Товариство з обмеженою відповідальністю "КЛЮЧОВІ СИСТЕМИ"

РЕГЛАМЕНТ
роботи акредитованого центру сертифікації ключів товариства з обмеженою відповідальністю "КЛЮЧОВІ СИСТЕМИ"

{Із змінами, внесеними згідно з Наказом ТОВ "КС" № 78 від 07.07.2016}

ЗМІСТ

Визначення термінів

Для даного Регламенту поняття, наявні в ньому, використовуються у такому значенні:

OCSP	–	Online Certificate Status Protocol, протокол інтерактивного визначення статусу сертифіката
TSP	–	Time Stamp Protocol, протокол фіксування часу
АС	–	автоматизована система
АЦСК	–	(акредитований) центр сертифікації ключів товариства з обмеженою відповідальністю "КЛЮЧОВІ СИСТЕМИ"
БД	–	база даних
ВПР	–	відокремлений пункт реєстрації
ЕЦП	–	електронний цифровий підпис
заявник	–	фізична або юридична особа, яка звертається до АЦСК з метою отримання послуг ЕЦП на підставі відповідного договору укладеного між заявником та АЦСК
КЗІ	–	криптографічний захист інформації
користувач	–	особа, яка використовує надійні засоби ЕЦП, посилені сертифікати відкритих ключів та дані про статус сертифікатів для перевірки ЕЦП та/або для узгодження ключів при роботі з криптографічними повідомленнями
КСЗІ	–	комплексна система захисту інформації
НСД	–	несанкціонований доступ
підписувач	–	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)
ПТК	–	програмно - технічний комплекс
сертифікат	–	посилений сертифікат відкритого ключа
СУБД	–	система управління базами даних
ТЗІ	–	технічний захист інформації
Товариство	–	ТОВ "КС"

Інші терміни, що вживаються в цьому Регламенті, застосовуються в значеннях, визначених нормативно-правовими актами, що регулюють відносини, які виникають у сфері ЕЦП.

1 Загальні положення

1.1 Статус Регламенту

Цей Регламент роботи акредитованого центру сертифікації ключів (далі – Регламент) визначає порядок та процедури обслуговування посилених сертифікатів відкритих ключів підписувачів, умови надання та правила користування послугами АЦСК, загальні організаційні, технічні та інші умови діяльності АЦСК під час надання послуг ЕЦП.

Регламент розроблено в відповідності до чинного законодавства України, яке регулює питання в сфері електронного цифрового підпису, а саме:

– Закону України «Про електронний цифровий підпис» від 22.05.2003 р. № 852-IV;

– Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу, затвердженому постановою Кабінету Міністрів України від 26 травня 2004 р. № 680;

– Порядку акредитації центру сертифікації ключів, затвердженому постановою Кабінету Міністрів України від 13 липня 2004 р. № 903;

– Порядку обов’язкової передачі документованої інформації, затвердженому постановою Кабінету Міністрів України від 28 жовтня 2004 р. №1454;

– Правил посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України № 3 від 13 січня 2005 р., зареєстрованим в Міністерстві юстиції України 27 січня 2005 р. за № 104/10384, у редакції наказу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України № 50 від 10 травня 2006 р., зареєстрованого в Міністерстві юстиції України 17 травня 2006 р. за № 568/12442.

Будь-яка зацікавлена особа може ознайомитися з Регламентом на електронному ресурсі або в АЦСК чи його відокремленому пункті реєстрації.

1.2 Застосування Регламенту

Дія Регламенту поширюється на АЦСК, відокремлені пункти реєстрації та користувачів послуг ЕЦП, що надаються АЦСК: юридичних осіб публічного та приватного права всіх форм власності, фізичних осіб – суб’єктів підприємницької діяльності, фізичних осіб – громадян України, осіб без громадянства, іноземців.

Норми даного Регламенту є обов'язковими для заявників (підписувача) та АЦСК з моменту подачі заявником (підписувачем) заяви на сертифікацію до АЦСК.

Вимоги даного Регламенту застосовуються протягом строку дії договору про надання послуг ЕЦП, якщо інше не зазначено у Регламенті.

АЦСК має право визначати обсяг положень Регламенту або інших документів, з якими необхідно ознайомлювати користувачів.

1.3 Порядок внесення змін та доповнень до Регламенту

АЦСК має право в односторонньому порядку вносити зміни та доповнення до Регламенту у встановленому законодавством порядку. Повідомлення про внесення змін та доповнень до Регламенту, а також уточнена редакція Регламенту розміщуються на електронному інформаційному ресурсі АЦСК не пізніше ніж за 10 (десять) робочих днів до вступу змін та доповнень у дію.

Усі зміни та доповнення, що вносяться до Регламенту в зв'язку із змінами законодавства, вступають у силу одночасно із змінами та доповненнями до відповідних нормативних актів.

Усі зміни та доповнення до Регламенту, з моменту їх вступу в дію, однаково поширюються на всіх підписувачів АЦСК, що приєдналися до Регламенту, в тому числі і на тих, що приєдналися до Регламенту раніше за дату вступу в дію змін та доповнень.

Якщо, підписувач АЦСК не згоден із внесеними змінами та доповненнями, він має право припинити використання посиленого сертифіката відкритого ключа.

1.4 Ідентифікаційні дані АЦСК

Повне найменування:	акредитований центр сертифікації ключів товариства з обмеженою відповідальністю "КЛЮЧОВІ СИСТЕМИ"
Скорочене найменування:	АЦСК ТОВ "КС"
ЄДРПОУ:	39034634
Місцезнаходження (поштова адреса):	02121, м. Київ, вул. Харківське шосе, 201-203, під'їзд 2, пов. 7
Номери телефонів:	(044) 538-15-93
Факс:	(044) 538-15-93
Електронна адреса електронного інформаційного ресурсу (веб-сайт):	ksystems.com.ua
Адреса електронної пошти (e-mail):	info@ksystems.com.ua

2 Перелік суб'єктів, задіяних в обслуговуванні і використанні сертифікатів та їх функції

Сукупність суб'єктів, що задіяні в обслуговуванні та використанні сертифікатів, складає інфраструктуру відкритих ключів. Інфраструктура відкритих ключів включає в себе:

– АЦСК;
– ВПР;
– підписувачів;
– користувачів.

2.1 АЦСК

АЦСК здійснює свою діяльність у сфері електронного документообігу, застосування ЕЦП органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності, іншими суб’єктами господарської діяльності та фізичними особами на договірних засадах.

Перелік послуг ЕЦП, що надаються АЦСК:

– реєстрація заявників;
– допомога під час генерації особистих та відкритих ключів;
– обслуговування сертифікатів (формування, розповсюдження, скасування, зберігання, блокування та поновлення);
– надання підписувачам надійних засобів ЕЦП;
– управління статусом сертифікатів та розповсюдження інформації про статус сертифікатів;
– надання послуги фіксування часу;
– надання послуги інтерактивного визначення статус сертифіката.

Окрім надання послуг ЕЦП, АЦСК надає консультаційні послуги за зверненнями підписувачів.

Надання зазначених послуг здійснюється АЦСК у відповідності до цього Регламенту та на підставі укладених договорів або договорів приєднання, укладених шляхом прийняття заяви-приєднання.

АЦСК надає послуги та здійснює діяльність на підставі свідоцтва про акредитацію.

2.2 Відокремлені пункти реєстрації (ВПР)

{Назва пункту 2.2 із змінами, внесеними згідно з Наказом ТОВ "КС" № 78 від 07.07.2016}

ВПР є відособленими підрозділами АЦСК без правового статусу юридичної особи, що реалізують функції АЦСК з реєстрації підписувачів та їх подальшого обслуговування на певній території.

Окрім надання послуг ЕЦП, ВПР надає консультаційні послуги за зверненнями підписувачів.

Безпосереднє управління ВПР здійснюється АЦСК.

2.3 Підписувачі та користувачі

Послугами АЦСК користуються підписувачі та інші користувачі.

Підписувачі мають договірні відносини з АЦСК, на законних підставах володіють особистими ключами, мають відповідні відкриті ключі та сформовані АЦСК сертифікати.

У договорі про надання послуг повинно бути зазначено:

– обов’язки сторін, у тому числі щодо обов’язковості використання надійних засобів ЕЦП;

– умови надання доступу користувачам до сертифіката підписувача (умови публікації сертифіката – згоди або не згоди підписувача надавати вільний доступ користувачам до його сертифіката).

Підписувачами можуть бути:

– фізичні особи, у тому числі посадові особи та наймані працівники;

– фізичні особи-підприємці;

– юридичні особи, у тому числі органи державної влади, органи місцевого самоврядування у випадках, встановлених законодавством.

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.

3 Сфера використання сертифікатів

Сертифікати, сформовані АЦСК, використовуються для засвідчення чинності та належності відкритого ключа підписувачу.

АЦСК здійснює обслуговування сертифікатів, сформованих для органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій всіх форм власності, фізичних осіб, не залежно від сфери їх використання.

Сферою використання сертифікатів, сформованих АЦСК, є організація електронного документообігу з використанням ЕЦП.

3.1 Обмеження щодо використання сертифікатів

АЦСК має право встановлювати обмеження сфери використання сформованих ним сертифікатів. Обмеження щодо використання сформованих АЦСК сертифікатів застосовуються у відповідності до положень цього Регламенту та діючого законодавства України.

Інформація щодо обмеження сфери або сфер використання сертифіката доводиться до заявника (підписувача) та зазначається у сформованому АЦСК сертифікаті.

3.2 Терміни дії сертифікатів

Термін дії сертифіката АЦСК, відповідний якому особистий ключ призначений для формування сертифікатів підписувачів, сертифікатів посадових осіб АЦСК, сертифікатів серверів АЦСК, не може перевищувати 5 років.

Термін дії сертифікатів серверів АЦСК не може перевищувати терміну дії сертифіката АЦСК.

Термін дії сертифіката підписувача та сертифікатів посадових осіб АЦСК не може перевищувати 2 роки. Після закінчення терміну дії свого сертифіката підписувач зобов’язаний знищити всі наявні копії особистого ключа.

Після закінчення терміну дії сертифіката, сертифікат вважається не дійсним.

4 Порядок розповсюдження (публікації) інформації

4.1 Інформаційний ресурс АЦСК

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

– довідкову інформацію (режими роботи АЦСК, положення Регламенту, нормативні документи, договори на надання послуг, форми заяв тощо);
– сертифікат АЦСК;
– сертифікати серверів АЦСК;
– сертифікати підписувачів;
– списки відкликаних сертифікатів, що містять інформацію про статуси сертифікатів серверів АЦСК та підписувачів.

Електронна адреса (DNS-ім'я) електронного інформаційного ресурсу: *ksystems.com.ua*.

Технічною основою інформаційного ресурсу АЦСК є сервери взаємодії, що входять до складу ПТК АЦСК.

Довідкова інформація розміщується на HTTP-сервері сервера взаємодії у вигляді набору web-сторінок.

Сертифікат АЦСК, сертифікати серверів АЦСК та підписувачів, а також списки відкликаних сертифікатів розміщуються:

у складі web-сторінок на HTTP-сервері сервера взаємодії;

у інформаційному дереві LDAP-каталогу на LDAP-сервері сервера взаємодії.

Доступ до HTTP-сервера здійснюється за DNS-ім'ям *ksystems.com.ua* за протоколом HTTP.

4.2 Порядок публікації сертифіката АЦСК та сертифікатів серверів АЦСК

Після формування сертифіката АЦСК виконується його публікація на інформаційному ресурсі.

Окрім власного сертифіката АЦСК виконується публікація сертифікатів серверів АЦСК:

- сервера обробки запитів (CMP-сервера);
- сервера позначок часу (TSP-сервера);
- сервера визначення статусу сертифікатів (OCSP-сервера).

Публікація сертифікатів серверів АЦСК виконується після формування сертифіката відповідного сервера.

4.3 Порядок публікації сертифікатів підписувачів

Публікація сертифікатів підписувачів на інформаційний ресурс АЦСК здійснюється за згодою заявників (підписувачів). Інформація про необхідність публікації сертифікатів кожного окремого підписувача вноситься в склад реєстраційних даних під час реєстрації підписувача.

4.4 Порядок публікації списків відкликаних сертифікатів

Публікація списків відкликаних сертифікатів на інформаційний ресурс АЦСК (на HTTP-сервері) здійснюється одразу після його випуску.

АЦСК виконує випуск списків відкликаних сертифікатів двох типів:

- повний список;
- частковий список.

Повний список випускається 1 (один) раз на тиждень та містить інформацію про всі відкликані сертифікати, які були сформовані АЦСК на діючому особистому ключеві.

Частковий список випускається кожні 2 (дві) години та містить інформацію про всі відкликані сертифікати, статус яких був змінений в

інтервалі між часом випуску останнього повного списку та часом формування поточного часткового списку.

Списки відкликаних сертифікатів (повний та частковий) чинні до випуску нових відповідних списків.

5 Порядок ідентифікації та автентифікації

5.1 Реєстрація заявника (підписувача)

5.1.1 Загальні положення

Бланки документів встановленої форми, що використовуються під час реєстрації заявників, розміщуються на інформаційному ресурсі АЦСК.

Процедура реєстрація заявника (підписувача) виконується тільки у робочий час в АЦСК або у ВПР на підставі заявки на сертифікацію.

Для проведення процедури реєстрації заявник (підписувач) надає до АЦСК (ВПР) пакет необхідних документів. Документи приймаються АЦСК (ВПР):

1) за особистої доставки заявником – за наявності паспорта (пред'являється);

2) за особистої доставки довіреною особою – за наявності паспорта (пред'являється) і довіреності встановленої форми (надається). Довіреність повинна бути засвідчена в встановленому порядку:

– для юридичних осіб (представників юридичних осіб) та фізичних осіб-підприємців – печаткою організації та особистим підписом, у разі відсутності печатки в фізичної особи-підприємця – нотаріально;

– для фізичних осіб – нотаріально;

3) засобами кур'єрської доставки кореспонденції (поштовим відправленням із використанням послуг операторів поштового зв'язку, що здійснюють кур'єрську доставку) у вигляді закритого, непошкодженого пакету, який разом із документами містить обов'язковий супроводжувальний лист із описом вмісту пакету (перелік документів у пакеті). Супровідний лист повинен бути засвідчений у встановленому порядку:

– для фізичних осіб – власноручним підписом,

– для фізичних осіб-підприємців – підписом та, у разі наявності, печаткою фізичної особи-підприємця,

– для юридичних осіб (представників юридичних осіб) – підписом керівника та печаткою юридичної особи.

5.1.2 Встановлення особи заявника

Працівники АЦСК, на яких покладено обов’язки адміністраторів реєстрації чи треті особи, що здійснюють представництво АЦСК і на яких відповідно до законодавства покладено функції щодо ідентифікації фізичних та юридичних осіб в порядку, передбаченому Цивільним кодексом України, при укладанні договорів про надання послуг електронного цифрового підпису, уповноважені здійснювати в інтересах АЦСК виключно процедуру встановлення, ідентифікації заявників відповідно до вимог законодавства у сфері електронного цифрового підпису, із покладанням на них відповідальності за невиконання чи неналежне виконання своїх обов’язків згідно чинного законодавства, здійснюють процедуру встановлення особи заявника, що проходить процедуру реєстрації:

{Абзац 1 пункту 5.1.2 із змінами, внесеними згідно з Наказом ТОВ "КС" № 78 від 07.07.2016}

– встановлення юридичної особи здійснюється за оригіналами або нотаріально засвідченими копіями установчих документів такої особи (виключно для ознайомлення) та копії документа про державну реєстрацію юридичної особи у єдиному державному реєстрі підприємств та організацій України, що засвідчена нотаріально або печаткою такої особи та підписом керівника. Крім цього, під час реєстрації встановлюється представник юридичної особи та його повноваження;

– встановлення представника юридичної особи здійснюється за документами, що підтверджують належність підписувача до юридичної особи-заявника, а саме: паспортом такої особи або за копією паспорту, засвідченою власноручним підписом особи-працівника юридичної особи та підписом керівника і печаткою юридичної особи, а також копією наказу (рішення, протоколу тощо) про прийняття на роботу такої фізичної особи та наказу (рішення, протоколу тощо) про надання повноважень на представництво юридичної особи, що засвідчені підписом керівника та печаткою юридичної особи;

– встановлення фізичної особи-підприємця здійснюється за наявності паспорта такої особи або за копією паспорту, засвідченою власноручним підписом фізичної особи та печаткою фізичної особи-підприємця (за наявності), а також за оригіналами документів такої особи про державну реєстрацію фізичної-особи підприємця, або копіями таких документів, які нотаріально посвідчені відповідно до законодавства (виключно для ознайомлення). Крім цього, під час реєстрації встановлюється представник фізичної особи-підприємця та його повноваження;

– встановлення представника фізичної особи-підприємця здійснюється за документами, що підтверджують належність підписувача до фізичної особи-

підприємця, а саме: паспортом такої особи або за копією паспорту, засвідченою власноручним підписом особи-працівника фізичної особи-підприємця та підписом керівника і печаткою (у разі наявності) фізичної особи-підприємця, а також копією наказу (рішення, протоколу тощо) про прийняття на роботу такої фізичної особи та наказу (рішення, протоколу тощо) про надання повноважень на представництво фізичної особи-підприємця, що засвідчені підписом керівника та печаткою (у разі наявності) фізичної особи-підприємця;

– встановлення фізичної особи здійснюється за паспортом (або іншим документом відповідно до законодавства України) такої особи або за копією паспорту (або іншого документа відповідно до законодавства України), засвідченою власноручним підписом та за підписом у заявці на проведення сертифікації, засвідченим нотаріально.

5.1.3 Перевірка наданих документів

Надані заявником документи розглядаються протягом 1 (однієї) години з моменту їх надходження.

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

За результатом розгляду наданих документів адміністратор реєстрації приймає рішення про відмову в реєстрації в разі:

– порушення цілісність конверта з носієм інформації, що містить електронний запит на сертифікацію, в разі подання документів через довірену особу чи засобами кур'єрської доставки кореспонденції;

– відсутності всіх необхідних для реєстрації документів;

– подання неналежно засвідчених копій документів;

– встановлення невідповідності даних, що визначені наданими документами, фактичним.

У випадку відмови в реєстрації, надані документи повертаються заявнику (довіреній особі) з позначкою адміністратора реєстрації про підстави відмови на заявці на сертифікацію.

При ухваленні позитивного рішення та виконання заявником необхідних умов надання послуг ЕЦП (попередня оплата, внесення авансу, подання додаткових документів тощо) адміністратор реєстрації виконує дії по занесенню реєстраційної інформації до реєстру користувачів АЦСК.

Всі документи, що були надані заявникам під час реєстрації передаються до архіву паперових документів АЦСК.

Реєстрація заявника є підставою для формування сертифіката підписувача.

5.2 Перелік документів, що надаються заявником (підписувачем)

Якщо до сертифіката необхідно внести дані з документів, які не зазначені в переліку, то відповідно засвідчені копії таких документів повинні надаватись додатково.

5.2.1 Фізичні особи не підприємці

Фізичні особи – резиденти України, що використовують послуги ЕЦП в персональному документообігу, надають

– електронний запит на сертифікацію,
– два примірники заявки на сертифікацію,
– копію документу, що засвідчує особу.

Додаткові документи

– копія довідки про присвоєння ідентифікаційного коду ДРФО власника ключа.

Копії документів засвідчуються особистим підписом фізичної особи.

В разі надання документів засобами кур'єрської доставки кореспонденції підписи на заявках на сертифікацію засвідчуються нотаріально.

5.2.2 Фізичні особи-підприємці

Фізичні особи-підприємці надають

– електронний запит на сертифікацію,
– два примірники заявки на сертифікацію,
– копію документа, що засвідчує особу,
– копію документа про державну реєстрацію фізичної особи-підприємця, або інші відомості відповідно до Закону України від 15 травня 2003 року № 755 - IV "Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань" (у редакції Закону України від 26.11.2015 № 835 - VIII).

{Підпункт 4 абзацу 1 пункту 5.2.2 із змінами, внесеними згідно з Наказом ТОВ "КС" № 78 від 07.07.2016}

Додаткові документи

– копія довідки про присвоєння ідентифікаційного коду ДРФО власника ключа;
– копія свідоцтва про реєстрацію платника податку на додану вартість (у разі, якщо особа є платником ПДВ).

Копії документів, крім нотаріально засвідчених, засвідчуються особистим підписом та, у разі наявності, печаткою фізичної особи-підприємця.

Якщо заявником подано оригінал документу, копія такого документу може бути засвідчена працівником АЦСК на якого покладено обов'язки

адміністратора реєстрації чи третьою особою, що здійснює представництво АЦСК.

{Абзац 4 пункту 5.2.2 із змінами, внесеними згідно з Наказом ТОВ "КС" № 78 від 07.07.2016}

В разі надання документів засобами кур'єрської доставки кореспонденції підписи на заявці на сертифікацію засвідчуються печаткою фізичної особи-підприємця, а за відсутності печатки – нотаріально.

5.2.3 Особи, які представляють юридичну особу

Особи, які представляють юридичну особу, надають

– електронний запит на сертифікацію,

– два примірники заявки на сертифікацію,

– копію документа про державну реєстрацію юридичної особи, або інші відомості відповідно до Закону України від 15 травня 2003 року № 755 - IV "Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань" (у редакції Закону України від 26.11.2015 № 835-VIII),

{Підпункт 3 абзацу 1 пункту 5.2.3 із змінами, внесеними згідно з Наказом ТОВ "КС" № 78 від 07.07.2016}

– копії установчих документів юридичної особи,

– копії документів, що наділяють відповідними повноваженнями власника відкритого ключа, що сертифікується,

– копії документів, що підтверджують обрання керівника юридичної особи та його повноваження,

– копії документів, що засвідчують особу керівника установи,

– копії документів, що засвідчують особу власника ключа.

Додаткові документи

– копія довідки про присвоєння ідентифікаційного коду ДРФО власника ключа,

– копія свідоцтва про реєстрацію платника податку на додану вартість (у разі, якщо особа є платником ПДВ).

Копії документів, крім нотаріально засвідчених, засвідчуються підписом керівника та печаткою юридичної особи.

Якщо заявником подано оригінал документу, копія такого документу може бути засвідчена працівником АЦСК на якого покладено обов'язки адміністратора реєстрації чи третьою особою, що здійснює представництво АЦСК.

{Абзац 4 пункту 5.2.3 із змінами, внесеними згідно з Наказом ТОВ "КС" № 78 від 07.07.2016}

В разі надання документів засобами кур’єрської доставки кореспонденції підписи на заявках на сертифікацію засвідчуються підписом керівника та печаткою юридичної особи.

5.2.4 Електронна печатка

Отримання юридичними особами та фізичними особами-підприємцями сертифіката для забезпечення застосування електронної печатки здійснюється в тому ж порядку, що й для ЕЦП. Для формування сертифіката відкритого ключа, що буде використовуватись як електронна печатка, до заявки на сертифікацію необхідно внести ознаку спеціального призначення ЕЦП (в якості електронної печатки).

5.3 Підтвердження володіння заявником (підписувачем) відповідним особистим ключем

Відкритий ключ заявника (підписувача) подається на сертифікацію у вигляді самопідписаного запиту відповідного формату, який засвідчується ЕЦП, сформованим за допомогою відповідного йому особистого ключа. Підтвердження володіння заявником (підписувачем) відповідним особистим ключем здійснюється без розкриття його особистого ключа шляхом перевіряння ЕЦП на запиті за допомогою відкритого ключа, що міститься у запиті.

5.4 Захист персональних даних підписувачів

Захист персональних даних підписувачів забезпечується шляхом вжиття:

– організаційних заходів щодо обліку та зберігання справ підписувачів, зокрема формування справи підписувачів та їх облік, призначення відповідальної особи за зберігання справ підписувачів, обмежений доступ обслуговуючого персоналу до приміщення (шаф), де зберігаються справи підписувачів;

– організаційно-технічних та технічних заходів реалізованих комплексною системою захисту інформації автоматизованої системи АЦСК (далі – КСЗІ), у тому числі: використанням надійних засобів ЕЦП, веденням журналів роботи системи в захищеному вигляді, розмежування та контролю інформаційних потоків між внутрішньою локальною мережею АЦСК та підсистемою відкритого доступу, використанням антивірусних засобів, міжмережних екранів тощо.

5.5 Автентифікація підписувача під час звернення щодо блокування, скасування та поновлення сертифіката

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

– у разі письмового звернення підписувача, законність звернення встановлюється за власноручним підписом та печатки юридичної особи (для юридичних осіб);

– у разі звернення шляхом направлення запиту на блокування або скасування сертифіката в електронному вигляді законність звернення встановлюється шляхом перевірки ЕЦП на запиті за допомогою чинного сертифіката підписувача;

– у разі звернення щодо блокування сертифіката по телефону законність звернення встановлюється за парольною фразою, що вказується підписувачем під час реєстрації.

6 Процедури та механізми, пов'язані з обслуговуванням сертифікатів

6.1 Порядок формування сертифікатів підписувачів

Формування сертифіката підписувача здійснюється після реєстрації підписувача на підставі даних, наданих для реєстрації.

Формат сертифіката відповідає вимогам Закону України "Про електронний цифровий підпис" та Вимогам до формату посиленого сертифіката відкритого ключа, затверджені наказом Мін’юсту, Адміністрації Держспецзв'язку від 20.08.2012 № 1236/5/453, та зареєстровані в Мін’юсті 20.08.2012 за № 1398/21710.

Унікальність відкритого ключа підписувача в реєстрі чинних, блокованих та скасованих сертифікатів, унікальність розпізнавального імені підписувача та унікальність реєстраційного номеру сертифіката в межах АЦСК забезпечується адміністратором реєстрації за допомогою засобів ПТК ЦСК.

Якщо процедуру реєстрації виконано успішно, адміністратор реєстрації надсилає реєстраційні дані підписувача та електронний запит на сертифікацію до серверу обробки запитів АЦСК.

У разі якщо особистий ключ та сертифікат повинен використовуватись виключно в певній сфері господарської або управлінської діяльності суб’єктів господарювання (звітність, митне декларування, інше) або як електронна цифрова печатка, адміністратор реєстрації в запиті на сертифікацію за допомогою автоматизованого робочого місця проставляє відповідний

ідентифікатор уточненого призначення ключів. В цьому випадку підписувач зобов’язаний використовувати ключі тільки в визначеній обмежувальним ідентифікатором сфері застосування. В іншому випадку, ключі можуть використовуватись без обмежень (різні види звітності, здійснення правочинів, листування тощо) у порядку, встановленому законодавством.

Строк обробки запита на сертифікацію підписувача не перевищує 2 (дві) години.

Адміністратор сертифікації забезпечує використання особистого ключа АЦСК під час формування сертифікатів підписувачів, списків відкликаних сертифікатів та сертифікатів серверів АС АЦСК.

Після формування АЦСК сертифіката підписувача адміністратор реєстрації засвідчує два примірника заявки на сертифікацію своїм підписом.

{Абзац 8 пункту 6.1 із змінами, внесеними згідно з Наказом ТОВ "КС" № 78 від 07.07.2016}

Один екземпляр заявки на сертифікацію передається до архіву паперових документів АЦСК. Другий екземпляр заявки на сертифікацію повертається підписувачу особисто, через довірену особу або засобами кур’єрської доставки кореспонденції.

6.2 Повторне формування сертифіката ключа

Повторне формування сертифіката ключа здійснюється відповідно до вимог пункту 5.3 Правил посиленої сертифікації, затверджених Наказом ДСТСЗІ СБ України від 13.01.2005 за № 3, зареєстрованих в Міністерстві Юстиції України 27.01.2005 за № 104/10384, та передбачає формування АЦСК нового сертифіката для підписувача, який є власником чинного сертифіката, сформованого АЦСК.

Повторне формування сертифіката здійснюється за зверненням підписувача в разі:

– закінчення терміну дії сертифіката підписувача;

– зміни даних, зазначених у сертифікаті підписувача, впродовж строку чинності сертифіката;

– компрометації або підозри в компрометації особистого ключа підписувача та інших причин, що унеможливлюють подальше використання особистого ключа підписувача.

Звернення в АЦСК (ВПР) щодо повторного формування сертифіката приймаються та опрацьовуються тільки у робочій час, процедура перевірки документів аналогічна п. 5.1.3. Строк обробки звернення щодо повторного формування сертифіката не перевищує 2 (дві) години з моменту його надходження до АЦСК (ВПР).

При повторному формуванні сертифіката адміністратором реєстрації здійснюється перевірка дійсності даних, які надавались заявником раніше під час його попереднього звернення.

В разі повторного формування сертифіката з причини закінчення терміну дії сертифіката або необхідності зміни даних, зазначених у сертифікаті, АЦСК може здійснити переформування сертифіката підписувачу із використанням попередньо засвідченого відкритого ключа підписувача у разі, якщо відповідний йому особистий ключ не був скомпрометований. Для цього підписувач надає необхідні документи в електронній формі у вигляді вкладення електронного листа, що підписані ЕЦП з застосуванням діючого особистого ключа.

В інших випадках повторне формування сертифіката здійснюється аналогічно порядку формування сертифікатів підписувачів.

6.2.1 Повторне формування сертифіката в разі закінчення терміну дії сертифіката підписувача та надання документів у електронній формі

У випадку повторного формування сертифіката в разі закінчення терміну дії сертифіката підписувач надає АЦСК в електронній формі у вигляді вкладення електронного листа наступні документи:

– електронний запит на сертифікацію;
– заявка на повторне формування сертифіката в електронній формі.

На всі документи для повторного формування сертифіката, які надаються в електронній формі у вигляді вкладення електронного листа, має бути накладено ЕЦП підписувача з використанням особистого ключа, що відповідає чинному сертифікату.

Шляхом накладання ЕЦП на документи, які надаються в електронній формі у вигляді вкладення електронного листа, підписувач засвідчує достовірність та актуальність на момент відправки зазначених документів усіх реєстраційних даних, що в них містяться, та реєстраційних даних, що надавались до АЦСК підписувачем під час його попереднього звернення. Автентифікація підписувача здійснюється шляхом перевірки ЕЦП підписувача на документах.

6.2.2 Повторне формування сертифіката в разі зміни даних, зазначених у сертифікаті підписувача та надання документів у електронній формі

У випадку повторного формування сертифіката в разі зміни даних, зазначених у сертифікаті, підписувач надає АЦСК в електронній формі у вигляді вкладення електронного листа наступні документи:

– електронний запит на сертифікацію,

– заявка на повторне формування сертифіката в електронній формі,

– електронні копії документів, які підтверджують зміну даних, виготовлені скануванням оригіналів документів на паперових носіях.

На всі документи для повторного формування сертифіката, які надаються в електронній формі у вигляді вкладення електронного листа, має бути накладено ЕЦП підписувача з використанням особистого ключа, що відповідає чинному сертифікату.

Шляхом накладання ЕЦП на електронні документи, які надаються в електронній формі у вигляді вкладення електронного листа, підписувач засвідчує достовірність та актуальність на момент відправки зазначених документів усіх реєстраційних даних, що в них містяться, та реєстраційних даних, що надавались до АЦСК підписувачем під час його попереднього звернення, крім тих, у яких відбулися зміни. Автентифікація підписувача здійснюється шляхом перевірки ЕЦП підписувача на документах.

{Пункт 6.2 із змінами, внесеними згідно з Наказом ТОВ "КС" № 78 від 07.07.2016}

6.3 Надання сформованого сертифіката підписувачу та визнання сертифіката його власником

За особистої присутності підписувача або довіреної особи, після проведення сертифікації сертифікат надсилається на адресу електронної пошти підписувача або, за бажанням підписувача, може бути записаний на носій підписувача.

Якщо документи на сертифікацію надійшли засобами кур’єрської доставки, то після проведення сертифікації сертифікат надсилається на адресу електронної пошти підписувача.

Після отримання сертифіката підписувач повинен перевірити правильність відомостей, що в ньому містяться. При виявленні некоректних даних (помилки в реквізитах), підписувач повинен повідомити про зазначене АЦСК (ВПР) у порядку, встановленому для скасування сертифіката. В такому випадку сертифікат скасовується та формується новий сертифікат. При відсутності в сертифікаті некоректних даних, підписувач визнає сертифікат шляхом його використання за призначенням.

6.4 Використання сертифіката та особистого ключа

6.4.1 Права та обов’язки заявника (підписувача)

Заявник зобов’язаний:

– ознайомитись з умовами надання послуг ЕЦП, визначених цим Регламентом та відповідними нормативними документами, та дотримуватись їх;

– надавати повну та дійсну інформацію під час реєстрації, необхідну для формування сертифіката підписувача;

– зберігати в таємниці особистий ключ та вживати усіх можливих заходів для запобігання його втрати, розкриття, перекручування чи несанкціонованого використання;

– не розголошувати та не повідомляти іншим особам пароль доступу до особистого ключа та ключову фразу голосової автентифікації;

– не розголошувати та не повідомляти іншим особам пароль доступу до захищеного носія ключової інформації, на якому знаходиться особистий ключ;

– використовувати особистий ключ виключно для мети, визначеної в сертифікаті відповідного відкритого ключа, та додержуватися інших обмежень щодо сфери використання сертифіката;

– використовувати надійні засоби ЕЦП для генерації особистих та відкритих ключів, формування та перевіряння ЕЦП, формування та розкриття криптографічних повідомлень;

– негайно інформувати АЦСК про наступні події, що трапилися до закінчення строку чинності сертифіката: компрометацію особистого ключа; компрометацію паролю захисту особистого ключа; виявлені неточності або зміни даних, зазначених у сертифікаті;

– не використовувати особистий ключ у 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 поновлення сертифіката;

– не використовувати для накладання ЕЦП особистий ключ, відповідний до сертифіката, що скасований або блокований.

Якщо заявник та підписувач є різними суб'єктами, заявник повинен зобов'язати підписувача виконувати вимоги цього Регламенту.

Заявник має право:

– своєчасно отримувати якісні послуги ЕЦП;

– цілодобового вільного доступу з використанням телекомунікаційних мереж загального користування до сертифікатів інших підписувачів, даних про статус сертифікатів, сертифіката АЦСК, нормативних документів з питань надання послуг ЕЦП;

– одержувати сертифікати АЦСК;

– одержувати список відкликаних сертифікатів, сформований АЦСК;

– застосовувати сертифікати АЦСК для перевірки справжності ЕЦП сертифікатів, сформованих АЦСК;

– застосовувати список відкликаних сертифікатів, сформований АЦСК, для перевірки статусу власного сертифіката та сертифікатів інших підписувачів;

– ознайомлюватись з інформацією щодо діяльності АЦСК та надання послуг ЕЦП;

– подавати заяви, скарги, претензії, позови;

– вимагати скасування, блокування або поновлення свого сертифіката;

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

– вимагати від АЦСК виконання вимог захисту персональних даних підписувача;

– оскаржити дії чи бездіяльність АЦСК у судовому порядку.

6.4.2 Обов'язки користувача

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.

6.5 Порядок скасування сертифікатів

Скасування припиняє чинність сертифіката. Скасовані сертифікати поновленню не підлягають.

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

Подача заяви на скасування сертифіката здійснюється тільки протягом робочого дня АЦСК.

Обробка заяви на скасування сертифіката та інформування заявника (підписувача) про скасування здійснюється протягом 2 (двох) годин з моменту надходження до АЦСК заяви на скасування сертифіката.

Часом скасування сертифіката ключа вважається час зміни його статусу в реєстрі сертифікатів АЦСК.

Підписувач не має права використовувати особистий ключ сертифікат ключа якого скасовано.

У випадку, якщо необхідне термінове скасування сертифікату ключа через об'єктивні підстави (наприклад, компрометація особистого ключа), з метою недопущення спричинення моральної та/або матеріальної шкоди, заявник (підписувач) має право заблокувати сертифікат за заявою в усній

формі, за наведеним далі порядком, та протягом строку блокування скасувати сертифікат відкритого ключа.

6.5.1 Підстави для скасування сертифікатів підписувачів

АЦСК негайно скасовує сформований сертифікат підписувача у разі:

– набрання законної сили рішенням суду про скасування сертифіката;
– смерті підписувача або оголошення його померлим за рішенням суду;
– визнання підписувача недієздатним за рішенням суду;
– припинення діяльності суб'єкта господарювання – заявника;
– розірвання підписувачем трудового договору з юридичною особою – заявником;
– надання заявником недостовірних даних;
– не поновлення заявником заблокованого сертифіката протягом 30 календарних днів;
– припинення (розірвання) договору приєднання про надання послуг ЕЦП;
– за заявою заявника або його уповноваженого представника;
– закінчення строку чинності сертифіката;
– компрометації особистого ключа.

АЦСК має право скасувати сертифікат у випадках використання підписувачем сертифіката в неоплачений строк користування послугами АЦСК або в разі несплати послуг АЦСК.

6.5.2 Обставини, за яких сертифікат повинен бути скасований заявником

Підписувач (заявник – юридична особа) зобов'язаний звернутися до АЦСК (ВПР) щодо скасування сертифіката у разі:

– компрометації особистого ключа підписувача (факт або обґрунтована підозра того, що особистий ключ став відомий іншим особам, втрата можливості подальшого використання особистого ключа із будь-яких обставин, зокрема, втрата або пошкодження носія ключової інформації тощо);
– зміни відомостей, зазначених у сертифікаті: переведення на іншу посаду або звільнення з роботи підписувача (для сертифікатів, в яких зазначена посада його власника); зміна прізвища; виявлення помилок у реквізитах сертифіката тощо.

6.6 Порядок блокування сертифікатів

Під блокуванням сертифіката розуміється тимчасове припинення чинності сертифіката.

Після блокування сертифіката, заявник зобов'язаний протягом 30 календарних днів поновити строк чинності сертифіката або подати заяву про його скасування. У випадку, якщо протягом зазначеного строку заявник не

поновить чинність блокованого сертифіката та не подасть заяви про його скасування, по закінченню вищезазначеного строку такий сертифікат автоматично скасовується АЦСК.

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

АЦСК має право блокувати сертифікат з подальшим його скасуванням у випадках використання підписувачем сертифіката в неоплачений строк користування послугами АЦСК або в разі несплати послуг АЦСК.

Часом блокування сертифіката вважається час зміни його статусу в реєстрі сертифікатів АЦСК.

6.6.1 Підстави для блокування сертифікатів підписувачів

АЦСК негайно блокує сертифікат:

– у разі подання заяви власника ключа або його уповноваженого представника;

– за рішенням суду, що набрало законної сили;

– у разі отримання відомостей щодо компрометації особистого ключа підписувача.

АЦСК має право заблокувати сертифікат замовника у разі несплати вартості послуг ЕЦП.

6.6.2 Блокування сертифіката за заявою в усній формі

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

– ідентифікаційні дані власника сертифіката;

– ключову фразу голосової автентифікації;

– реєстраційний номер сертифіката.

Заява в усній формі приймається тільки в випадку позитивної автентифікації (збігу голосової фрази та ідентифікаційних даних підписувача з інформацією в реєстрі користувачів).

Усна заява може бути подана цілодобово. Обробка усної заяви на блокування сертифіката та інформування власника сертифіката здійснюється протягом 2 (двох) годин з моменту подачі заяви.

Усна заява повинна бути підтверджена письмовою заявою на протязі 7 (семи) робочих днів з часу прийняття усної заяви.

6.6.3 Блокування сертифіката за заявою у письмовій формі

Письмова заява подається до АЦСК або до ВПР, де було сформовано сертифікат відкритого ключа, за встановленою формою та засвідчується власноручним підписом заявника.

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

Подача письмової заяви на блокування сертифіката до АЦСК та її розгляд здійснюється протягом робочого дня.

Обробка такої заяви та інформування заявника про блокування повинні бути здійснені протягом 2 (двох) годин з моменту надходження до АЦСК заяви на блокування сертифіката.

6.6.4 Блокування сертифіката за електронним запитом

Електронний запит на блокування сертифіката передається до ПТК АЦСК (ВПР) засобами електронної пошти або у вигляді HTTP-запиту.

Електронний запит формується підписувачем за допомогою програмних засобів, які надаються АЦСК.

Електронний запит на блокування сертифіката засвідчується ЕЦП відповідного сертифіката підписувача.

Блокування сертифіката за електронним запитом не може застосовуватись у разі, якщо особистий ключ, сертифікат якого необхідно заблокувати, було скомпрометовано.

У разі передачі запиту на блокування сертифіката у вигляді HTTP-запиту, обробка запиту та інформування підписувача про блокування здійснюються в режимі реального часу.

У разі передачі запиту на блокування сертифіката засобами електронної пошти, обробка запиту та інформування підписувача про блокування повинні бути здійснені протягом 2 (двох) годин після отримання запиту АЦСК.

Заява у вигляді електронного запиту повинна бути підтверджена письмовою заявою на протязі 7 (семи) робочих днів з часу прийняття АЦСК електронного запиту.

6.7 Порядок поновлення чинності сертифікатів

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

Для здійснення поновлення чинності сертифіката заявник подає до АЦСК(ВПР) письмову заяву встановленого зразка.

Подача письмової заяви на поновлення чинності сертифіката до АЦСК та її розгляд здійснюється тільки протягом робочого дня.

Обробка письмової заяви на поновлення чинності сертифіката та інформування заявника про поновлення повинні бути здійснені протягом 2 (двох) годин з моменту надходження до АЦСК заяви на поновлення сертифіката.

Часом поновлення чинності сертифіката вважається час зміни його статусу у реєстрі сертифікатів АЦСК.

6.7.1 Підстави для поновлення чинності сертифікатів

Блокований посилений сертифікат поновлюється АЦСК:

- 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.

6.8 Розповсюдження інформації про статус сертифікатів

Розповсюдження інформації про статус сертифіката здійснюється шляхом публікації списку відкликаних сертифікатів (див. 4.4) та надання послуги інтерактивного визначення статусу сертифіката.

У разі скасування (блокування, поновлення) сертифіката, оновлений частковий список відкликаних сертифікатів випускається та публікується не пізніше 2 (двох) годин після внесення відповідних змін до реєстру сертифікатів АЦСК.

АЦСК надає всім користувачам послугу інтерактивного визначення статусу сертифіката. Послуга надається шляхом відправлення запиту на OCSP-сервер АЦСК.

Послуга інтерактивного визначення статусу сертифіката надається цілодобово.

6.9 Закінчення строку чинності сертифіката підписувача

Дата й час початку та закінчення дії особистого ключа визначається датою й часом початку та закінчення дії сертифіката відповідного відкритого ключа. Термін дії відкритого ключа встановлено рівним терміну дії відповідного сертифіката.

Після закінчення строку чинності сертифіката, він вилучається з інформаційного ресурсу АЦСК та поміщається в архів. АЦСК зберігає сертифікат та пов’язані з ним списки відкликаних сертифікатів безстроково. За запитом користувачів, АЦСК надає доступ до необхідного сертифіката та пов’язаних з ним списків відкликаних сертифікатів з архівних записів АЦСК у

строки, встановлені законодавством України для відповідей на звернення громадян.

6.10 Порядок надання послуги фіксування часу

АЦСК надає всім користувачам послугу фіксування часу. Послуга надається шляхом відправлення запиту на TSP-сервер АЦСК.

Послуга фіксування часу надається цілодобово.

6.11 Порядок надання у користування надійних засобів ЕЦП

Надійні засоби ЕЦП надаються у користування шляхом розміщення посилання для завантаження у відповідному розділі на сайті ksystems.com.ua або, за бажанням заявника, безпосередньо на зовнішньому носії інформації в АЦСК (ВПР).

7 Управління та операційний контроль

7.1 Фізичне середовище

7.1.1 Приміщення АЦСК

Локальна обчислювальна мережа центрального сегмента ЦСК (далі – серверна частина) розташована за адресою: 03057, м. Київ, вул. Смоленська, 31-33.

Робочі станції адміністратора безпеки, адміністратора сертифікації, системного адміністратора, адміністраторів реєстрації, робоча станція генерації ключів (далі – адміністративна частина) розташовані в орендованій частині сьомого поверху будинку за адресою: 02121, м. Київ, вул. Харківське шосе, 201-203, під'їзд 2.

Серверна частина є об'єктом обмеженого доступу і являє собою серверну зону.

Адміністративна частина є об’єктом загального доступу із обмеженням перебування осіб. Приміщення розділяється на такі зони:

– зону для відвідувачів,
– зону адміністраторів.

Компоненти АС ПТК ЦСК встановлено в наступних зонах:

– зоні відвідувачів;
– зоні адміністраторів;
– серверній зоні.

Безпека інформаційних ресурсів в АЦСК досягається шляхом впровадження організаційних, інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації комплексної системи захисту інформації.

Приміщення АЦСК обладнані системою охоронної та пожежної сигналізації.

Для забезпечення необхідного рівня захисту інформації, яка циркулює в серверній зоні, для захисту від електромагнітного випромінювання засоби обчислювальної техніки розташовані в екранованій шафі.

Для заземлення екранованої шафи влаштований захисно-сигнальний контур заземлення. Електроживлення вводиться до екранованої шафи через протизавадний фільтр.

Серверна зона відповідає вимогам додатку до п. 4.1.1 Правил посиленої сертифікації.

7.1.2 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.

Особи, що порушують перепускний і внутрішній режим, притягуються до дисциплінарної відповідальності.

7.2 Процедурний контроль

7.2.1 Склад організаційної структури АЦСК

До складу АЦСК входять:

– керівництво АЦСК;
– служба реєстрації;
– служба сертифікації;
– служба захисту інформації;
– відокремлені пункти реєстрації.

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

7.2.2 Функції та завдання організаційних підрозділів АЦСК

7.2.2.1 Керівництво АЦСК

До складу керівництва входить керівник АЦСК.

Функції та завдання керівництва АЦСК:

– визначення та підтримка в актуальному стані політики та цілей АЦСК;
– визначення основних шляхів розвитку, координація, регламентування, контроль та аналіз діяльності АЦСК;
– визначення цілей структурних підрозділів АЦСК;
– забезпечення структурних підрозділів АЦСК необхідними ресурсами для досягнення визначених цілей;
– контроль за виконанням зауважень, пропозицій та вимог підписувачів, направлених на удосконалення роботи АЦСК.

7.2.2.2 Служба реєстрації АЦСК

До складу служби реєстрації входить адміністратор реєстрації.

Функції та завдання служби реєстрації:

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

– перевірка даних, обов’язкових для формування сертифіката, а також даних, які вносяться в сертифікат на вимогу заявників;

– забезпечення обробки запитів на формування, скасування, блокування та поновлення сертифікатів підписувачів;

– ведення реєстру користувачів АЦСК;

– організація встановлення належності підписувачу особистого ключа та його відповідність відкритому ключу, якщо їх генерація здійснювалася не в АЦСК (ВПР);

– підготовка та перевірка договірних документів про надання послуг ЕЦП;

– отримання від заявників заявок на формування, скасування, блокування та поновлення сертифікатів;

– надання допомоги під час генерації особистих та відкритих ключів у разі отримання відповідного звернення та вживання заходів щодо забезпечення безпеки інформації під час генерації;

– перевірка законності звернень про блокування, поновлення та скасування сертифікатів;

– надання заявникам, підписувачам, користувачам консультацій щодо умов та порядку надання послуг ЕЦП.

7.2.2.3 Служба сертифікації АЦСК

До складу служби сертифікації входить адміністратор сертифікації.

Функції та завдання служби сертифікації:

– збереження та контроль за використанням особистого ключа АЦСК;

– формування сертифікатів підписувачів, посадових осіб АЦСК, серверів АЦСК, списків відкликаних сертифікатів та позначок часу;

– контроль процесу публікації сертифікатів та списків відкликаних сертифікатів;

– ведення, архівація та відновлення реєстру сформованих сертифікатів;

– подання до центрального засвідчувального органу даних, які необхідні для формування сертифіката АЦСК та засвідчення відкритого ключа АЦСК;

– участь у генерації та знищенні особистого ключа АЦСК та ключів серверів АЦСК з їх відповідними резервними копіями;

– контроль за веденням журналів прийому-передачі ключів.

7.2.2.4 Служба захисту інформації

До складу служби захисту інформації (СЗІ) входять:

– начальник СЗІ;

– адміністратор безпеки;

– системний адміністратор.

Функції та завдання служби захисту інформації:

– забезпечення повноти та якісного виконання організаційно-технічних заходів із захисту інформації;

– розроблення розпорядчих документів, згідно з якими у АЦСК повинен забезпечуватися захист інформації, контроль за їх виконанням;

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

– контроль за зберіганням особистого ключа АЦСК та його резервної копії, особистих ключів посадових осіб АЦСК;

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

– ведення контролю за процесом резервування сертифікатів та списків відкликаних сертифікатів, а також інших важливих ресурсів;

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

– забезпечення спостереження (реєстрація та аудит подій в ПТК, моніторинг подій тощо) за функціонуванням КСЗІ;

– забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій ПТК;

– ведення журналу обліку адміністратора безпеки;

– організація експлуатації та технічного обслуговування ПТК;

– підтримка електронного інформаційного ресурсу АЦСК;

– адміністрування засобів ПТК;

– участь у впровадженні та забезпеченні функціонування КСЗІ;

– ведення журналів аудиту подій, що реєструються засобами ПТК;

– встановлення та налагодження програмного забезпечення системи резервного копіювання;

– формування та ведення резервних копій загальносистемного та спеціального програмного забезпечення ПТК;

– забезпечення актуальності еталонних, архівних і резервних копій реєстрів сертифікатів, що створюються в АЦСК, їх зберігання.

7.2.2.5 Відокремлені пункти реєстрації

До складу персоналу відокремлених пунктів реєстрації входять:

– керівник ВПР

– адміністратор реєстрації ВПР (віддалений адміністратор реєстрації).

Функції та завдання відокремлених пунктів реєстрації:

– ідентифікація (встановлення) осіб, які звернулися до АЦСК з метою формування сертифіката;

– перевірка даних, обов'язкових для формування сертифіката, а також даних, які вносяться в сертифікат на вимогу заявника (підписувача);

– укладення договорів про надання послуг ЕЦП;

– проведення реєстрації заявників (підписувачів);

– отримання від підписувачів заявок на формування, скасування, блокування та поновлення сертифікатів;

– надання допомоги підписувачам під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення та вживання заходів щодо забезпечення безпеки інформації під час генерації;

– перевірка законності звернень про блокування, поновлення та скасування сертифікатів;

– надання підписувачам консультацій щодо умов та порядку надання послуг ЕЦП;

– забезпечення захисту інформації в відокремленому пункті реєстрації.

7.2.3 Функціональні обов'язки посадових осіб, безпосередньо пов'язаних з обслуговуванням сертифікатів

Наступні посадові особи безпосередньо пов'язані з обслуговуванням сертифікатів:

– керівник АЦСК;

– адміністратор безпеки;

– адміністратор сертифікації;

– системний адміністратор;

– адміністратор реєстрації.

В залежності від навантаження на АЦСК обов'язки зазначених посад можуть суміщатись. Разом з тим, забороняється суміщення посади адміністратора безпеки з іншими посадами.

Керівник та посадові особи зобов'язані:

– відповідально ставитися до виконання своїх службових обов'язків та сумлінно їх виконувати;

– приймати рішення в межах наданих повноважень;

– не розголошувати та не використовувати з вигодою для себе чи для третіх осіб конфіденційну інформацію, яка стала відома їм при виконанні своїх службових обов'язків, зокрема відомості про персональні дані.

7.2.3.1 Керівник АЦСК

Керівник АЦСК несе персональну відповідальність за діяльність АЦСК, за невиконання або неналежне виконання покладених на нього посадових обов'язків відповідно до законодавства України.

7.2.3.2 Адміністратор безпеки

Адміністратор безпеки відповідає за належне функціонування КСЗІ та контроль за використанням криптографічних засобів АЦСК.

Посадові обов'язки адміністратора безпеки:

– реєстрування факту генерації особистих ключів співробітників АЦСК у відповідному журналі обліку;

– генерація та резервне копіювання особистого ключа АЦСК, реєстрація цих фактів в журналі генерації, резервного копіювання, відновлення та знищення ключових даних;

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

– контроль розмежування доступу до ресурсів ПТК;

– моніторинг подій, перегляд журналу аудиту подій в ПТК, контроль за функціонуванням КСЗІ;

– участь у розробці розпорядчих документів, згідно з якими в АЦСК повинен забезпечуватися захист інформації, контроль за їх виконанням;

– участь в заходах з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій ПТК;

– своєчасне реагування на спроби несанкціонованого доступу до ресурсів АЦСК, порушення правил експлуатації засобів захисту інформації;

– контроль за зберіганням особистого ключа АЦСК та його резервної копії, особистих ключів посадових осіб АЦСК;

– знищення особистого ключа АЦСК та його резервних копій, контроль за правильним і своєчасним знищенням посадовими особами особистих ключів.

7.2.3.3 Системний адміністратор

Системний адміністратор відповідає за функціонування ПТК АЦСК та конфігурування загального програмного забезпечення ПТК.

Посадові обов’язки системного адміністратора:

– організація експлуатації та технічного обслуговування ПТК;

– забезпечення підтримки електронного інформаційного ресурсу, публікації сертифікатів та списку відкликаних сертифікатів;

– адміністрування засобів ПТК;

– участь у впровадженні та забезпеченні функціонування КСЗІ;

– забезпечення ведення журналів аудиту подій, що реєструються засобами ПТК;

– встановлення, інсталяція та налагодження, конфігурування програмного забезпечення та системи резервного копіювання;

– забезпечення актуальності еталонних і архівних копій загальносистемного та спеціального програмного забезпечення ПТК;

– формування та ведення резервних копій (дублювання) загальносистемного та спеціального програмного забезпечення ПТК;

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

– забезпечення спостереження (реєстрація та аудит подій в АЦСК, моніторинг подій тощо) за функціонуванням КСЗІ;

– забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій ПТК.

7.2.3.4 Адміністратор сертифікації

Адміністратор сертифікації відповідає за формування сертифікатів, списків відкликаних сертифікатів, збереження та використання особистого ключа АЦСК.

Посадові обов’язки адміністратора сертифікації:

– підготовка та подання до ЦЗО документів, необхідних для формування сертифіката та засвідчення відкритого ключа АЦСК;

– участь у генерації та знищенні особистого ключа АЦСК, ключів серверів АЦСК та їх резервних копій, участь у формуванні сертифікатів співробітників АЦСК;

– забезпечення використання особистого(их) ключа(ів) АЦСК під час формування сертифікатів, списків відкликаних сертифікатів;

– забезпечення використання ключа TSP-сервера під час формування позначки часу;

– збереження особистого(их) ключа(ів) АЦСК;

– забезпечення актуальності резервних копій баз сертифікатів, списків відкликаних сертифікатів та їх зберігання;

– забезпечення ведення, архівації та відновлення еталонної бази даних сформованих сертифікатів та списків відкликаних сертифікатів.

7.2.3.5 Адміністратор реєстрації

Адміністратор реєстрації відповідає за ідентифікацію фізичних та юридичних осіб під час формування, блокування, поновлення та скасування сертифіката.

Посадові обов’язки адміністратора реєстрації:

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

– перевірка даних, обов'язкових для формування сертифіката, а також даних, які вносяться у сертифікат на вимогу підписувача;

– укладення договорів про надання послуг ЕЦП;

– ведення реєстрації підписувачів (заявників);

– отримання від підписувачів заявок на формування, скасування, блокування та поновлення сертифікатів;

– забезпечення обробки запитів на формування, скасування, блокування та поновлення сертифікатів підписувачів;

– надання допомоги підписувачам під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення та вживання заходів щодо забезпечення безпеки інформації під час генерації;

– перевірка законності звернень про блокування, поновлення та скасування сертифікатів;

– надання підписувачам консультацій щодо умов та порядку надання послуг ЕЦП;

– використання та зберігання особистого ключа адміністратора реєстрації;

Посадові обов'язки, кваліфікаційні вимоги та відповідальність посадових осіб, діяльність яких безпосередньо пов'язана з наданням послуг ЕЦП та обслуговуванням сертифікатів, визначається окремим положенням.

7.3 Ведення журналів аудиту

ПТК забезпечує реєстрацію у журналах аудиту АС АЦСК таких подій:

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

– генерації, знищення та використання ключової інформації;

– зміни ключів;

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

– спроби несанкціонованого доступу до ПТК;

– надання доступу до ПТК персоналу АЦСК;

– збої у роботі ПТК.

ПТК АЦСК забезпечує реєстрацію у журналах аудиту АС ВПР таких подій:

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

– генерації, знищення та використання ключової інформації;

– спроб несанкціонованого доступу до ПТК;

– збоїв у роботі ПТК.

Захист журналів аудиту АС забезпечується засобами ПТК, налагодження та контроль за якими здійснюється адміністратором безпеки АЦСК.

Журнали аудиту автоматизованої системи АЦСК переглядаються не рідше ніж раз на добу.

Перегляд журналів аудиту автоматизованої системи може здійснювати працівник СЗІ.

Строк зберігання протокольних записів аудиту не обмежений.

7.4 Ведення архівів

Архівному зберіганню підлягають наступні документи АЦСК:

– укладені з заявниками договори та інші документи (завірені в установленому порядку копії документів), що використовуються під час реєстрації;
– сертифікати АЦСК;
– сертифікати серверів АЦСК;
– сертифікати посадових осіб АЦСК;
– сертифікати підписувачів;
– заяви на реєстрацію заявників;
– заяви на сертифікацію підписувачів;
– заяви на скасування сертифікатів підписувачів;
– заяви на блокування сертифікатів підписувачів;
– заяви на поновлення сертифікатів підписувачів;
– службові документи АЦСК, у тому числі журнали аудиту ПТК тощо.

Документи АЦСК на паперових носіях, у тому числі й сертифікати підписувачів, зберігаються в порядку, встановленому законодавством України про архіви та архівні справи. Документи, що підлягають архівному зберіганню, є документами тимчасового зберігання. Термін зберігання архівних документів – не менше 5 (п'яти) років.

Сертифікати АЦСК, сертифікати посадових осіб АЦСК, сертифікати серверів АЦСК, сертифікати підписувачів та списки відкликаних сертифікатів, дані про надання послуг фіксування часу зберігаються постійно.

Для перевірки електронних документів, підписаних особистими ключами підписувачів, відповідні сертифікати яких не є чинними, АЦСК надає можливість доступу до таких сертифікатів через власний інформаційний ресурс. Додатково забезпечується можливість перевірки статусу сертифіката на момент накладання ЕЦП.

Знищення архівних документів здійснюється комісією, сформованою із посадових осіб АЦСК при безпосередній участі керівника АЦСК та адміністратора безпеки, про що складається відповідний акт.

Засоби системи управління базами даних (далі – СУБД), що входять до складу серверу АЦСК виконують автоматичне резервне копіювання бази даних сертифікатів та списків відкликаних сертифікатів (далі – БД). Автоматичне створення резервної копії засобами СУБД виконується раз на добу, під час найменшого завантаження серверу. Додатково виконується резервне копіювання бази даних та журналів аудиту ПТК в ручному режимі на оптичні носії, або інші з’ємні носії інформації. Резервне копіювання виконується засобами операційної системи або засобами, що надаються із пристроями

запису на з’ємні носії. Після створення нової резервної копії, попередня резервна копія стає архівною.

Для зберігання носіїв з резервними та архівними копіями виділяється окреме сховище, територіально відокремлене від приміщення АЦСК, із забезпеченням захисту від несанкціонованого доступу.

З’ємний носій зберігається в упаковці, яку власноручно підписує уповноважена посадова особа АЦСК, яка відповідає за створення та зберігання резервних та архівних копій. Окрім цього на упаковці вказується номер копії, та ведеться журнал, у якому реєструється створення копії, зокрема її номер, дата та час створення, прізвище, ім’я та по батькові, посада та особистий підпис особи, що створила копію.

Архівні копії журналів аудиту ПТК АЦСК зберігаються в приміщенні АЦСК не менше 2 (двох) років. Відповідальність за контроль автоматичного резервного копіювання та виконання резервного копіювання в ручному режимі покладається на системного адміністратора АЦСК. Адміністратор безпеки періодично контролює процес створення та зберігання резервних копій.

Документи в електронній формі, отримані від підписувачів для повторного формування сертифікатів, повинні зберігатись на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність. Строк зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері. При зберіганні електронних документів обов'язкове додержання таких вимог:

1) інформація, що міститься в електронних документах, повинна бути доступна для її подальшого використання;

2) має бути забезпечена можливість відновлення електронного документа у форматі, в якій він був створений або одержаний;

3) повинна зберігатися інформація, яка дає змогу встановити дату та час створення або отримання документа.

{Пункт 7.4 доповнено абзацом 10 згідно з Наказом ТОВ "КС" № 78 від 07.07.2016}

8 Управління ключами

8.1 Порядок генерації ключів підписувача

Відкритий та особистий ключі підписувача можуть бути згенеровані:

– на робочому місці заявника;
– на робочій станції генерації ключів підписувачів у АЦСК (ВПР).

Під час генерації ключової пари особистий ключ підписувача захищається паролем та записується на носій ключової інформації.

Після генерації ключової пари формується запит на сертифікацію у відповідному форматі, що містить відкритий ключ підписувача та додаткову інформацію для формування сертифіката в АЦСК. Для засвідчення запиту формується ЕЦП за допомогою особистого ключа, який відповідає відкритому ключу, що міститься в запиті – створюється самопідписаний запит.

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

Строк дії особистого ключа підписувача не може перевищувати 2 (двох) років. Початком строку дії особистого ключа підписувача вважається дата та час формування сертифіката відповідного відкритого ключа.

Процедура подання запиту на сертифікацію для підписувачів, які мають чинний сертифікат ключа ідентична процедурам подання запиту на сертифікацію наведеним вище.

8.1.1 Генерація на робочому місці 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 носієві інформації особисто підписувачем, довіреною особою або засобами кур'єрської доставки кореспонденції.

У випадку передачі носія інформації, що містить запит на сертифікацію, довіреною особою або засобами кур'єрської доставки кореспонденції такий носій повинен вміщуватись в окремий конверт, який запечатується та скріплюється підписом власника особистого ключа на місці запечатування, з метою відслідковування факту пошкодження конверту.

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.

8.1.2 Генерація ключів на робочій станції АЦСК

Ключі підписувача генеруються ним особисто або довіреною особою заявника на робочій станції генерації ключів підписувачів, що входить до складу ПТК АЦСК, де застосовуються надійні засоби ЕЦП. Особистий ключ підписувача захищається паролем.

По закінченні процедури генерації особистий ключ підписувача автоматично записується на носій ключової інформації та залишається у підписувача, а запит на сертифікацію, що містить відкритий ключ, передається через службовий носій інформації на робочу станцію адміністратора реєстрації.

Особисті ключі підписувачів не зберігаються в АЦСК. Після генерації та запису на носій ключової інформації вони автоматично знищуються надійним засобом ЕЦП.

Генерація ключів довіреною особою здійснюється на робочій станції генерації ключів. У такому випадку по закінченні процедури генерації носій ключової інформації та парольна фраза вкладається в непрозорий конверт, який запечатується, скріплюється підписами довіреної особи і адміністратора реєстрації.

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

У разі, якщо генерація ключів здійснювалась довіреною особою, підписувач при отриманні особистого ключа зобов’язаний перевірити цілісність конверта. Якщо цілісність не порушена, то невідкладно, до першого використання особистого ключа, підписувач зобов’язаний змінити пароль доступу до нього.

У разі, якщо неможливо змінити пароль шляхом перезапису ключа на той самий носій ключової інформації, то після зміни паролю на новому носієві на старому носієві особистий ключ зі старим паролем необхідно знищити в надійний спосіб.

Якщо цілісність конверта порушена, заявник (підписувач) невідкладно зобов’язаний звернутись до АЦСК із заявою про скасування сертифіката відповідного ключа.

8.2 Порядок генерації та резервного копіювання особистого ключа АЦСК

Генерація особистого ключа АЦСК виконується в апаратному засобі КЗІ, що входить до складу ПТК АЦСК, за участі двох осіб – адміністратора сертифікації та адміністратора безпеки.

В процесі генерації особистий ключ АЦСК зберігається в апаратному засобі КЗІ, що входить до складу ПТК АЦСК. Запит на формування сертифіката АЦСК, що містить відкритий ключ, записується на НЖМД сервера АЦСК.

Для забезпечення можливості відновлення особистого ключа АЦСК, у випадку виходу з ладу апаратного засобу КЗІ, після генерації особистого ключа створюється не менше однієї резервної копії ключа з апаратного засобу КЗІ. Резервне копіювання виконується двома особами – адміністратором сертифікації та адміністратором безпеки. Кожна резервна копія особистого ключа АЦСК записується з розподілом таємниці на два захищені носія інформації. Захищені носії інформації з копіями особистого ключа АЦСК поміщуються в тубуси (конверти), які опечатуються печаткою керівника АЦСК. Резервні копії особистих ключів АЦСК зберігаються в сейфах адміністратора сертифікації та адміністратора безпеки.

Факти генерації та резервного копіювання особистого ключа АЦСК заносяться в журнал генерації, резервного копіювання, відновлення та знищення ключових даних.

Строк дії особистого ключа АЦСК не перевищує 5 (п’яти) років. Початком строку дії особистого ключа АЦСК вважається дата та час початку строку дії сертифіката відповідного відкритого ключа АЦСК.

Після генерації особистого ключа АЦСК здійснюється формування запиту на формування сертифіката в ЦЗО.

8.3 Порядок використання (введення) особистого ключа АЦСК

Введення особистого ключа АЦСК виконується на сервері АЦСК (основному) у присутності не менше ніж двох осіб – керівника АЦСК, адміністратора безпеки, адміністратора сертифікації. Особистий ключ АЦСК зберігається та застосовується тільки в апаратному засобі КЗІ, що входить до складу ПТК АЦСК.

Перед процесом введення здійснюється автентифікація адміністратора безпеки або адміністратора сертифікації у апаратному модулі для ініціалізації механізмів ЕЦП та введення службової інформації особистого ключа у сервер. Автентифікація в апаратному модулі здійснюється з використанням даних автентифікації.

В процесі введення сертифікат АЦСК, що містить відкритий ключ, зчитується з НЖМД сервера.

8.4 Порядок планової зміни ключів АЦСК

Планова зміна особистого ключа АЦСК виконується не пізніше 2 (двох) років до завершення дії сертифіката поточного відкритого ключа АЦСК.

Процедура планової зміни особистого ключа АЦСК здійснюється в наступному порядку:

– адміністратор сертифікації разом з адміністратором безпеки виконують генерацію нового особистого ключа АЦСК;

– адміністратор сертифікації ініціює процес засвідчення чинності нового відкритого ключа АЦСК в ЦЗО шляхом передачі запиту на формування сертифіката;

– після отримання сертифіката АЦСК від ЦЗО новий сертифікат АЦСК публікується на інформаційному ресурсі АЦСК;

– при цьому поточна ключова пара АЦСК стає попередньою, а нова ключова пара АЦСК стає поточною.

Поточний особистий ключ АЦСК повинен зберігатися і застосовуватися в апаратному засобі КЗІ, що входить до складу ПТК АЦСК.

Попередній особистий ключ АЦСК повинен зберігатися і застосовуватися в апаратному засобі КЗІ, що входить до складу ПТК АЦСК, та використовуватися для обслуговування сертифікатів підписувачів, які були сформовані за допомогою цього ключа.

Перенесення попереднього особистого ключа АЦСК здійснюється шляхом створення та відновлення резервної копії особистого ключа.

Факти створення та відновлення резервної копії попереднього особистого ключа АЦСК та його перенесення з одного до іншого засобу КЗІ реєструються адміністратором безпеки у відповідному журналі обліку.

Попередній особистий ключ АЦСК та всі його резервні копії знищуються надійним способом після закінчення терміну дії відповідного сертифіката АЦСК. Факти знищення особистого ключа АЦСК та його резервних копій заноситься в журнал генерації, резервного копіювання, відновлення та знищення ключових даних.

Перевірка ЕЦП на документах, підписаних за допомогою попереднього особистого ключа АЦСК, здійснюється шляхом застосування відповідного сертифіката АЦСК, який зберігається в інформаційному ресурсі АЦСК або в архіві ЦЗО.

Планова зміна особистого ключа сервера АЦСК виконується не пізніше завершення строку дії сертифіката поточного відкритого ключа сервера АЦСК.

Процедура планової зміни особистого ключа сервера АЦСК здійснюється в наступному порядку:

– адміністратор сертифікації за участі адміністратора безпеки виконує генерацію нового особистого ключа сервера АЦСК;

– адміністратор сертифікації ініціює процес засвідчення чинності нового відкритого ключа сервера АЦСК;

– після формування сертифіката сервера АЦСК новий сертифікат сервера АЦСК публікується на інформаційному ресурсі АЦСК;

– при цьому поточна ключова пара сервера АЦСК стає попередньою, а нова ключова пара сервера АЦСК стає поточною.

Попередній особистий ключ сервера АЦСК та всі його резервні копії знищуються надійним способом після закінчення терміну дії відповідного сертифіката сервера АЦСК. Факти знищення особистого ключа АЦСК та його резервних копій заноситься в журнал генерації, резервного копіювання, відновлення та знищення ключових даних.

Перевірка ЕЦП на документах, підписаних за допомогою попереднього особистого ключа, здійснюється шляхом застосування відповідного йому сертифіката, який зберігається в інформаційному ресурсі АЦСК.

У випадку компрометації або загрози компрометації особистого ключа сервера АЦСК виконується позапланова зміна ключа.

Процедура позапланової зміни ключа сервера АЦСК виконується в порядку, визначеному процедурою планової зміни особистого ключа сервера АЦСК.

Після публікації нового сертифіката сервера АЦСК у загальнодоступних каталогах (LDAP-каталоги) та на інформаційному ресурсі АЦСК (web-сторінці), попередній особистий ключ та всі його резервні копії знищуються надійним способом. Факти знищення особистого ключа сервера АЦСК та його резервних копій заноситься в журнал генерації, резервного копіювання, відновлення та знищення ключових даних.

Планова зміна особистого ключа посадової особи АЦСК виконується не пізніше завершення строку дії сертифіката поточного відкритого ключа посадової особи АЦСК.

Процедура планової заміни ключів посадових осіб АЦСК здійснюється в наступному порядку:

– посадова особа АЦСК генерує новий особистий ключ та відповідний йому відкритій ключ;

– адміністратор сертифікації формує новий сертифікат посадової особи АЦСК;

– попередній особистий ключ посадової особи АЦСК знищується надійним способом, а попередній сертифікат скасовується.

У випадку компрометації особистого ключа посадової особи АЦСК сертифікат посадової особи АЦСК скасовується. Після скасування сертифіката ключа посадової особи АЦСК виконується процедура позапланової заміни ключів посадової особи АЦСК. Процедура позапланової заміни ключів посадової особи АЦСК виконується в порядку, визначеному у процедурі планової заміни ключів посадової особи АЦСК.

8.5 Порядок позапланової зміни ключів АЦСК

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

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

Після публікації нового сертифіката АЦСК у загальнодоступних каталогах (LDAP-каталоги) та на інформаційному ресурсі АЦСК (web-сторінці), попередній особистий ключ та всі його резервні копії знищуються надійним способом. Факти знищення особистого ключа АЦСК та його резервних копій заноситься в журнал генерації, резервного копіювання, відновлення та знищення ключових даних.

Сертифікати всіх підписувачів, посадових осіб АЦСК, серверів АЦСК скасовуються шляхом занесення в список відкликаних сертифікатів.

Список відкликаних сертифікатів підписується новим особистим ключем АЦСК.

АЦСК офіційно оповіщає заявників про факт позапланової зміни ключів АЦСК.

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