 Заявник може доручити довіреній особі подання необхідних документів на реєстрацію в АЦСК, якщо заявник за будь-якої причини не може прийняти особисту участь в процедурі реєстрації. У цьому випадку довірена особа надає довіреність (доручення) на подання документів для реєстрації.

Довіреність (доручення) засвідчується:

- для юридичної особи (фізичної особи – підприємця): підписом керівника (або особи, яка його заміщує), фізичної особи – підприємця та печаткою (за наявності);
- для фізичної особи: нотаріально.

У разі, якщо під час реєстрації встановлюється підписувач – фізична особа як представник юридичної особи, заявник повинен додатково надати до АЦСК відомості щодо належності підписувача до цієї юридичної особи.

Якщо заявником подано оригінал документу, копія такого документу може бути засвідчена посадовою особою АЦСК (ВПР).

9.2.5 Перелік документів, які надаються АЦСК:

9.2.5.1 Для формування сертифікату відкритого ключа фізичної особи, що представляє юридичну особу (фізичну особу-підприємця) як підписувач:

- заява, встановленої форми, на формування сертифіката для представника (кожного з представників, для яких буде сформовано сертифікат) юридичної особи (фізичної особи-підприємця), підписана уповноваженою особою юридичної особи (фізичною особою-підприємцем) та засвідчена печаткою юридичної особи (фізичної особи-підприємця, у разі наявності). У заяві обов’язково зазначається адреса, телефон або інша інформація, що дозволяє зв'язатися з підписувачем;
- копія документу, що підтверджує реєстрацію в Єдиному державному реєстрі юридичних осіб та фізичних осіб – підприємців, засвідчена в установленому порядку;
- оригінал установчих документів (витягів із них), що містять положення про права, обов’язки, повноваження та порядок створення органів управління юридичної особи (надається тільки юридичною особою) або їх нотаріально засвідчена копія (для ознайомлення);
- копія документа про обрання (призначення) керівника юридичної особи, засвідчена в установленому порядку (надається тільки юридичною особою);
- копії 1 - 4 сторінок, з паспорту фізичної особи, що представляє юридичну особу (фізичну особу-підприємця) як підписувач, засвідчені в установленому порядку;

- копія довідки про реєстрацію облікової картки платників податків з Державного реєстру фізичних осіб – платників податків.

- оригінал довіреності, що підтверджує правомочність дій представника юридичної особи (фізичної особи-підприємця), який подає документи у АЦСК, від імені юридичної особи (фізичної особи-підприємця);

- копія свідоцтва про реєстрацію платника податку на додану вартість (у разі, якщо особа є платником ПДВ), засвідчена в установленому порядку;

- копія документу, що підтверджує статус (посаду) підписувача, засвідчена в установленому порядку;

- запечатаний непрозорий конверт з парольною фразою та допоміжним питанням, яке дасть змогу її згадати (у разі, якщо вона не вказана у заяві на формування сертифіката відкритого ключа).

При подачі документів представник, який подає документи у АЦСК, повинен мати при собі паспорт.

9.2.5.2 Для формування сертифікату відкритого ключа фізичної особи-підприємця:

- заява на формування сертифіката фізичної особи-підприємця, підписана фізичною особою-підприємцем та засвідчена печаткою фізичної особи-підприємця (у разі наявності). У заяві обов’язково зазначається адреса, телефон або інша інформація, що дозволяє зв'язатися з ним;

- копія документу, що підтверджує реєстрацію в Єдиному державному реєстрі юридичних осіб та фізичних осіб – підприємців, засвідчена в установленому порядку;

- копії 1 - 4 сторінок та сторінки, у якій вказано місце реєстрації, з паспорту фізичної особи-підприємця, засвідчені в установленому порядку;

- копія довідки про реєстрацію облікової картки платників податків з Державного реєстру фізичних осіб – платників податків, засвідчена в установленому порядку;

- запечатаний непрозорий конверт з парольною фразою та допоміжним питанням, яке дасть змогу її згадати (у разі, якщо вона не вказана у заяві на формування сертифіката відкритого ключа);

При подачі документів фізична особа-підприємець або його представник, який подає документи у АЦСК, повинна мати при собі паспорт.

9.2.5.3 Для формування сертифікату відкритого ключа печатки (штампа) юридичної особи (фізичної особи-підприємця):

- заява на формування сертифіката для печатки (штампа) юридичної особи (фізичної особи-підприємця), підписана уповноваженою особою юридичної особи (фізичною особою-підприємцем) та засвідчена печаткою юридичної особи (фізичної особи-підприємця, у разі наявності). У заяві обов’язково зазначається адреса, телефон або інша інформація, що дозволяє зв'язатися з керівником юридичної особи (фізичною особою-підприємцем);

- копія документу, що підтверджує реєстрацію в Єдиному державному реєстрі юридичних осіб та фізичних осіб – підприємців, засвідчена в установленому порядку;

- оригінал установчих документів (витягів із них), що містять положення про права, обов’язки, повноваження та порядок створення органів управління юридичної особи (надається тільки юридичною особою) або їх нотаріально засвідчена копія (для ознайомлення);

- копія документа про обрання (призначення) керівника юридичної особи, засвідчена в установленому порядку;

- копії 1 - 4 сторінок, з паспорту керівника юридичної особи (фізичної особи-підприємця), засвідчені в установленому порядку;

- копія свідоцтва про реєстрацію платника податку на додану вартість (у разі, якщо особа є платником ПДВ), засвідчена в установленому порядку;

- оригінал довіреності, що підтверджує правомочність дій представника юридичної особи (фізичної особи-підприємця), який подає документи у АЦСК, від імені юридичної особи (фізичної особи-підприємця);

- запечатаний непрозорий конверт з парольною фразою та допоміжним питанням, яке дасть змогу її згадати (у разі, якщо вона не вказана у заяві на формування сертифіката відкритого ключа).

При подачі документів керівник юридичної особи (фізична особа-підприємець) або її представник, який подає документи у АЦСК, повинен мати при собі паспорт.

9.2.5.4 Для формування сертифікату відкритого ключа фізичної особи:

- заява на формування сертифіката для фізичної особи, підписана фізичною особою. У заяві обов'язково зазначається адреса, телефон або інша інформація, що дозволяє зв'язатися з ним;

- копія 1 - 4 сторінок та сторінки, у якій вказано останнє місце реєстрації, з паспорту, засвідчені фізичною особою;

- копія довідки про реєстрацію облікової картки платників податків з Державного реєстру фізичних осіб – платників податків, засвідчена фізичною особою;

- якщо інтереси фізичної особи представляє інша особа, додається нотаріально засвідчена довіреність, що підтверджує повноваження цієї особи;

- запечатаний непрозорий конверт з парольною фразою та допоміжним питанням, яке дасть змогу її згадати (у разі, якщо вона не вказана у заяві на формування сертифіката відкритого ключа).

При подачі документів особа, яка подає документи до АЦСК (фізична особа або її представник), повинна мати при собі паспорт та оригінал довідки про включення до Державного реєстру фізичних осіб.

9.2.6 АЦСК не приймає до розгляду документи, які мають підчистки, дописки, закреслені слова, інші незастережні виправлення або написи олівцем, а також пошкодження, внаслідок чого їхній текст не можна прочитати.

9.2.7 За результатами розгляду наданих документів адміністратор (оператор) реєстрації приймає рішення про відмову у реєстрації у наступних випадках:

- у разі невідповідності поданого пакету документів зі встановленим комплектом АЦСК;

- у разі подання неналежно засвідчених копій документів;

- у разі встановлення невідповідності наданих під час реєстрації даних фактичним.

9.2.8 У разі відмови у реєстрації, адміністратор (оператор) реєстрації повертає надані документи заявнику з роз'ясненням причин повернення.

9.2.9 Особа, вважається встановленою, при одночасному виконанні наступних умов:

- відомості, зазначені у заяві на формування сертифіката відкритого ключа підписувача, збігаються із відповідними відомостями, наведеними в представлених документах;

- представлені документи встановленого чинним законодавством вигляду та не містять ознак навмисного внесення змін до їх змісту (підчистки, затирання окремих місць, незавірені виправлення тощо).

9.2.10 У разі, якщо нормативно-правовими актами тимчасово встановлюються інші вимоги до певних видів документів, то на цей час будуть діяти відповідні норми прийнятих нормативно-правових актів без внесення додаткових змін до цього Регламенту.

9.3 Механізми автентифікації для підписувачів, які мають чинний сертифікат відкритого ключа, сформований в АЦСК

В АЦСК існують наступні механізми автентифікації для підписувачів, які мають чинний сертифікат відкритого ключа, сформований в АЦСК:

- при особистому зверненні: паспорт або інший документ, який посвідчує особу підписувача (для фізичної особи); паспорт, який посвідчує особу представника, та довіреність (для представника юридичної особи або фізичної особи – підприємця) або нотаріально засвідчена довіреність (для представника фізичної особи);

- при письмовому (паперовому) зверненні: лист за підписом підписувача (для фізичної особи); лист на фірмовому бланку за підписом уповноваженої особи заявника,

до якого належить підписувач, з проставлянням печатки (для юридичної особи або фізичної особи – підприємця, у разі її наявності);

- при зверненні телефонною мережею загального користування: умовне таємне слово (фраза) із парольної фрази, яка відома лише підписувачу (заявнику);
- при зверненні загальнодоступними телекомунікаційними мережами з використанням електронних запитів: електронний цифровий підпис, сформований з використанням особистого ключа підписувача.

9.4 Механізми автентифікації під час звернення до АЦСК щодо блокування, скасування та поновлення сертифіката відкритого ключа

В залежності від порядку звернення щодо блокування, скасування та поновлення сертифікату ключа передбачені різні форми автентифікації підписувача та перевірки законності такого звернення:

- у разі письмового звернення заявника законність звернення встановлюється за власноручним підписом уповноваженої особи заявника та печаткою організації заявника (для юридичних осіб та фізичних осіб – підприємців, у разі її наявності);
- у разі звернення заявника у електронній формі законність звернення встановлюється за електронним цифровим підписом (у разі виконання вимог п. 6.3.3 цього Регламенту), створеним за допомогою особистого ключа заявника (до закінчення строку його чинності) та печатки організації заявника (для юридичних осіб та фізичних осіб – підприємців, у разі її наявності);
- у разі звернення щодо блокування сертифікату ключа в телефонному режимі законність звернення встановлюється за парольною фразою голосової автентифікації, що вказується заявником під час реєстрації.

10 УМОВИ, ПРОЦЕДУРИ ТА МЕХАНІЗМИ, ПОВ'ЯЗАНІ ІЗ ФОРМУВАННЯМ, БЛОКУВАННЯМ, СКАСУВАННЯМ ТА ВИКОРИСТАННЯМ СЕРТИФІКАТА ВІДКРИТОГО КЛЮЧА

10.1 Процес подання заяви на формування сертифіката відкритого ключа

10.1.1 Перелік суб'єктів, які можуть подавати документи на формування сертифіката відкритого ключа

Документи на формування сертифіката відкритого ключа можуть подати наступні заявники:

- фізичні особи, що бажають отримати сертифікат відкритого ключа, або їх уповноважені представники;
- юридичні особи (фізичні особи – підприємці), що бажають отримати сертифікат відкритого ключа, в особі їх посадових осіб, або їх уповноважені представники.

10.1.2 Порядок подачі та оброблення заяви на формування сертифіката відкритого ключа

Заявник повинен обов'язково ознайомитися з документами, висвітленими на електронному інформаційному ресурсі АЦСК.

Заявник готує необхідний пакет документів для подання до АЦСК (визначено цим Регламентом та висвітлено на електронному інформаційному ресурсі АЦСК) та передає його особисто, через довірену особу або надсилає поштою до АЦСК.

Адміністратор (оператор) реєстрації АЦСК попередньо опрацьовує наданий пакет документів, після чого, у разі відповідності пакету документів вимогам даного Регламенту, узгоджує з заявником дату його прибуття до АЦСК для встановлення особи заявника та формування сертифіката відкритого ключа.

У разі невідповідності пакету документів вимогам даного Регламенту, він повертається заявнику.

Адміністратор (оператор) реєстрації АЦСК встановлює особу заявника, перевіряє надані ним дані та заповнює заяву на формування сертифіката відкритого ключа в електронному вигляді за наданими даними.

Генерація особистих і відкритих ключів ЕЦП виконується при формуванні нового сертифіката ключа, а також при плановій та позаплановій замінах особистого ключа підписувача.

Відкритий і особистий ключі підписувача генеруються з використанням робочої станції адміністратора реєстрації або з робочого місця підписувача (заявника) виключно з використанням надійних засобів ЕЦП.

В процесі генерації ключів створюється особистий ключ, що записується на носій ключової інформації в форматі PKCS#8, та запит на формування сертифіката ключа. Запит на формування сертифіката ключа, що передається на сертифікацію до АЦСК, є самопідписаним запитом формату PKCS#10, який засвідчується ЕЦП за допомогою особистого ключа заявника (підписувача). Запит на формування сертифіката обробляється в АЦСК протягом доби з моменту його надходження.

Під час обробки запиту на формування сертифіката ключа здійснюється перевірка належності особистого ключа підписувача відкритому ключу, який міститься у запиті. Перевірка здійснюється з використанням програмного забезпечення ПТК АЦСК автоматично, шляхом перевірки ЕЦП, накладеного на запит на формування сертифіката ключа, з використанням відкритого ключа, що міститься у запиті. Формування сертифіката ключа можливе лише за умов успішної перевірки.

10.1.2.1 Генерація ключів на робочій станції адміністратора реєстрації

Якщо заявником (підписувачем) не було надано запит на сертифікацію у відповідному форматі, адміністратор реєстрації або заявник (підписувач) з використанням робочої станції адміністратора реєстрації забезпечує генерацію ключової пари для підписувача з використанням надійного засобу ЕЦП, після чого особистий ключ підписувача записується у зашифрованому вигляді на зйомний (захищений) носій ключової інформації.

Адміністратор реєстрації забезпечує конфіденційність особистого ключа підписувача під час генерації ключів та під час запису ключів на зйомний носій ключової інформації.

10.1.2.2 Генерація ключів на робочій станції заявника

Для генерації відкритого та особистого ключів на робочому місці заявника застосовуються надійні засоби ЕЦП. При цьому генерація здійснюється з використанням технічних засобів заявника.

Відповідальність за забезпечення конфіденційності та цілісності особистого ключа несе заявник.

Надійні засоби ЕЦП, що надаються заявнику АЦСК, формують запит на сертифікацію у відповідному форматі.

Передача до АЦСК (ВПР) сформованого підписувачем запиту на сертифікацію здійснюється на носії інформації особисто підписувачем, довіреною особою або засобами кур'єрської доставки кореспонденції.

При отриманні запиту на сертифікацію адміністратор реєстрації перевіряє формат наданого запиту. Перевірка здійснюється з використанням програмного забезпечення ПТК АЦСК автоматично. В разі невідповідності адміністратор реєстрації відмовляє в формуванні сертифіката. При цьому, надані раніше документи повертаються заявнику з позначкою адміністратора реєстрації в картці реєстрації ключа.

10.1.2.3 Подання заяви на формування сертифіката відкритого ключа на сертифікацію

Адміністратор реєстрації перевіряє заяву на формування сертифіката відкритого ключа у електронному вигляді, оформлену оператором реєстрації (за необхідності), заявником (підписувачем) або особисто формує її. Заява на формування сертифіката відкритого ключа за умови правильності наданих у ній даних надсилається для подальшої обробки адміністратору сертифікації. В разі виявлення розбіжностей наведених відомостей у заяві на формування сертифіката відкритого ключа фактичним даним (або інших негативних результатів встановлення фізичної або юридичної особи, див. пп. 9.2.6 та 9.2.7) адміністратор реєстрації відхиляє її.

Адміністратор сертифікації з використанням робочої станції адміністратора сертифікації здійснює перевірку ЕЦП на засвідченій заяві на формування сертифіката відкритого ключа (така перевірка здійснюється автоматично прикладним програмним забезпеченням робочої станції адміністратора сертифікації). В разі встановлення відповідності ЕЦП адміністратор сертифікації формує сертифікат відкритого ключа ЕЦП з використанням особистого ключа АЦСК, що розміщений у зашифрованому вигляді в базі даних ПТК АЦСК на жорсткому диску серверу АЦСК або на захищеному знімному носію ключової інформації.

Також, під час формування сертифіката підписувача АЦСК присвоює унікальний реєстраційний номер сертифікату та перевіряє унікальність відкритого ключа підписувача в реєстрі чинних, блокованих та скасованих сертифікатів. Одночасно, АЦСК забезпечує унікальність розпізнавального імені підписувача в межах АЦСК.

Особистий ключ надається заявнику (підписувачу) або його довіреній особі на носії ключової інформації (дискеті, CD-диску, флеш-носії тощо). Якщо ключова пара підписувача була згенерована за допомогою ПТК, у присутності підписувача знищується копія згенерованого особистого ключа підписувача, що розміщується в запам’ятовуючих пристроях ПТК АЦСК, шляхом, що унеможливлює її поновлення. Підписувач власноручно вводить значення коду доступу до носія особистого ключа.

Якщо при формуванні сертифіката присутній заявник або представник, код доступу до носія особистого ключа підписувача вводить адміністратор реєстрації, після чого адміністратор реєстрації записує їх на аркуші та запечатує в непрозорий конверт. Підписувач після отримання повинен обов’язково змінити код доступу на особистий.

Підписувач при отриманні конверта зобов'язаний перевірити його цілісність. Якщо цілісність конверта порушена, підписувач невідкладно зобов'язаний звернутися до АЦСК із заявою про скасування сертифіката ключа.

Зберігання особистих ключів підписувачів в АЦСК та ознайомлення з ними персоналу АЦСК забороняються.

10.1.3 Порядок повторної реєстрації заявника після закінчення строку обслуговування сертифіката відкритого ключа

Процедура повторної реєстрації заявника після закінчення строку обслуговування сертифікату ключа ідентична процедурі первинної реєстрації заявника.

10.1.4 Порядок використання особистого ключа послуг фіксування часу

Особистий ключ послуг фіксування (штемпелювання) часу застосовується програмним забезпеченням зі складу ПТК АЦСК. Особистий ключ послуг фіксування (штемпелювання) часу знаходиться у робочому стані на сервері АЦСК.

При надходженні запиту на отримання позначки часу (токена часового штемпеля) програмне забезпечення зі складу ПТК АЦСК автоматично формує позначку часу (до складу якої входить інформація із запиту на отримання позначки часу та поточне значення часу на сервері АЦСК, синхронізоване відповідно до чинного законодавства.

10.2 Надання сформованого сертифіката відкритого ключа підписувачу

Сформований сертифікат, за бажанням заявника адміністратор реєстрації:

- записує на носій інформації та передає заявнику;
- надає сертифікат – документ у паперовій формі, який засвідчується підписом начальника АЦСК.

Після отримання сертифікату відкритого ключа заявник повинен перевірити достовірність даних, що містяться в ньому. У разі виявлення розбіжностей між даними, що подавались для формування сертифікату відкритого ключа, та даними, що містяться у сертифікаті, заявник повідомляє про це АЦСК, який вживає заходи щодо приведення сертифікату відкритого ключа у відповідність.

У разі, якщо розбіжностей не виявлено, заявник визнає свої сертифікати відкритих ключів шляхом підписання акту прийому-передачі наданих послуг.

З моменту отримання носія особистого ключа підписувач вважається власником сертифіката відкритого ключа та може виступати суб'єктом правових відносин у сфері надання послуг ЕЦП.

Після передачі конверта з носієм ключової інформації довіреній особі заявника, відповідальність за забезпечення конфіденційності та цілісності особистого ключа несе заявник.

10.3 Публікація сформованого сертифіката відкритого ключа підписувача

В разі, якщо при формуванні сертифіката відкритого ключа підписувача заявник погодився на його опублікування, сформований сертифікат відкритого ключа автоматично стане доступним за протоколами HTTP.

10.4 Використання сертифіката відкритого ключа та особистого ключа

10.4.1 Відповідальність підписувача – власника сертифіката відкритого ключа під час використання особистого ключа та сертифіката відкритого ключа

Заявник несе відповідальність за організацію, а підписувач за безпосереднє надійне збереження особистого ключа та носія ключової інформації, на якому він знаходиться, а також значення коду доступу до цього носія.

Підписувач несе відповідальність за розповсюдження власного сертифікату відкритого ключа (якщо заявник не дав згоду на його публікацію в АЦСК). В цьому випадку, підписувач повинен надавати сертифікат всім особам, з якими він вступає у правові відносини у сфері електронного цифрового підпису.

10.4.2 Відповідальність підписувачів (користувачів) під час використання сертифіката відкритого ключа

Підписувачі (користувачі) несуть відповідальність за вільне (безконтрольне) розповсюдження сертифікатів відкритих ключів інших осіб – суб'єктів правових відносин у сфері електронного цифрового підпису. Підписувачі (користувачі) повинні усвідомлювати, що сертифікат відкритого ключа містить персональні дані цих осіб та його розповсюдження без згоди власника призведе до неконтрольованого поширення зазначених відомостей, що може нанести цій особі моральні або матеріальні збитки.

10.5 Процедура подачі в електронній формі заяви на формування сертифіката відкритого ключа для підписувачів, які мають чинний сертифікат відкритого ключа, сформований АЦСК

В разі, якщо підписувач має чинний сертифікат відкритого ключа, термін дії якого закінчується, він може отримати новий сертифікат відкритого ключа за визначеною нижче процедурою для отримання сертифікату відкритого ключа.

Заявник заповнює заяву на формування сертифіката підписувача в електронному вигляді, робить сканкопії решти документів (згідно пункту 9.2.5) та підписує і завіряє їх встановленим чином за допомогою свого особистого ключа (до закінчення строку його чинності) і засвідчує електронною печаткою організації (в разі наявності).

Після цього повний пакет документів передається для розгляду до АЦСК.

У разі, якщо з часу попереднього подання пакету документів до АЦСК змін даних, зазначених в них, не було, то заявник може надіслати відповідного листа в електронній формі, за формою висвітленою на електронному інформаційному ресурсі АЦСК, та підписаного за допомогою свого особистого ключа (до закінчення строку його чинності) і засвідчує електронною печаткою організації (в разі наявності).

10.6 Порядок скасування (блокування, поновлення) сертифіката відкритого ключа

10.6.1 Обставини скасування (блокування, поновлення) сертифіката відкритого ключа

Підписувач зобов'язаний виконати дії зі скасування сертифікату у разі:

- компрометації особистого ключа підписувача;
- зміни відомостей, зазначених у сертифікаті відкритого ключа;
- зміни обставин, на підставі яких було надано право підпису;
- припинення діяльності юридичної особи – власника ключа.

У випадках:

- смерті фізичної особи – підписувача або оголошення його померлим за рішенням суду;
- визнання підписувача недієздатним за рішенням суду,

правонаступник підписувача або заявник (якщо підписувач відноситься до заявника) зобов'язаний сповістити АЦСК про ці події письмово та протягом семи робочих днів надати до АЦСК завірені копії документів, що підтверджують цю подію. АЦСК блокує сертифікат підписувача при надходженні відповідного письмового сповіщення та скасовує його після отримання документальних свідоцтв.

АЦСК автоматично скасовує сертифікат при закінченні строку його чинності.

До подій, пов'язаних з компрометацією ключів підписувачів, відносяться наступні:

Будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа, зокрема:

- втрата носіїв, на які записані особисті ключі;
- втрата носіїв, на які записані особисті ключі, з наступним виявленням;
- звільнення співробітників, що мали особисті ключі;
- порушення правил зберігання особистих ключів;
- виникнення підозр на несанкціоноване застосування особистого ключа;
- втрату контролю щодо особистого ключа через компрометацію коду доступу до носія особистого ключа;

- випадки, коли не можна вірогідно встановити, що відбулося з носіями, що містять ключову інформацію (у тому числі, випадки, коли носій вийшов з ладу й доказово не спростована можливість того, що даний факт відбувся в результаті несанкціонованих дій зловмисника).

У випадку компрометації ключа підписувач зобов'язаний терміново сповістити про цей факт АЦСК та виконати дії згідно пункту 10.6.3.

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 сертифіката відкритого ключа (для сертифікатів ключів юридичних осіб/посадових осіб);
- зміна прізвища;
- зміна місця прописки/реєстрації в частині, що вказана в реквізитах власника сертифіката відкритого ключа;
- виявлення помилок у реквізитах тощо.

Зміна зовнішніх обставин, які навіть при збереженні реквізитів власника сертифіката відкритого ключа змінюють його статус, що впливає на правомочність ЕЦП, зокрема, зміна положення про посаду, що призводить до того, що зазначені в сертифікаті відкритого ключа повноваження більше йому не належать (в тому числі втрата права підпису звітності, керування банківським рахунком тощо) потребує скасування сертифіката.

За виникнення будь-яких вищезазначених причин та обставин підписувач зобов'язаний невідкладно заблокувати сертифікат відкритого ключа та протягом терміну дії блокування виконати операції зі скасування сертифіката відкритого ключа згідно пункту 10.6.3.

АЦСК блокує сертифікат відкритого ключа підписувача:

- у разі подання заяви власника ключа або його уповноваженого представника;
- за рішенням суду, що набрало законної сили;
- у разі компрометації особистого ключа;
- у разі порушення умов договору до їх усунення.

Блокований сертифікат відкритого ключа поновлюється:

- у разі подання заяви власника ключа або його уповноваженого представника;
- за рішенням суду, що набрало законної сили;
- у разі встановлення недостовірності даних про компрометацію особистого ключа.

10.6.2 Перелік суб'єктів, уповноважених подавати заяву на скасування (блокування, поновлення) сертифіката відкритого ключа

Уповноваженими на подання заяви на скасування (блокування, поновлення) сертифіката відкритого ключа є підписувачі та заявники (щодо підписувачів, що відносяться до заявника).

10.6.3 Процедура подання заяви на скасування (блокування, поновлення) сертифіката відкритого ключа

10.6.3.1 Загальні відомості щодо скасування (блокування, поновлення) сертифіката відкритого ключа

Блокування тимчасово припиняє дію сертифіката відкритого ключа. Після блокування сертифіката заявник зобов'язаний або поновити сертифікат, або виконати скасування сертифікату.

Скасування припиняє дію сертифікату. Скасовані сертифікати поновленню не підлягають.

Поновлення чинності сертифікату ключа можливе лише для сертифікатів, що заблоковані і термін чинності сертифіката не скінчився.

Про зміну статусу сертифіката на електронну адресу підписувача, зазначену в заяві на формування сертифіката, направляється відповідне повідомлення.

10.6.3.2 Порядок блокування сертифіката відкритого ключа

Для здійснення блокування сертифіката заявник подає заяву на блокування до АЦСК.

Блокування сертифіката здійснюється АЦСК на підставі заяви, що надходить установленим порядком в АЦСК в усній, паперовій формі чи у вигляді електронного документа.

Часом блокування сертифіката вважається час опублікування на електронному інформаційному ресурсі АЦСК списку відкликаних сертифікатів з включеними до нього даними про зміну статусу даного сертифіката.

10.6.3.2.1 Блокування сертифіката за заявою в усній формі

Заява на блокування в усній формі подається в АЦСК за телефоном.

Заявник повинен повідомити адміністратору реєстрації АЦСК наступну інформацію:

- ідентифікаційні дані власника сертифікату відкритого ключа;

- серійний номер сертифіката, що блокується (якщо підписувач має більш, ніж один діючий сертифікат);

- парольну фразу (слово з парольної фрази) голосової автентифікації.

Заява в усній формі приймається тільки у випадку позитивної автентифікації (збігу даних підписувача та парольної фрази, переданих в заяві, з інформацією, що наявною в реєстрі підписувачів АЦСК).

Приймання і обробка заяви в усній формі здійснюється цілодобово. Обробка заяви в усній формі на блокування сертифіката та інформування заявника здійснюється безпосередньо після приймання заяви протягом двох годин.

Якщо блокування сертифіката відкритого ключа підписувача здійснюється в усній формі у неробочий час (пн-чт з 17.15 до 8.30, п’ятниця з 16.00) або у вихідні, святкові та неробочі дні, адміністратор (оператор) реєстрації протягом 1 (однієї) години з моменту надходження телефонного запиту від підписувача телефонує підписувачу, здійснює його автентифікацію та отримує усне підтвердження щодо правильності поданого ним запиту. Подальша обробка запиту відбувається згідно вищеописаного порядку.

10.6.3.2.2 Блокування сертифіката за заявою в паперовій формі

Заява в паперовій формі подається в АЦСК за встановленою формою, яку можливо отримати з електронного інформаційного ресурсу АЦСК.

Заява на блокування сертифіката засвідчується відповідно до п. 9.4 Регламенту.

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

Обробка заяви на блокування сертифіката та інформування заявника здійснюється протягом двох годин з моменту отримання заяви.

10.6.3.2.3 Блокування сертифіката за заявою у електронній формі

Електронна заява подається до АЦСК за встановленою формою та засвідчується заявником за допомогою свого особистого ключа (до закінчення строку його чинності) і електронною печаткою організації (в разі наявності). Заяви приймаються на електронну пошту info.acsk@ukrpatent.org.

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

Обробка заяви на блокування сертифіката та інформування заявника здійснюється протягом двох годин з моменту отримання заяви.

10.6.3.3 Порядок скасування сертифіката відкритого ключа

Для скасування сертифіката заявник подає заяву на скасування до АЦСК.

Скасування сертифіката здійснюється АЦСК на підставі заяви, що надходить встановленим порядком в АЦСК в паперовій або електронній формі.

Заява на скасування сертифіката в паперовій формі подається в АЦСК за відповідною формою, яка доступна на інформаційному ресурсі АЦСК.

Електронна заява подається до АЦСК за встановленою формою та засвідчується заявником за допомогою свого особистого ключа (до закінчення строку його чинності) і електронною печаткою організації (в разі наявності). Заяви приймаються на електронну пошту info.acsk@ukrpatent.org.

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

У випадку, якщо необхідне термінове скасування сертифіката ключа через об'єктивні обставини, з метою недопущення майнової шкоди, заявник (підписувач) має заблокувати сертифікат такого особистого ключа в усній формі з подальшим поданням письмової заяви про скасування сертифіката ключа.

Обробка заяви на скасування сертифіката здійснюється протягом двох годин з моменту отримання заяви.

Часом скасування сертифіката вважається час опублікування списку відкликаних сертифікатів з включеними до нього даними про зміну статусу даного сертифіката.

В разі припинення діяльності юридичної особи вона або її правонаступник звертається до АЦСК і подає:

- письмову заяву встановленого зразка про скасування всіх сертифікатів, які відносяться до юридичної особи, яку засвідчено підписом керівника та скріплено печаткою (у разі її наявності);

- довідку встановленого зразка про припинення діяльності юридичної особи, надану відповідним державним органом.

При скасуванні сертифікатів в даному випадку скасовуються всі чинні на момент скасування сертифікати, в яких код ЄДРПОУ юридичної особи співпадає із кодом ЄДРПОУ юридичної особи, що припинила діяльність.

10.6.3.4 Порядок поновлення сертифіката відкритого ключа

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

Поновлення чинності сертифіката здійснюється АЦСК на підставі заяви, що надходить встановленим порядком в АЦСК в паперовій формі, разом з запечатаним непрозорим конвертом з новою парольною фразою.

Заява на поновлення сертифіката подається в АЦСК за відповідною формою, яка доступна на інформаційному ресурсі АЦСК.

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

Обробка заяви на поновлення сертифіката здійснюється протягом двох годин з моменту отримання заяви.

Часом поновлення сертифіката вважається час опублікування списку відкликаних сертифікатів з виключеними з нього даними про зміну статусу даного сертифіката.

10.6.4 Час оброблення заяви на скасування (блокування, поновлення) сертифіката відкритого ключа

Приймання і обробка заяви на блокування сертифіката в усній формі здійснюється цілодобово.

Обробка заяви на скасування (блокування, поновлення) сертифіката в паперовій формі здійснюється протягом двох годин з моменту отримання такої заяви.

10.6.5 Частота формування списку відкликаних сертифікатів та строки його дії

Публікація списків відкликаних сертифікатів на електронному інформаційному ресурсі АЦСК здійснюється одразу після їх формування.

АЦСК виконує формування списків відкликаних сертифікатів двох типів:

− повний список;

− частковий список.

Повний список випускається не рідше 1 (одного) разу на місяць та містить інформацію про всі відкликані сертифікати ключів підписувачів протягом строку чинності сертифіката відкритого ключа АЦСК відповідного особистому ключу АЦСК, яким підписаний даний повний список.

Частковий список випускається не рідше 1 (одного) разу на тиждень або протягом двох годин після отримання заяви на скасування, блокування або поновлення сертифіката та містить інформацію про всі сертифікати, статус яких був змінений в інтервалі між часом

випуску останнього повного списку та часом формування поточного часткового списку. Кожний оновлений частковий список формується шляхом накопичення нових даних про всі сертифікати, статус яких був змінений. Після оновлення повного списку, інформація в частковому списку очищається та формується заново.

У списках відкликаних сертифікатів обов'язково зазначається точна дата та час публікації наступного списку відкликаних сертифікатів.

Новий список відкликаних сертифікатів може бути опублікований до визначеного часу видання наступного списку, вказаного у поточному списку відкликаних сертифікатів.

10.6.6 Відомості про можливість та умови надання інформації про статус сертифіката відкритого ключа у режимі реального часу

Заінтересована особа має можливість отримувати інформацію щодо чинних, скасованих і блокованих сертифікатів відкритих ключів з електронного інформаційного ресурсу АЦСК використовуючи комплекс користувача.

10.7 Закінчення строку чинності сертифіката відкритого ключа підписувача

Статус сертифіката змінюється автоматично на "нечинний" при закінченні строку чинності сертифіката відкритого ключа. Така зміна статусу не потребує переформування списку відкликаних сертифікатів.

10.8 Терміни дії ключових даних, що формуються та використовуються в АЦСК

Термін дії для особистих ключів дорівнює терміну дії відповідних їм відкритих ключів. Термін дії відкритих ключів визначається терміном чинності сертифікатів відкритих ключів.

Терміни чинності сертифікатів відкритих ключів:

- сертифікат відкритого ключа АЦСК – не більше ніж 5 років;
- сертифікат відкритого ключа послуг фіксування часу та послуг визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP – не більше ніж 5 роки;
- сертифікат відкритого ключа посадової особи АЦСК – не більше ніж 2 роки;
- сертифікат відкритого ключа підписувача – не більше ніж 2 роки.

Проміжки часу, протягом яких є чинними ключі посадової особи АЦСК та ключі, що застосовуються при наданні послуг фіксування часу, повинні цілком знаходитися у проміжку часу, протягом якого є чинним ключ АЦСК.

Термін дії довгострокового ключового елемента (заповнення вузлів заміни) для алгоритму гешування, визначеного ГОСТ 34.311-95, не обмежується.

По закінченні терміну дії ключів вони змінюються в установленому порядку.

11 УПРАВЛІННЯ ТА ОПЕРАЦІЙНИЙ КОНТРОЛЬ

11.1 Фізичне середовище

11.1.1 Опис спеціального приміщення

11.1.1.1 Компоненти ПТК АЦСК розміщуються у наступних приміщеннях: спеціальному приміщенні (серверне приміщення), у якому знаходиться захищена (екранована) шафа з обладнанням АЦСК, та робочих приміщеннях АЦСК.

11.1.1.2 Приміщення відповідають вимогам техніки безпеки та протипожежної безпеки, комплектуються необхідними засобами енергозабезпечення, охоронної та протипожежної сигналізації, відеоспостереження (за необхідності), допоміжними технічними засобами (у робочому приміщенні АЦСК - механічний та електронний замок, відеодомофон; у спеціальному приміщенні АЦСК: перші двері - механічний замок та електронний замок, другі двері – механічний замок та спеціальний замок із запором), системами життєзабезпечення (кондиціонерами).

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

Відповідальність за організацію охорони, стан перепускного й внутрішнього режиму АЦСК в цілому покладається на службу захисту інформації.

Загальне керівництво й контроль за організацією охорони, станом перепускного й внутрішнього режиму здійснює начальник служби захисту інформації АЦСК.

11.1.1.3 Спеціальне приміщення АЦСК відповідає 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 криптографічного захисту інформації та відповідає вимогам нормативних документів в сфері технічного захисту інформації стосовно створення комплексної системи захисту інформації.

11.1.1.4 У спеціальному приміщенні АЦСК розміщені:

- захищена (екранована) шафа, в якій розміщується обладнання АЦСК і яка забезпечує виконання вимог Правил посиленої сертифікації щодо захисту від витоку та деструктивного впливу зовнішніх електромагнітних полів;
- робоче місце адміністратора сертифікації.

11.1.1.5 Захищена (екранована) шафа має механічний замок, ключ від якого є лише у системного адміністратора (дублікат ключа зберігається в сейфі начальника АЦСК) та забезпечує можливість її опломбування.

11.1.2 Пропускний і внутрішній режим

Пропускний і внутрішній режим визначається окремим внутрішнім документом, який передбачає порядок допуску співробітників і представників інших організацій на територію АЦСК, порядок внесення і винесення матеріальних цінностей, а також виконання особами, що перебувають на території АЦСК, встановлених вимог режиму й розпорядку робочого дня.

Загальне керівництво й контроль за організацією охорони, станом перепускного й внутрішнього режиму здійснює керівник служби захисту інформації АЦСК.

11.2 Процедурний контроль

11.2.1 Права та обов'язки посадових осіб та структурних одиниць АЦСК

11.2.1.1 Начальник АЦСК:

– організовує роботу АЦСК, несе персональну відповідальність за виконання покладених на АЦСК завдань, визначає ступінь відповідальності працівників;

– забезпечує визначення та підтримку в актуальному стані політики та цілей АЦСК;

– контролює дотримання персоналом АЦСК вимог керівних, нормативних, методичних та інших документів, які стосуються АЦСК;

– розробляє та подає на затвердження директору підприємства посадові інструкції персоналу, контролює взаємну несуперечність документів;

– подає директору підприємства пропозиції щодо призначення в установленому порядку на посаду та звільнення з посади персоналу АЦСК;

– видає у межах своєї компетенції накази та розпорядження з метою виконання положень цього документу, організовує і контролює їх виконання;

– організовує підвищення кваліфікації персоналу;

– вживає заходів для підвищення ефективності роботи працівників АЦСК та відокремлених пунктів;

– здійснює контроль за забезпеченням безпеки інформаційних ресурсів АЦСК;

– забезпечує ефективне використання і збереження майна АЦСК, організує діловодства АЦСК;

– подає до ЦЗО дані, які необхідні для формування та засвідчення сертифіката відкритого ключа АЦСК.

11.2.1.2 Адміністратор безпеки:

– здійснює контроль за діяльністю персоналу щодо виконання ним вимог цього регламенту, інших нормативних документів АЦСК при генерації ключових даних та поводженні з ключовими документами;

– подає начальнику АЦСК пропозиції щодо дій у випадку виявлення порушень або у випадку виникнення реальної загрози порушення безпеки при генерації ключових даних або поводженні з ключовими документами;

– складає і подає начальнику АЦСК акти щодо виявлених порушень безпеки при генерації ключових даних або поводженні з ключовими документами, готує рекомендації щодо їхнього усунення;

– проводить службові розслідування у випадках виявлення порушень безпеки при генерації ключових даних або поводженні з ключовими документами;

– готує пропозиції щодо забезпечення АЦСК необхідними технічними і програмними засобами та іншою спеціальною технікою, які дозволені для використання в Україні з метою застосування їх при генерації ключових даних або для роботи з ключовими документами;

– звертається до начальника АЦСК з пропозиціями щодо подання заяви до відповідних державних органів на постачання ключових документів для потреб АЦСК;

– узгоджує умови включення до складу ПТК АЦСК нових компонентів та подає начальнику АЦСК пропозиції щодо заборони їхнього включення, якщо вони становлять небезпеку або зменшують рівень захищеності при генерації ключових даних або поводженні з ключовими документами;

– надає висновки з питань, які стосуються забезпечення безпеки при генерації ключових даних або поводженні з ключовими документами;

– зобов'язаний переглядати журнали аудиту, що ведуться ПТК АЦСК з метою виявлення сукупності подій (серед зареєстрованих у журналі аудиту), які свідчать про ситуацію, яка призвела або може призвести до порушень безпеки експлуатації комплексу;

– звертається до начальника АЦСК з пропозиціями щодо узгодження планів і регламенту відвідування приміщень, в яких здійснюється генерація ключових даних або іде робота з ключовими документами, сторонніми особами.

– організовує забезпечення повноти та якісного виконання організаційно-технічних заходів з захисту інформації при генерації ключових даних та поводженні з ключовими документами;

– перевіряє відповідність нормативних документів щодо їх відповідності вимогам цього документу, здійснює контроль за виконанням цих вимог;

– вчасно і в повному обсязі доводить до персоналу АЦСК інформацію, яка їх стосується, щодо захисту ключових даних при їх генерації та ключових документів при поводженні з ними;

– здійснює контрольні перевірки стану захищеності ключових даних при їх генерації та ключових документів при поводженні з ними;

– забезпечує конфіденційність робіт з монтажу, експлуатації та технічного обслуговування засобів, що використовуються в ПТК АЦСК при генерації ключових даних або поводженні з ключовими документами;

– сприяє і, у разі необхідності, бере безпосередню участь у проведенні уповноваженими органами перевірок стану захисту ключових даних при їх генерації та ключових документів при поводженні з ними.

11.2.1.3 Адміністратор сертифікації:

– під контролем начальника АЦСК та адміністратора безпеки здійснює формування та знищення особистого ключа АЦСК і його резервної копії;

– надає начальнику АЦСК повну та дійсну інформацію, необхідну для формування сертифіката відкритого ключа АЦСК засвідчувальним органом;

– отримує від адміністратора безпеки носій особистого ключа АЦСК та застосовує особистий ключ АЦСК під контролем адміністратора безпеки для накладання електронного цифрового підпису на сертифікати (для формування сертифікатів) та на інформацію про статус сертифіката (для формування списків відкликаних сертифікатів);

– звертається до адміністратора безпеки у встановленому порядку з питань щодо необхідності здійснення формування, скасування, блокування або поновлення сертифіката відкритого ключа АЦСК;

– інформує начальника АЦСК та адміністратора безпеки про події, що трапилися до закінчення строку чинності сертифіката відкритого ключа АЦСК, а саме:

- компрометацію особистого ключа;
- втрату контролю щодо особистого ключа АЦСК через компрометацію коду доступу до носія особистого ключа;
- виявлену неточність або зміну даних, зазначених у сертифікаті АЦСК.

11.2.1.4 Адміністратор реєстрації:

– здійснює перевірку законності звернень про блокування, поновлення та скасування сертифікатів і відповідає;

– відповідає за обробку отриманих від заявників (підписувачів) заяв на формування, скасування, блокування та поновлення сертифікатів ключів і засвідчує ЕЦП, використовуючи свій особистий ключ, дані заявок;

– здійснює генерацію особистих та відкритих ключів підписувачів та вжиття заходів щодо забезпечення безпеки інформації під час генерації;

– надає допомогу заявникам під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення та вживання заходів щодо забезпечення безпеки інформації під час генерації;

– інформує адміністратора безпеки, про події, що трапилися до закінчення строку чинності сертифіката відкритого ключа адміністратора реєстрації, а саме:

- компрометацію особистого ключа;
- втрату контролю щодо особистого ключа АЦСК через компрометацію коду доступу до носія особистого ключа адміністратора реєстрації;
- виявлену неточність або зміну даних, зазначених у сертифікаті відкритого ключа адміністратора реєстрації.

11.2.1.5 Оператор реєстрації:

– здійснює встановлення осіб, які звернулися до АЦСК з метою формування сертифіката;

– забезпечує підготовку договорів про надання послуг ЕЦП та інших супутніх документів;

– забезпечує отримання від заявників (підписувачів) заяв на формування, скасування, блокування та поновлення сертифікатів ключів;

– забезпечує надання заявникам (підписувачам) консультацій щодо умов та порядку надання послуг ЕЦП.

11.2.1.6 Системний адміністратор:

– організує експлуатацію та технічне обслуговування інформаційно-телекомунікаційної системи АЦСК;

– веде моніторингу функціонування інформаційно-телекомунікаційної системи АЦСК;

– відновлює інформаційно-телекомунікаційної системи АЦСК після збоїв та відмов;

– підтримує електронний інформаційний ресурс АЦСК;

– бере участь у забезпеченні функціонування комплексної системи захисту інформації;

– формує та веде резервні копії конфігурацій загальносистемного та спеціального програмного забезпечення ПТК;

– контролює архівацію та відновлення реєстру сформованих сертифікатів;

– забезпечує актуальність еталонних, архівних і резервних копій реєстрів сертифікатів, що створюються в АЦСК, передачу їх на зберігання;

– відповідає за адміністрування антивірусного програмного забезпечення, забезпечення актуальності антивірусних баз.

11.2.2 Права та обов'язки СЗІ:

До складу служби захисту інформації входять:

– начальник СЗІ;

– адміністратор безпеки.

СЗІ:

– забезпечує повноту та якісне виконання організаційно-технічних заходів із захисту інформації;

– розробляє розпорядчі документи, згідно з якими в АЦСК повинен забезпечуватися захист інформації, контролює їх виконання;

– своєчасно реагує на спроби несанкціонованого доступу до ресурсів ПТК АЦСК, порушення правил експлуатації засобів захисту інформації;

– контролює зберігання особистого ключа АЦСК та його резервної копії, особистих ключів посадових осіб АЦСК;

– бере участь у знищенні особистого ключа АЦСК, здійснює контроль за правильним і своєчасним знищенням посадовими особами особистих ключів;

– веде контроль за процесом резервування сертифікатів ключів та списків відкликаних сертифікатів, а також інших важливих ресурсів;

– організує розмежування доступу до ресурсів ПТК АЦСК, зокрема розподілення між посадовими особами паролів, ключів, сертифікатів тощо;

– забезпечує спостереження (реєстрація та аудит подій в ПТК АЦСК, моніторинг подій тощо) за функціонуванням комплексної системи захисту інформації;

– забезпечує організацію та проведення заходів з модернізації, тестування, оперативного відновлення функціонування комплексної системи захисту інформації після збоїв, відмов та аварій ПТК.

11.2.3 Права та обов’язки ВПР:

ВПР створюються при необхідності провадження сервісу АЦСК у територіально віддалених від центрального офісу районах.

Права та обов’язки ВПР визначені у пунктах 2.1.5 та 2.1.6.

11.3 Порядок ведення журналів аудиту інформаційно-телекомунікаційної системи АЦСК

11.3.1 Типи подій, що фіксуються у журналах аудиту

ПТК АЦСК налаштований на реєстрацію наступних подій:

– спроб створення, знищення, встановлення пароля, зміни прав доступу, системних привілеїв тощо у ПТК;

– заміни ключів;

– формування, блокування, скасування та поновлення сертифікатів ключів, а також формування списків відкликаних сертифікатів;

– спроб несанкціонованого доступу до ПТК;

– надання доступу до ПТК персоналу АЦСК;

– збоїв у роботі ПТК.

Параметри реєстрації подій в ПТК АЦСК:

– дата, час, тип події, результат (успішність/неуспішність) події;

– ідентифікатор підписувача (процесу), що ініціював подію.

11.3.2 Частота перегляду журналів аудиту

Журнали аудиту, що ведуться в ПТК АЦСК, переглядаються адміністратором безпеки періодично, але не рідше одного разу на добу з метою виявлення сукупності подій (серед зареєстрованих у журналі аудиту), які свідчать про ситуацію, яка призвела або може призвести до порушення безпеки експлуатації комплексу.

11.3.3 Строки зберігання журналів аудиту

Журнали аудиту, що ведуться в ПТК АЦСК, зберігаються не менше 5-х років від дати останньої події.

11.3.4 Порядок захисту та резервного копіювання журналів аудиту

Резервні копії журналів аудиту на відокремлюваних носіях зберігаються в окремому приміщенні із забезпеченням їх захисту від несанкціонованого доступу.

Резервне копіювання журналів аудиту здійснюється раз на добу (на резервний сервер АЦСК), резервне копіювання журналів аудиту на відокремлювані носії здійснюється раз на тиждень.

Резервування здійснюється системним адміністратором відповідними засобами, що входять до складу операційної системи ПЕОМ, системи керування базами даних та засобами ПТК АЦСК, під контролем та за участю адміністратора безпеки. Факти проведення резервування у АЦСК протоколюються (за період) та засвідчуються підписами відповідальних осіб.

Управління доступом до резервних копій журналів аудиту та контроль за їх зберіганням та застосуванням здійснює адміністратор безпеки.

11.3.5 Перелік посад, що можуть здійснювати перегляд журналів аудиту

Перегляд журналів аудиту, що ведуться в ПТК АЦСК, дозволяється здійснювати лише начальнику АЦСК та адміністратору безпеки.

11.4 Порядок ведення архівів

11.4.1 Перелік конфіденційної та відкритої інформації, що обробляється в АЦСК

До конфіденційної інформації, що обробляється у АЦСК, віднесено:

– особисті ключі АЦСК (в тому числі, послуг фіксування часу та адміністратора реєстрації);

– персональні дані підписувачів, що надаються в АЦСК та не підлягають безпосередньому розповсюдженню в складі сертифіката відкритого ключа;

– конфігурація технічних та програмних засобів ПТК АЦСК;

– зміст журналів аудиту ПТК АЦСК;

– документи, які циркулюють в АЦСК.

Особистий ключ підписувача є конфіденційною інформацією підписувача.

Захист персональних даних підписувачів забезпечується шляхом застосування:

– організаційних заходів з формування, обліку та зберігання справ заявників, призначення відповідальної особи за зберігання цих справ, обмеження доступу обслуговуючого персоналу до приміщення (шаф), де вони зберігаються;

– організаційно-технічних та технічних заходів, реалізованих комплексною системою захисту інформації автоматизованої системи АЦСК, у тому числі, використанням надійних засобів ЕЦП, веденням журналів роботи системи у захищеному вигляді, розмежуванням та контролем за інформаційними потоками між внутрішньою локальною мережею АЦСК та підсистемою відкритого доступу, застосуванням антивірусних засобів, міжмережевих екранів тощо.

Інформація, що не є конфіденційною інформацією, вважається відкритою інформацією.

Інформація, що включається в сертифікати відкритих ключів підписувачів (у разі згоди заявників, до яких вони відносяться) та списки відкликаних сертифікатів, що випущені АЦСК, не вважається конфіденційною.

Відкрита інформація може публікуватися за рішенням АЦСК. Місце, спосіб і час публікації відкритої інформації визначається АЦСК.

11.4.2 Типи документів та даних, що підлягають архівуванню

Архівному зберіганню підлягають наступні документи АЦСК:

– справи підписувачів з укладеними договорами та іншими документами (завіреними в установленому порядку копіями документів), що використовуються під час їх реєстрації;
– сертифікати відкритих ключів АЦСК (в електронному вигляді);
– сертифікати посадових осіб АЦСК (в електронному вигляді);
– сертифікати відкритих ключів підписувачів (в електронному вигляді);
– заяви на скасування (блокування, поновлення) сертифікатів підписувачів;
– службові документи АЦСК, у тому числі журнали аудиту ПТК тощо.

11.4.3 Строки зберігання архівів

Документи АЦСК на паперових носіях, що підлягають архівному зберіганню, є документами тимчасового зберігання. Термін зберігання архівних документів в АЦСК – 5 (п’ять) років.

Сертифікати відкритих ключів АЦСК, сертифікати відкритих ключів посадових осіб АЦСК та сертифікати ключів підписувачів, а також списки відкликаних сертифікатів зберігаються безстроково.

11.4.4 Механізми та порядок зберігання, захисту та знищення архівних документів

Документи АЦСК на паперових носіях, у тому числі сертифікати відкритих ключів підписувачів, зберігаються в порядку, встановленому законодавством України про архіви та архівні справи.

Архівні документи в електронному вигляді зберігаються на відокремлюваних носіях в опечатаному системним адміністратором тубусі у сховищі начальника центру сертифікації ключів із забезпеченням їх захисту від несанкціонованого доступу.

Виділення архівних документів до знищення та знищення виконується комісією, яка складається із посадових осіб АЦСК при безпосередній участі начальника АЦСК та адміністратора сертифікації, адміністратора безпеки або уповноважених начальником АЦСК посадових осіб АЦСК. По факту проведення процедури знищення архівних документів складається відповідний акт.

12 УПРАВЛІННЯ КЛЮЧАМИ

12.1 Порядок генерації ключів

12.1.1 Порядок генерації ключів АЦСК

Усі дії, пов’язані з генерацією, використанням та знищенням особистого ключа АЦСК відображаються у Журналі роботи з ключами.

Генерація ключів АЦСК здійснюється у захищеній (екранованій) шафі, яка відповідає вимогам Правил посиленої сертифікації, що унеможливлює витік відомостей про зміст особистого ключа за рахунок побічних електромагнітних випромінювань та наведень.

Перед генерацією ключів АЦСК усі відповідні засоби ПТК АЦСК повинні бути встановлені та пройти тестування в установленому порядку.

Генерація ключів АЦСК, введення даних, необхідних для створення запиту на формування сертифіката відкритого ключа АЦСК, здійснюється адміністратором сертифікації у присутності начальника АЦСК та під контролем адміністратора безпеки.

Відразу після генерації ключів АЦСК автоматично створюється (у електронному вигляді) запит на формування сертифіката відкритого ключа АЦСК, що містить дані (в тому числі, значення відкритого ключа АЦСК), підписані особистим ключем АЦСК, необхідні для формування засвідчувальним органом сертифіката АЦСК. Далі цей запит використовується при підготовці документів для сертифікації відкритого ключа АЦСК в ЦЗО.

Згенероване значення особистого ключа АЦСК розміщується у зашифрованому вигляді в базі даних ПТК АЦСК на жорсткому диску серверу АЦСК або на захищеному знімному носії ключової інформації, а також записується його резервна копія у зашифрованому вигляді на знімний носій ключової інформації або на захищений знімний носій ключової інформації, після чого копія особистого ключа АЦСК, що знаходиться в запам’ятовуючих пристроях серверу АЦСК, знищується.

Системний адміністратор під контролем адміністратора безпеки перевіряє факт знищення копії особистого ключа АЦСК в запам’ятовуючих пристроях серверу АЦСК. Застосовувати особистий ключ АЦСК, якщо виникали збої (помилки) при знищенні його копії на сервері АЦСК, забороняється.

Після формування сертифікату відкритого ключа АЦСК він опубліковується на електронному інформаційному ресурсі АЦСК.

Адміністратор сертифікації під контролем адміністратора безпеки вводить значення коду доступу до особистого ключа таким чином, щоб ніхто не мав можливості з ним ознайомитися.

Код доступу до особистого ключа АЦСК, повинен бути відомий лише адміністратору сертифікації.

Адміністратор сертифікації записує (таким чином, щоб не допустити ознайомлення з ним інших осіб) на аркуші паперу значення коду доступу до особистого ключа АЦСК, вміщує цей аркуш в непрозорий конверт, надписує його, опечатує конверт разом з адміністратором безпеки та передає на зберігання начальнику АЦСК.

Не менше ніж за один календарний рік до закінчення строку дії поточного особистого ключа АЦСК переходить на застосування нового особистого ключа АЦСК завчасно згенерованого та сертифікованого в ЦЗО.

12.1.2 Порядок запису резервної копії особистого ключа АЦСК на знімний носій ключової інформації або на захищений знімний носій ключової інформації

Запис резервної копії особистого ключа АЦСК у зашифрованому вигляді на знімний носій ключової інформації або на захищений знімний носій ключової інформації здійснюється адміністратором сертифікації засобами ПТК АЦСК.

Адміністратор сертифікації під контролем адміністратора безпеки вводить значення коду доступу до зйомного носія ключової інформації або до захищеного зйомного носія ключової інформації, на якому розміщується резервна копія особистого ключа АЦСК, таким чином, щоб ніхто не мав можливості з ним ознайомитися, після чого цей носій вміщується в тубус (контейнер), який запечатується адміністратором сертифікації.

Код доступу до знімного носія ключової інформації або захищеного знімного носія ключової інформації, який містить резервну копію особистого ключа АЦСК, повинен бути відомий лише адміністратору сертифікації.

Адміністратор сертифікації записує (таким чином, щоб не допустити ознайомлення з ним інших осіб) на аркуші паперу значення коду доступу до знімного носія ключової інформації або захищеного знімного носія ключової інформації, що містить резервну копію особистого ключа АЦСК, вміщує цей аркуш в непрозорий конверт, надписує його, опечатує конверт разом з адміністратором безпеки та передає на зберігання начальнику АЦСК.

12.1.3 Порядок генерації ключів послуг фіксування часу та послуг визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP

Генерація ключів послуг фіксування часу та послуг визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP здійснюється засобами ПТК АЦСК в спеціальному приміщенні АЦСК.

Перед генерацією ключів послуг фіксування часу та послуг визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP усі необхідні засоби ПТК АЦСК повинні бути встановлені та пройти тестування в установленому порядку, повинні бути згенеровані ключі АЦСК, для відкритого ключа АЦСК центральним засвідчувальним органом повинен бути сформований сертифікат відкритого ключа АЦСК. Сертифікат відкритого ключа АЦСК має бути чинним на час генерації ключів послуг фіксування часу та послуг визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP, термін чинності сертифіката відкритого ключа послуг фіксування часу не повинен виходити за термін дії сертифіката відкритого ключа АЦСК.

Генерація ключів послуг фіксування часу та послуг визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP здійснюється адміністратором сертифікації у присутності начальника АЦСК та під контролем адміністратора безпеки. Введення даних, необхідних для створення запиту на формування сертифіката відкритого ключа послуг фіксування часу та послуг визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP, здійснюється адміністратором сертифікації у присутності начальника АЦСК та під контролем адміністратора безпеки.

Після генерації ключів послуг фіксування часу та послуг визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP системним адміністратором під контролем адміністратора безпеки здійснюється перевірка правильності атрибутів доступу до каталогу (де міститься файл, що містить особистий ключ послуг фіксування часу або особистий ключ послуг визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP) та атрибутів доступу до файлу, що містить особистий ключ послуг фіксування часу або особистий ключ послуг визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP на сервері АЦСК (атрибути для каталогу повинні надавати право тільки для читання для відповідних засобів ПТК АЦСК, атрибути для файлу, що містить особистий ключ послуг фіксування часу, повинні надавати право тільки для читання його вмісту лише для відповідних засобів ПТК АЦСК).

Відразу після генерації ключів послуг фіксування часу та послуг визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP засобами ПТК АЦСК автоматично створюється запит на формування сертифіката відкритого ключа послуг фіксування часу та сертифіката відкритого ключа послуг визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP (у електронному вигляді). На основі відповідного запиту адміністратор сертифікації у спеціальному приміщенні АЦСК за участю адміністратора безпеки засобами ПТК АЦСК формує сертифікат послуг визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP.

Сертифікат послуг фіксування часу формується відповідно до вимог чинного законодавства.

12.1.4 Порядок генерації ключів підписувачів

Порядок генерації ключів підписувача наведено в п. 10.1.2.

12.2 Процедури надання особистого ключа після генерації його власнику та

механізм надання відкритого ключа підписувача для сертифікації

Опис процедур надання особистого ключа після генерації його власнику та механізм надання відкритого ключа підписувача для сертифікації наведені в п. 10.1.2 та п. 10.2.

13 ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ОСОБИСТОГО КЛЮЧА АЦСК

13.1 Порядок захисту та доступу до особистого ключа АЦСК

Особистий ключ АЦСК зберігається у зашифрованому вигляді в базі даних ПТК АЦСК на жорсткому диску серверу ЦСК або на захищеному знімному носії ключової інформації, який під'єднаний до серверу ЦСК, а резервна копія особистого ключа АЦСК розміщується на знімному носії ключової інформації або на захищеному знімному носії ключової інформації.

Для застосування особистого ключа АЦСК необхідно ввести код доступу до нього.

Особистий ключ АЦСК застосовується лише у захищеній (екранованій) шафі в спеціальному приміщенні АЦСК двома посадовими особами АЦСК: адміністратором сертифікації в присутності адміністратором безпеки.

13.2 Порядок резервного копіювання особистого ключа АЦСК, порядок доступу та використання резервної копії особистого ключа АЦСК

Порядок резервного копіювання особистого ключа АЦСК наведено в п. 12.1.2.

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

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

13.3 Умови зберігання ключів АЦСК

Особистий ключ розміщується у зашифрованому вигляді в базі даних ПТК АЦСК на жорсткому диску серверу АЦСК або на захищеному знімному носії ключової інформації та постійно знаходиться у захищеній (екранованій) шафі, яка відповідає вимогам Правил посиленої сертифікації.

Запечатаний та надписаний конверт із значенням коду доступу до особистого ключа АЦСК, опечатаний адміністратором сертифікації та адміністратором безпеки, зберігається у сейфі начальника АЦСК.

Запечатаний та надписаний конверт (тубус, контейнер), із знімним носієм ключової інформації або з захищеним знімним носієм ключової інформації, що містить резервну копію особистого ключа АЦСК, опечатаний адміністратором сертифікації, зберігається у захищеній (екранованій) шафі, яка відповідає вимогам Правил посиленої сертифікації.

Запечатаний та надписаний конверт із значенням коду доступу до знімного носія ключової інформації або до захищеного знімного носія ключової інформації, що містить резервну копію особистого ключа АЦСК, опечатаний адміністратором сертифікації та адміністратором безпеки, зберігається у сейфі начальника АЦСК.

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

14 ПОРЯДОК НАДАННЯ ПОСЛУГ ФІКСУВАННЯ ЧАСУ

14.1 TSP система надає послугу фіксування часу що відповідає умовам та вимогам до процедури засвідчення наявності електронного документа відповідно до постанови Кабінету Міністрів від 26 травня 2004 № 680 «Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу».

14.2. Послуга фіксування часу надається цілодобово.