ПРОЄКТ

ЗАТВЕРДЖЕНО
Наказ Міністерства цифрової трансформації України
_____2021 року № ____

РЕГЛАМЕНТ
роботи центрального засвідчувального органу

I. Загальні положення

1. Цей Регламент визначає організаційно-методологічні, технічні та технологічні умови діяльності центрального засвідчувального органу (далі – ЦЗО) під час надання ним кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки, порядок взаємодії кваліфікованих надавачів електронних довірчих послуг (далі – надавачі) з ЦЗО у процесі надання ним кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки, а також внесення юридичних осіб та фізичних осіб – підприємців, які мають намір надавати електронні довірчі послуги, до Довірчого списку.

2. Цей Регламент є обов’язковим для юридичних осіб та фізичних осіб – підприємців, які мають намір надавати електронні довірчі послуги, та для кваліфікованих надавачів електронних довірчих послуг.

3. Дія цього Регламенту не поширюється на надавачів електронних довірчих послуг, що не мають наміру надавати кваліфіковані електронні довірчі послуги, а також на надавачів, що мають намір надавати кваліфіковані довірчі послуги у банківській системі та під час здійснення переказу коштів.

4. У цьому Регламенті терміни вжито в таких значеннях:

адміністратор інформаційно-телекомунікаційної системи ЦЗО (далі – Адміністратор ІТС ЦЗО) – державне підприємство «ДІЯ» (далі – ДП «ДІЯ»), яке належить до сфери управління головного органу у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних довірчих послуг, та здійснює технічне й технологічне забезпечення виконання функцій ЦЗО;

інформаційно-телекомунікаційна система ЦЗО (далі – ІТС ЦЗО) – сукупність інформаційних та телекомунікаційних систем ЦЗО, які у процесі обробки інформації діють як єдине ціле та об'єднують програмно-технічний комплекс, що використовується під час надання послуг (далі – програмно-технічний комплекс), фізичне середовище, інформацію, що обробляється в цих системах, а також найманих працівників ЦЗО, які безпосередньо задіяні у наданні послуг або обслуговують програмно-технічний комплекс (далі – наймані працівники);

політика сертифіката – перелік усіх правил, що застосовуються Адміністратором ІТС ЦЗО у процесі надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;

положення сертифікаційних практик – перелік усіх практичних дій та процедур, які застосовуються для реалізації політики сертифіката ЦЗО.

Інші терміни, що вживаються у цьому Регламенті, застосовуються у значеннях, визначених нормативно-правовими актами, що регулюють відносини у сфері електронних довірчих послуг.

5. Головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг, на який покладено виконання функцій ЦЗО, є Міністерство цифрової трансформації України (далі – Мінцифри):

місцезнаходження (поштова адреса): вул. Ділова, 24, м. Київ, 03150;

код за ЄДРПОУ: 43220851;

телефон: (044) 207-17-39.

Адреса електронного інформаційного ресурсу ЦЗО, доступ до якого забезпечується через телекомунікаційні мережі загального користування цілодобово (далі – офіційний вебсайт ЦЗО): www.czo.gov.ua.

Адреса електронної пошти для офіційного листування: inbox@czo.gov.ua

6. Адміністратор ІТС ЦЗО:

місцезнаходження (поштова адреса): вул. Ділова, 24, м. Київ, 03150;

код за ЄДРПОУ: 43395033;

адреса електронної пошти технічної підтримки: support.its@czo.gov.ua.

7. Мінцифри виконує функції ЦЗО, визначені підпунктом 20 пункту 4 Положення про Міністерство цифрової трансформації України, затвердженого постановою Кабінету Міністрів України від 18 вересня 2019 року № 856.

Структурним підрозділом, визначеним у Мінцифри відповідальним за виконання функцій ЦЗО, є експертна група розвитку електронних довірчих послуг директорату функціонального розвитку цифровізації.

8. Адміністратор ІТС ЦЗО здійснює технічне та технологічне забезпечення виконання таких функцій ЦЗО:

функціонування програмно-технічного комплексу ЦЗО та захисту інформації, що в ньому обробляється, відповідно до вимог законодавства;

функціонування вебсайту ЦЗО;

ведення Довірчого списку;

ведення реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

генерація пари ключів та створення самопідписаних сертифікатів ключів електронної печатки ЦЗО;

надання послуг надавачам з використанням самопідписаного сертифіката електронної печатки ЦЗО, що призначений для надання таких послуг;

надання послуги постачання передачі сигналів точного часу, синхронізованого з Державним еталоном одиниць часу і частоти;

технологічне забезпечення інтероперабельності та технологічної нейтральності національних технічних рішень, а також недопущення їх дискримінації;

використання ІТС ЦЗО для визнання в Україні електронних довірчих послуг, іноземних сертифікатів відкритих ключів, що використовуються під час надання юридично значущих електронних послуг у процесі взаємодії між суб'єктами різних держав;

надання цілодобового доступу до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів та до інформації про статус сертифікатів ключів через телекомунікаційні мережі загального користування;

скасування, блокування та поновлення сертифікатів ключів у випадках, передбачених законом;

приймання та зберігання документованої інформації, сформованих сертифікатів (у тому числі посилених, кваліфікованих) відкритих ключів, реєстрів чинних, блокованих та скасованих сертифікатів відкритих ключів у разі припинення діяльності кваліфікованого надавача електронних довірчих послуг.

9. Робота Мінцифри організована в одну робочу зміну з понеділка по четвер з 09:00 до 18:00, обідня перерва – з 13:00 до 13:45; у п'ятницю – з 09:00 до 16:45, обідня перерва – з 13:00 до 13:45. Заяви та документи для внесення відомостей про юридичних осіб, фізичних осіб – підприємців до Довірчого списку приймаються та розглядаються за адресою: вул. Ділова, 24, м. Київ, 03150.

10. Робота Адміністратора ІТС ЦЗО організована в одну робочу зміну з понеділка по четвер з 09:00 до 18:00, обідня перерва – з 13:00 до 13:45; у п'ятницю – з 09:00 до 16:45, обідня перерва – з 13:00 до 13:45, за винятком приймання заяв надавачів на блокування, скасування та поновлення їх сертифікатів ключів, що є цілодобовим. Заяви на блокування, скасування та поновлення сертифікатів ключів надсилаються в електронній формі з накладенням кваліфікованого електронного підпису керівника надавача або його

уповноваженої особи на адресу електронної пошти: support.its@czo.gov.ua. Документована інформація, що передається надавачем до Адміністратора ІТС ЦЗО у разі припинення його діяльності приймається та розглядається за адресою: вул. Ділова, 24, м. Київ, 03150.

11. Цей Регламент та зміни до нього розміщуються на офіційному вебсайті ЦЗО.

12. Формати, структура та протоколи, що застосовуються під час формування сертифікатів ключів ЦЗО, формування кваліфікованих сертифікатів відкритих ключів надавачів, формування списків відкликаних сертифікатів (далі – СВС) ЦЗО мають відповідати стандартам, які визначені Переліком стандартів, що застосовуються кваліфікованими надавачами електронних довірчих послуг під час надання кваліфікованих електронних довірчих послуг, та вимогам до технічних засобів, у тому числі до алгоритмів, форматів, структури, протоколів та інтерфейсів, які реалізуються такими засобами, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання кваліфікованих електронних довірчих послуг, які встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг та спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв’язку та захисту інформації відповідно до постанови Кабінету Міністрів України від 16 грудня 2015 року № 1057 «Про визначення сфер діяльності, в яких центральні органи виконавчої влади та Служба безпеки України здійснюють функції технічного регулювання» (далі – Постанова).

ІІ. Перелік кваліфікованих електронних довірчих послуг, надання яких забезпечує Адміністратор ІТС ЦЗО

1. Адміністратор ІТС ЦЗО надає кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого

сертифіката електронного підпису чи печатки надавачам з урахуванням вимог статті 29 Закону України «Про електронні довірчі послуги» (далі – Закон).

2. Адміністратор ІТС ЦЗО надає кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки безоплатно для органів державної влади, місцевого самоврядування, інших юридичних осіб публічного права.

3. Адміністратор ІТС ЦЗО надає кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачам з урахуванням пункту 2 цього розділу відповідно до тарифів, затверджених в установленому законодавством порядку.

ІІІ. Посадовий склад та функції найманих працівників Адміністратора ІТС ЦЗО

1. Для виконання технічних та технологічних функцій ЦЗО Адміністратор ІТС ЦЗО створює технічний підрозділ, який складається з:

посадової особи, на яку покладено обов’язки керівника технічного підрозділу;

адміністратора реєстрації;

адміністратора сертифікації;

адміністратора безпеки та аудиту;

системного адміністратора.

Посада адміністратора безпеки та аудиту не має суміщатися з іншими посадами найманих працівників, обов’язки яких безпосередньо пов’язані з наданням послуг.

2. Наймані працівники повинні мати необхідні для надання послуг знання, досвід і кваліфікацію.

На посади адміністратора сертифікації, системного адміністратора, адміністратора безпеки та аудиту може бути призначена особа, яка має вищу

освіту за спеціальністю у сферах інформаційних технологій, захисту інформації або кібербезпеки, а також стаж роботи за фахом в зазначених сферах не менше 3 років.

3. Керівник та наймані працівники повинні бути ознайомлені з положеннями їх посадових інструкцій та діяти відповідно до своїх посадових функцій та завдань.

4. З метою забезпечення захисту інформації в ІТС ЦЗО шляхом вирішення питань, пов’язаних з проектуванням, розробленням, модернізацією, введенням в експлуатацію та підтримкою працездатності комплексної системи захисту інформації (далі – КСЗІ), та додержання режиму безпеки в ІТС ЦЗО створюється підрозділ служби захисту інформації (далі – СЗІ).

До складу СЗІ входять:

посадова особа, на яку покладено обов’язки керівника СЗІ;

адміністратор безпеки та аудиту;

системний адміністратор.

Основними функціями СЗІ є:

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

розроблення розпорядчих документів, згідно з якими Адміністратор ІТС ЦЗО має забезпечувати захист інформації, контроль за їх виконанням;

своєчасне реагування на спроби несанкціонованого доступу до інформаційних ресурсів ІТС ЦЗО, порушення правил експлуатації засобів захисту інформації.

Обов’язки керівника СЗІ покладаються на посадову особу, на яку покладено обов’язки керівника технічного підрозділу.

Керівник СЗІ забезпечує належне виконання СЗІ її функцій.

5. Адміністратор реєстрації забезпечує належну перевірку документів, наданих заявниками, їх заяв про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого

сертифіката електронного підпису чи печатки надавачу, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів.

Основними обов’язками адміністратора реєстрації є:

1) ідентифікація та автентифікація заявників;

2) перевірка заяв про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів;

3) встановлення належності відкритого ключа та відповідного йому особистого ключа надавачу;

4) ведення обліку надавачів та контроль за розрахунками за надану їм кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;

5) ведення архіву.

6. Адміністратор сертифікації забезпечує належне формування сертифікатів ключів, ведення Довірчого списку та електронного реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів, зберігання та використання особистих ключів ЦЗО, а також створення їх резервних копій.

Основними обов’язками адміністратора сертифікації є:

1) участь у генерації пар ключів ЦЗО та створенні резервних копій особистих ключів ЦЗО;

2) зберігання особистих ключів ЦЗО та їх резервних копій;

3) ведення Довірчого списку;

4) забезпечення використання особистих ключів ЦЗО під час формування та обслуговування сертифікатів ключів ЦЗО та кваліфікованих сертифікатів відкритих ключів надавачів, а також внесення відомостей до Довірчого списку;

5) перевірка заяв про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката

електронного підпису чи печатки надавачу на відповідність вимогам цього Регламенту;

6) участь у знищенні особистих ключів ЦЗО;

7) ведення, архівування та відновлення баз даних кваліфікованих сертифікатів відкритих ключів надавачів;

8) публікація кваліфікованих сертифікатів відкритих ключів надавачів та СВС на офіційному вебсайті ЦЗО;

9) створення резервних копій сертифікатів ключів ЦЗО та Довірчого списку;

10) зберігання кваліфікованих сертифікатів відкритих ключів надавачів, їх резервних копій, СВС та інших важливих ресурсів ІТС ЦЗО.

7. Адміністратор безпеки та аудиту забезпечує належне функціонування КСЗІ та здійснення перевірок дотримання найманими працівниками вимог внутрішньої організаційно-розпорядчої документації та документації на КСЗІ.

Основними обов’язками адміністратора безпеки та аудиту є:

1) участь у генерації пар ключів та створенні резервних копій особистих ключів ЦЗО;

2) контроль за формуванням, обслуговуванням та створенням резервних копій сертифікатів ключів ЦЗО, кваліфікованих сертифікатів відкритих ключів надавачів та СВС;

3) контроль за зберіганням особистих ключів ЦЗО та їх резервних копій, особистих ключів адміністраторів;

4) участь у знищенні особистих ключів ЦЗО, контроль за правильним і своєчасним знищенням адміністраторами їх особистих ключів;

5) організація розмежування доступу до ресурсів ІТС ЦЗО;

6) спостереження за функціонуванням КСЗІ (реєстрація подій в ІТС ЦЗО, моніторинг подій тощо);

7) організація та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій ІТС ЦЗО;

8) забезпечення режиму доступу до приміщень ЦЗО, в яких розміщена ІТС ЦЗО;

9) ведення журналів обліку адміністратора безпеки та аудиту, передбачених документацією на КСЗІ;

10) здійснення перевірок журналів аудиту подій, що реєструють технічні засоби ІТС ЦЗО;

11) здійснення перевірок відповідності внутрішньої організаційно-розпорядчої документації ЦЗО та документації на КСЗІ;

12) контроль за дотриманням найманими працівниками внутрішньої організаційно-розпорядчої документації та документації на КСЗІ;

13) контроль за веденням баз даних;

14) контроль за веденням архіву.

8. Системний адміністратор забезпечує належне функціонування засобів та обладнання програмно-технічного комплексу (далі – технічні засоби) ІТС ЦЗО.

Основними обов’язками системного адміністратора є:

1) організація експлуатації та технічного обслуговування ІТС ЦЗО і адміністрування її технічних засобів;

2) забезпечення функціонування офіційного вебсайту ЦЗО;

3) участь у впровадженні та забезпеченні функціонування КСЗІ;

4) налаштування ведення журналів аудиту подій, що реєструють технічні засоби ІТС ЦЗО;

5) встановлення, налаштування та забезпечення підтримки працездатності загальносистемного та спеціального програмного забезпечення ІТС ЦЗО;

6) встановлення та налагодження штатної підсистеми резервного копіювання бази даних ІТС ЦЗО;

7) забезпечення актуалізації баз даних, створюваних та оброблюваних в ІТС ЦЗО, після збоїв.

IV. Політика сертифіката

1. Сфера використання кваліфікованих сертифікатів відкритих ключів ЦЗО та надавачів

1. Адміністратор ІТС ЦЗО формує кваліфікований самопідписаний сертифікат відкритого ключа електронної печатки ЦЗО (далі – самопідписаний сертифікат електронної печатки ЦЗО) з обов'язковими реквізитами відповідно до таблиці 2 додатка 1 до цього Регламенту, що містить відкритий ключ, відповідний йому особистий ключ ЦЗО, призначений для формування кваліфікованих сертифікатів відкритих ключів надавачів та СВС.

Для засвідчення інформації в Довірчому списку та даних про статус кваліфікованих сертифікатів відкритих ключів надавачів, що визначаються в режимі реального часу, використовуються окремі спеціально призначені кваліфіковані сертифікати відкритого ключа електронної печатки ЦЗО, засвідчені з використанням самопідписаного сертифіката електронної печатки ЦЗО.

Використання особистих та відповідних їм відкритих ключів за іншим призначенням (сферою використання) здійснюється з урахуванням пункту 1 глави 5 цього розділу.

2. Адміністратор ІТС ЦЗО формує кваліфіковані сертифікати відкритих ключів надавачів, що містять відкриті ключі, відповідні їм особисті ключі, призначені для формування сертифікатів ключів підписувачів, створювачів електронних печаток, СВС, надання інших кваліфікованих електронних довірчих послуг, передбачених частиною другою статті 16 Закону.

Для кожної кваліфікованої електронної довірчої послуги надавачі використовують окремий кваліфікований сертифікат відкритого ключа, сформований Адміністратором ІТС ЦЗО.

Під час розгляду заяви про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу Адміністратор ІТС ЦЗО

здійснює перевірку унікальності відкритого ключа надавача в електронному реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів. Засвідчення відкритого ключа, який не пройшов перевірку на унікальність в електронному реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів, забороняється.

2. Порядок розповсюдження інформації ЦЗО

1. На офіційному вебсайті ЦЗО розповсюджується (публікується) така інформація:

Довірчий список;

електронний реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів;

сертифікати відкритих ключів ЦЗО;

СВС;

рішення ЦЗО про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку;

відомості про прийняття від надавачів на зберігання документованої інформації у разі припинення їх діяльності;

нормативно-правові акти, що регулюють відносини у сфері електронних довірчих послуг, цей Регламент, форма договору про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки та інших документів, методичні та довідкові матеріали;

інформація щодо поточної діяльності ЦЗО.

2. Публікація чинних кваліфікованих сертифікатів відкритих ключів ЦЗО та надавачів здійснюється відповідно до Порядку ведення реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів, затвердженого наказом Міністерства цифрової трансформації 29 липня 2020 року № 112, зареєстрованого в Міністерстві юстиції України 18 серпня 2020 року за № 798/35081.

Доступ до сертифікатів ключів ЦЗО та кваліфікованих сертифікатів відкритих ключів надавачів забезпечується цілодобово.

3. Інформація щодо скасованих та блокованих кваліфікованих сертифікатів відкритих ключів надавачів публікується на офіційному вебсайті ЦЗО у вигляді повного та часткового СВС.

4. Повні СВС публікуються не рідше одного разу на тиждень не пізніше закінчення строку дії попереднього СВС та містять інформацію про всі відкликані сертифікати ключів, які були сформовані Адміністратором ІТС ЦЗО.

5. Часткові СВС публікуються не рідше одного разу на дві години не пізніше закінчення строку дії попереднього СВС та містять інформацію про всі відкликані сертифікати ключів, статус яких був змінений в інтервалі між часом випуску останнього повного СВС та часом формування поточного часткового СВС.

Доступ до СВС забезпечується цілодобово.

3. Порядок ідентифікації та автентифікації надавачів

1. Адміністратор ІТС ЦЗО здійснює ідентифікацію, автентифікацію та перевірку обсягу цивільної правоздатності та дієздатності заявників під час формування, блокування, скасування та поновлення кваліфікованого сертифіката відкритого ключа надавача на підставі відповідної заяви надавача з дотриманням вимог статті 22 Закону.

2. Для надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки Адміністратор ІТС ЦЗО здійснює ідентифікацію заявника шляхом перевірки ідентифікаційних даних особи з документів, що надаються заявником, та даних, одержаних з інформаційних систем органів державної влади.

3. Ідентифікація юридичної особи здійснюється за її установчими документами та даними, одержаними з Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань.

4. Ідентифікація фізичної особи здійснюється за паспортом громадянина України або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи.

5. Перевірка обсягів повноважень уповноваженого представника юридичної особи здійснюється за документом або за даними з Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань, що визначають повноваження представника.

6. Перевірка обсягів повноважень уповноваженого представника колегіального органу юридичної особи здійснюється за документом, у якому визначено повноваження відповідного органу та розподіл обов’язків між його членами.

7. Перевірка обсягів повноважень фізичної особи – підприємця здійснюється за даними з Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань.

8. Ідентифікація іноземців здійснюється відповідно до законодавства.

9. Підтвердження володіння надавачем особистим ключем, відповідним йому відкритим ключем, який надається для сертифікації, здійснюється шляхом електронної автентифікації з використанням алгоритмів криптографічного захисту інформації, реалізованих засобами ІТС ЦЗО.

10. Механізм підтвердження володіння надавачем особистим ключем являє собою перевірку удосконаленого електронного підпису чи печатки, накладеного(ї) на запит на формування сертифіката ключа, особистим ключем надавача за допомогою відкритого ключа, що міститься у запиті.

11. Підтвердження володіння надавачем особистим ключем здійснюється без розкриття особистого ключа.

4. Управління та операційний контроль

1. Фізичне середовище:

1) програмно-технічний комплекс ЦЗО розташовується та експлуатується згідно з вимогами до умов експлуатації та за місцезнаходженням, що зазначені в експертному висновку за результатами державної експертизи у сфері технічного захисту інформації, який є невід'ємною частиною атестата відповідності комплексної системи захисту інформації вимогам нормативних документів у сфері захисту інформації;

2) у локальній обчислювальній мережі (далі – ЛОМ) управління ІТС ЦЗО об'єднані робочі станції найманих працівників, на яких покладено виконання обов'язків адміністратора реєстрації, адміністратора сертифікації, адміністратора безпеки та аудиту, системного адміністратора (далі – адміністратори) з використанням комутаційного обладнання, розміщуються відокремлено від серверів і підключаються до ЛОМ серверів ІТС ЦЗО через телекомунікаційні мережі загального користування. Підключення здійснюється через шлюз захисту мережевих з'єднань, який розміщується на стороні ЛОМ серверів ІТС ЦЗО так, що утворюється єдина віртуальна ЛОМ. Шлюз захисту мережевих з'єднань призначений для автентифікації адміністраторів під час

підключення до ЛОМ серверів шляхом встановлення захищеного мережевого з’єднання з робочими станціями адміністраторів;

3) приміщення, де розміщено ЛОМ серверів ІТС ЦЗО, обладнуються згідно з вимогами до спеціальних приміщень надавачів, які передбачають проведення заходів щодо пасивного захисту інформації від її витоку каналами побічних електромагнітних випромінювань та наведень, а також від порушення її цілісності внаслідок деструктивного впливу зовнішніх електромагнітних полів (далі – спеціальне приміщення);

4) спеціальне приміщення обладнується автоматичною системою контролю доступу, яка забезпечує фізичний доступ до приміщень тільки особам, визначеним наказом керівника Адміністратора ІТС ЦЗО;

5) фізичний доступ до обладнання програмно-технічного комплексу, що забезпечує сертифікацію, управління статусом сертифіката, генерацію ключів ЦЗО, обмежується та надається тільки визначеному колу осіб із числа найманих працівників;

6) Адміністратор ІТС ЦЗО вживає запобіжних заходів щодо недопущення крадіжки, втрати та ушкодження обладнання, крадіжки та знищення (руйнування) інформації або інших дій, що можуть призвести до виведення ІТС ЦЗО із штатного режиму роботи;

7) спеціальні приміщення використовуються для розташування технічних засобів, за допомогою яких здійснюються генерація та використання особистих ключів ЦЗО, а також обробки інформації, необхідність технічного захисту якої визначена у технічному завданні на створення КСЗІ;

8) технічний захист інформації, в тому числі захист від впливу зовнішніх електромагнітних полів, у спеціальних приміщеннях здійснюється шляхом створення умов для забезпечення електромагнітного екранування технічних засобів та розміщення шаф в один із таких способів:

суцільне екранування усієї внутрішньої поверхні спеціальних приміщень;

розміщення технічних засобів та шаф в окремій екранованій кабіні (декількох кабінах);

розміщення у неекранованих спеціальних приміщеннях лише екранованих шаф і технічних засобів в екранованому виконанні;

9) спеціальні приміщення відокремлюються від зовнішніх стін (з боку оточуючої міської забудови) коридорами тощо;

10) вікна спеціального приміщення обладнуються надійними металевими ґратами, захищаються від зовнішнього спостереження за допомогою скла з матовою чи рельєфною поверхнею (нерівностями назовні), непрозорих штор;

11) спеціальні приміщення обладнуються системою контролю доступу та пожежною сигналізацією. Двері спеціальних приміщень обладнуються кодовим замком або системою доступу;

12) величина ефективності екранування спеціальних приміщень (інших варіантів пасивного захисту) та екранованих шаф для зберігання має складати не менше 20 дБ у діапазоні частот 0,15 – 1000 МГц щодо захисту від впливів зовнішніх електромагнітних полів;

13) розроблення, виготовлення, монтаж і визначення ефективності екранування спеціальних приміщень проводяться відповідно до вимог нормативних документів з питань технічного захисту інформації, що стосуються екранованих приміщень;

14) спеціальні екрановані приміщення (окрема екранована кабіна (шафа), технічні засоби в екранованому виконанні) оснащуються:

протизавадними фільтрами для захисту вводів мереж електроживлення;

протизавадними фільтрами конструкції типу "позамежний хвильовід" для захисту місць вводу систем опалення, вентиляції і кондиціонування повітря;

іншими відповідними протизавадними фільтрами (у разі необхідності) для захисту вводів оптоволоконних, сигнальних мереж тощо;

15) протизавадні фільтри за своїми характеристиками мають забезпечувати ефективність екранування у всьому діапазоні частот екранування не нижче величин, визначених у підпункті 12 цього пункту;

16) екрануючі поверхні спеціальних приміщень (інші варіанти пасивного захисту) та екранованих шаф не повинні мати гальванічного зв’язку з

металоконструкціями будівлі (коробами, екрануючими та захисними оболонками кабелів тощо), що мають вихід за межі контрольованої зони Адміністратора ІТС ЦЗО;

17) для електроживлення технічних засобів, що розміщуються у спеціальних приміщеннях, спільно з протизавадними фільтрами захисту кіл електроживлення встановлюються пристрої безперервного електроживлення;

18) система заземлення спеціальних приміщень та їх складових елементів обладнується відповідно до вимог до спеціальних приміщень.

2. Контроль доступу:

1) Адміністратор ІТС ЦЗО передбачає та впроваджує захист внутрішньої обчислювальної мережі від несанкціонованого доступу з боку користувачів зовнішньої мережі (глобальних мереж), у тому числі надавачів та третіх сторін. Засоби контролю доступу до інформаційних ресурсів ЦЗО здійснюють блокування всіх мережевих протоколів та спроб доступу, що необов’язкові для функціонування ІТС ЦЗО;

2) Адміністратор ІТС ЦЗО забезпечує розмежування доступу найманих працівників до ресурсів системи та надання функцій згідно з їх авторизацією так, щоб наймані працівники виконували лише ті функції, що доступні та асоційовані з їх функціями та завданнями;

3) наймані працівники повинні бути успішно ідентифіковані та автентифіковані перед початком виконання процедур, пов’язаних із формуванням сертифіката ключа або зміною його статусу;

4) всі дії найманих працівників, пов’язані із генерацією пар ключів, формуванням сертифікатів відкритих ключів або зміною їх статусу, протоколюються із забезпеченням захисту протоколів від несанкціонованого доступу;

5) резервні копії сертифікатів відкритих ключів та журналів аудиту подій зберігаються в окремому приміщенні Адміністратора ІТС ЦЗО із забезпеченням їх захисту від несанкціонованого доступу;

6) програмно-технічний комплекс має забезпечувати реєстрацію дій найманих працівників;

7) журнали аудиту подій повинні мати захист від несанкціонованого доступу, модифікації або знищення (руйнування) інформації.

3. Процедурний контроль:

1) посадові особи, на яких покладено обов'язки керівника технічного підрозділу, адміністратора реєстрації, адміністратора сертифікації, адміністратора безпеки та аудиту, системного адміністратора, забезпечують належне виконання своїх обов'язків, нерозголошення конфіденційної інформації, зокрема відомостей про персональні дані надавачів, згідно із законом;

2) інші обов'язки посадових осіб, зокрема обов'язки керівника технічного підрозділу, адміністратора реєстрації, адміністратора сертифікації, адміністратора безпеки та аудиту, системного адміністратора, визначаються розпорядчими документами Адміністратора ІТС ЦЗО та документацією КСЗІ ІТС ЦЗО.

4. Ведення журналів аудиту подій:

1) у журналах аудиту подій ІТС ЦЗО реєструються дії та події таких типів:

спроби створення, знищення, встановлення паролів, зміни прав доступу в ІТС ЦЗО тощо;

заміна технічних засобів ІТС ЦЗО та пар ключів;

формування, блокування, скасування та поновлення сертифікатів ключів, формування всіх СВС;

спроби несанкціонованого доступу до ІТС ЦЗО;

надання доступу персоналу до ІТС ЦЗО;

зміна системних конфігурацій та технічне обслуговування ІТС ЦЗО;

збої в роботі ІТС ЦЗО;

інші події, відомості про які фіксуються в журналі аудиту подій ІТС ЦЗО;

2) усі записи в журналах аудиту подій в електронній або паперовій формі повинні містити дату та час дії або події, а також ідентифікувати суб’єкта, що її здійснив або ініціював.

Системний адміністратор забезпечує належне ведення журналів аудиту подій, що реєструють технічні засоби ІТС ЦЗО;

3) журнали аудиту подій підлягають перегляду не рідше одного разу на тиждень. Перегляд передбачає перевірку журналу аудиту подій на предмет несанкціонованих модифікацій, вивчення всіх дій та/або подій у журналі аудиту подій зі зверненням особливої уваги на повідомлення про невідповідності та попередження про небезпечні ситуації.

Перегляд журналів аудиту подій ІТС ЦЗО здійснює адміністратор безпеки та аудиту. Результати перегляду адміністратор безпеки та аудиту фіксує у відповідному журналі;

4) система ведення електронного журналу аудиту подій має бути синхронізована із Всесвітнім координованим часом із точністю до секунди та містити механізми його захисту від неавторизованого перегляду, модифікації і знищення.

Журнали аудиту подій в електронній формі резервуються з періодичністю не менше одного разу на тиждень;

5) Адміністратор ІТС ЦЗО зберігає журнали аудиту подій на місці їх створення протягом 10 років, після чого забезпечує їх передавання для архівного зберігання.

5. Ведення архівів ЦЗО:

1) архівування інформації здійснюється згідно із внутрішніми організаційно-розпорядчими документами Адміністратора ІТС ЦЗО;

2) обов’язковому архівуванню підлягають:

сертифікати відкритих ключів ЦЗО, серверів ЦЗО та адміністраторів;

кваліфіковані сертифікати відкритих ключів надавачів;

запити на формування сертифікатів відкритих ключів в електронній формі;

журнали аудиту подій ІТС ЦЗО;

укладені договори про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;

документи та копії документів, що використовуються під час ідентифікації та автентифікації;

заяви про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу, скасування, блокування та поновлення кваліфікованих сертифікатів відкритих ключів надавачів;

3) документи у паперовій та електронній формах мають зберігатися у порядку, встановленому законодавством у сфері архівної справи;

4) знищення архівних документів має здійснюватися комісією, до складу якої входять керівник Адміністратора ІТС ЦЗО, адміністратор сертифікації, адміністратор безпеки та аудиту. Після завершення процедури знищення архівних документів складається відповідний акт, який затверджує керівник Адміністратора ІТС ЦЗО;

5) сертифікати відкритих ключів ЦЗО, сертифікати відкритих ключів серверів ЦЗО та сертифікати відкритих ключів адміністраторів, кваліфіковані сертифікати відкритих ключів надавачів, а також СВС зберігаються постійно;

6) для зберігання носіїв з резервними та архівними копіями виділяється окреме сховище (сейф чи відсік сейфу) з двома екземплярами ключів і пристроями для опечатування. Один екземпляр ключа від сховища знаходиться у адміністратора безпеки та аудиту, другий – в опечатаному вигляді зберігається у сховищі (сейфі) керівника СЗІ ІТС ЦЗО;

7) засоби, що входять до складу центрального сервера автоматизованої системи ЦЗО, забезпечують автоматичне резервне копіювання сертифікатів відкритих ключів. Автоматичне створення резервної копії має виконуватися не рідше одного разу на добу під час найменшого завантаження центрального сервера;

8) додатково може виконуватися резервне копіювання сертифікатів відкритих ключів на оптичні носії або інші з'ємні носії інформації у ручному режимі. Після створення нової резервної копії попередня стає архівною;

9) відновлення сертифікатів відкритих ключів з резервної копії здійснюється засобами центрального сервера комплексу шляхом зчитування сертифікатів відкритих ключів з останньої (актуальної) резервної копії та запису їх у базу даних сервера;

10) з'ємні носії зберігаються у конвертах чи упаковках, що опечатуються печаткою адміністратора сертифікації, при цьому на упаковці зазначається обліковий номер копії. Факти створення та використання копій фіксуються в окремому журналі;

11) архівні копії журналів реєстрації зберігаються в приміщенні Адміністратора ІТС ЦЗО не менше 2 років. Контроль за здійсненням автоматичного резервного копіювання та виконання резервного копіювання в ручному режимі покладаються на системного адміністратора. Адміністратор безпеки та аудиту періодично контролює процес створення та зберігання резервних копій;

12) архівне приміщення обладнується технічними засобами, які виключають можливість проникнення сторонніх осіб та неконтрольованого доступу до інформації, що підлягає архівуванню;

13) надавач, що засвідчив свій відкритий ключ у ЦЗО, у разі припинення діяльності з надання послуг здійснює передавання документованої інформації Адміністратору ІТС ЦЗО;

14) механізм обов'язкового передавання на зберігання Адміністратору ІТС ЦЗО сертифікатів ключів, документованої інформації надавачем у разі припинення його діяльності з надання послуг, а також забезпечення передавання її на архівне зберігання визначаються Порядком зберігання документованої інформації та її передавання центральному засвідчувальному органу в разі припинення діяльності кваліфікованого надавача електронних довірчих послуг,

затвердженим постановою Кабінету Міністрів України від 10 жовтня 2018 року № 821.

5. Управління парами ключів ЦЗО

1. В ІТС ЦЗО використовуються особисті та відповідні їм відкриті ключі за такими призначеннями (сферою використання) та з такими параметрами:

особисті та відповідні їм відкриті ключі ЦЗО для накладення та перевірки електронної печатки ЦЗО на кваліфікованих сертифікатах відкритих ключів надавачів та СВС зі ступенем розширення основного поля еліптичної кривої не менше 431 згідно з ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння", затвердженим наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31 (далі – ДСТУ 4145-2002);

особисті та відповідні їм відкриті ключі ЦЗО для накладення та перевірки електронної печатки ЦЗО на Довірчому списку зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;

особисті та відповідні їм відкриті ключі ЦЗО для накладення та перевірки електронної печатки ЦЗО на даних про статус кваліфікованих сертифікатів відкритих ключів надавачів, що визначається в режимі реального часу, зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;

особисті та відповідні їм відкриті ключі шлюзів захисту мережевих з’єднань та шифраторів мережевого потоку зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;

особисті та відповідні їм відкриті ключі адміністраторів, що використовуються для криптографічного захисту мережевих з’єднань, зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;

особисті та відповідні їм відкриті ключі ЦЗО для накладення та перевірки електронної печатки ЦЗО на кваліфікованих сертифікатах відкритих ключів

надавачів, СВС із використанням іменованої еліптичної кривої NIST P-256 (secp256r1) для алгоритму ECDSA згідно з ДСТУ ETSI TS 119 312:2015 «Електронні підписи й інфраструктури (ESI). Криптографічні комплекти» (далі – ДСТУ ETSI EN 119 312:2015);

особисті та відповідні їм відкриті ключі ЦЗО для накладення та перевірки електронної печатки ЦЗО на даних про статус кваліфікованих сертифікатів відкритих ключів надавачів, що визначається в режимі реального часу, із використанням іменованої еліптичної кривої NIST P-256 (secp256r1) для алгоритму ECDSA згідно з ДСТУ ETSI EN 119 312:2015;

особисті та відповідні їм відкриті ключі ЦЗО для накладення та перевірки електронної печатки ЦЗО на кваліфікованих сертифікатах відкритих ключів надавачів, СВС з довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI EN 119 312:2015;

особисті та відповідні їм відкриті ключі ЦЗО для накладення та перевірки електронної печатки ЦЗО на Довірчому списку з довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI EN 119 312:2015;

особисті та відповідні їм відкриті ключі ЦЗО для накладення та перевірки електронної печатки ЦЗО на даних про статус кваліфікованих сертифікатів відкритих ключів надавачів, що визначається в режимі реального часу, з довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI EN 119 312:2015.

2. Процедури генерації особистих та відповідних їм відкритих ключів, що використовуються в ІТС ЦЗО, створення резервних копій, відновлення з резервних копій, використання та знищення особистих ключів, що використовуються в ІТС ЦЗО, здійснюються в частині, що не суперечить вимогам цього Регламенту, а також з урахуванням встановлених Державною службою спеціального зв’язку та захисту інформації України вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації.

3. Генерація особистих та відповідних їм відкритих ключів ЦЗО здійснюється у спеціальному приміщенні ІТС ЦЗО адміністратором сертифікації під контролем адміністратора безпеки та аудиту.

4. Після генерації особистих та відкритих ключів ЦЗО здійснюється формування відповідних сертифікатів ключів.

5. Строки дії особистих ключів ЦЗО відповідають строкам чинності сертифікатів відповідних їм відкритих ключів і становлять:

для особистих ключів ЦЗО для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів надавачів та СВС – не більше 10 років;

для особистих ключів ЦЗО для накладення електронної печатки ЦЗО на дані про статус кваліфікованих сертифікатів відкритих ключів надавачів, що визначається в режимі реального часу, – не більше 5 років;

для особистих ключів ЦЗО для накладення електронної печатки ЦЗО на Довірчому списку – не більше 2 років;

для особистих ключів шлюзу захисту мережевих з’єднань – не більше 2 років;

для особистих ключів адміністраторів – не більше 2 років.

6. Планова заміна особистого та відповідного йому відкритого ключа ЦЗО виконується не пізніше ніж за 20 робочих днів до закінчення строку дії відповідного сертифіката ключа на підставі окремого наказу Мінцифри.

7. Під час планової заміни особистого та відповідного йому відкритого ключа ЦЗО адміністратором сертифікації і адміністратором безпеки та аудиту відповідно до вимог пунктів 2 – 5 цієї глави здійснюється генерація нових особистого та відповідного йому відкритого ключа ЦЗО, формування відповідного сертифіката відкритого ключа та створення резервних копій особистого ключа.

8. Після введення в дію нових особистого та відповідного йому відкритого ключа ЦЗО особистий ключ, який належить до пари ключів, для якої завершився термін дії сертифіката відкритого ключа, та всі його резервні копії знищуються способом, що унеможливлює їх відновлення, за участю адміністратора сертифікації та адміністратора безпеки та аудиту.

9. Позапланова заміна особистого та відповідного йому відкритого ключа ЦЗО здійснюється у випадках компрометації або підозри на компрометацію особистого ключа ЦЗО та/або особистого ключа одного із адміністраторів.

10. Під час позапланової заміни особистого та відповідного йому відкритого ключа ЦЗО адміністратором сертифікації та адміністратором безпеки та аудиту відповідно до вимог пунктів 2 – 5 цієї глави здійснюються генерація нових особистого та відповідного йому відкритого ключа ЦЗО, формування відповідного сертифіката відкритого ключа та створення резервних копій особистого ключа.

11. У разі підтвердження факту компрометації особистих ключів ЦЗО для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів та СВС усі попередньо сформовані кваліфіковані сертифікати відкритих ключів надавачів та сертифікат ключа для перевірки електронної печатки ЦЗО на Довірчому списку скасовуються та формується СВС, який підписується з використанням нового особистого ключа ЦЗО для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів надавачів та СВС.

12. Усі особисті ключі ЦЗО та особисті ключі адміністраторів, факт компрометації яких було підтверджено, знищуються способом, що унеможливлює їх відновлення, за участю двох адміністраторів, у тому числі адміністратора безпеки та аудиту.

13. Факти знищення особистих ключів ЦЗО, особистих ключів адміністраторів та їх резервних копій реєструються адміністратором безпеки та аудиту у відповідному журналі обліку.

14. Не пізніше завершення половини строку дії поточного особистого та відповідного йому відкритого ключів ЦЗО для накладення та перевірки електронної печатки ЦЗО на кваліфікованих сертифікатах відкритих ключів надавачів та СВС здійснюються генерація нових особистого та відповідного йому відкритого ключа ЦЗО для накладення та перевірки електронної печатки ЦЗО на кваліфікованих сертифікатах відкритих ключів надавачів та СВС та формування відповідного сертифіката ключа, при цьому поточний особистий ключ ЦЗО для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів надавачів та СВС стає попереднім, а новий – поточним.

15. Адміністратор ІТС ЦЗО невідкладно інформує надавачів, Мінцифри та контролюючий орган про здійснення планової чи позапланової заміни особистих та відкритих ключів ЦЗО.

6. Забезпечення захисту особистого ключа ЦЗО

1. Особисті ключі ЦЗО для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів та СВС, особисті ключі ЦЗО для накладення електронної печатки ЦЗО на Довірчому списку та особисті ключі ЦЗО для накладення електронної печатки ЦЗО на дані про статус кваліфікованих сертифікатів відкритих ключів надавачів, що визначається в режимі реального часу, розміщуються у засобі кваліфікованого електронного підпису чи печатки, що є апаратно-програмним або апаратним пристроєм, за допомогою якого здійснювалася генерація пари ключів.

2. Для зберігання особистих ключів шлюзів захисту мережевих з’єднань, шифраторів мережевого потоку та особистих ключів адміністраторів застосовують виключно засоби кваліфікованого електронного підпису чи печатки, які відповідають вимогам, встановленим частинами першою та другою статті 19 Закону.

3. Поточні особисті ключі ЦЗО для накладення електронної печатки ЦЗО на кваліфікованих сертифікатах відкритих ключів надавачів та СВС мають зберігатися, застосовуватися у засобах кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями і входять до складу ІТС ЦЗО, та використовуватися для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів надавачів та СВС.

4. Попередні особисті ключі ЦЗО для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів та СВС мають розміщуватися у засобі кваліфікованого електронного підпису чи печатки, що є апаратно-програмним або апаратним пристроєм, за допомогою якого здійснювалася генерація пари ключів, та використовуватися для обслуговування кваліфікованих сертифікатів відкритих ключів надавачів, які були сформовані за допомогою цих ключів.

5. Передавання особистих ключів ЦЗО здійснюється за актом приймання-передавання ключів.

Забороняється:

передавання особистих ключів адміністраторів між адміністраторами;

виносити особисті ключі ЦЗО та їх резервні копії із спеціального приміщення ІТС ЦЗО.

6. Резервне копіювання та відновлення особистих ключів ЦЗО здійснюються адміністратором сертифікації під контролем адміністратора безпеки та аудиту.

7. Для забезпечення можливості відновлення особистого ключа ЦЗО для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів та СВС, особистого ключа ЦЗО для накладення електронної печатки ЦЗО на Довірчий список, особистого ключа ЦЗО для накладення електронної печатки ЦЗО на дані про статус кваліфікованих сертифікатів відкритих ключів надавачів, що визначається в режимі реального часу, у разі виходу з ладу засобів

кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями, виконується резервне копіювання відповідного особистого ключа із такого засобу виключно на засоби кваліфікованого електронного підпису чи печатки, які відповідають вимогам, встановленим частинами першою та другою статті 19 Закону.

8. Для забезпечення можливості відновлення особистих ключів шлюзів захисту мережевих з’єднань, шифраторів мережевого потоку та особистих ключів адміністраторів у разі виходу з ладу засобу кваліфікованого електронного підпису чи печатки виконується резервне копіювання особистого ключа з цих засобів на окремі резервні засоби кваліфікованого електронного підпису чи печатки, які відповідають вимогам, встановленим частинами першою та другою статті 19 Закону.

9. Факти генерації та створення резервних копій особистого ключа ЦЗО для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів та СВС, особистого ключа ЦЗО для накладення електронної печатки ЦЗО на Довірчий список, особистого ключа ЦЗО для накладення електронної печатки ЦЗО на дані про статус кваліфікованих сертифікатів відкритих ключів надавачів, що визначається в режимі реального часу, особистих ключів шлюзів захисту мережевих з’єднань, особистих ключів шифраторів мережевого потоку, особистих ключів адміністраторів та відповідних їм відкритих ключів реєструються адміністратором безпеки та аудиту у відповідному журналі обліку.

10. Технічні специфікації форматів, які реалізуються у засобах кваліфікованого електронного підпису чи печатки, встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері електронних довірчих послуг, спільно зі спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв’язку та захисту інформації.

V. Положення сертифікаційних практик

1. Подання запиту на формування кваліфікованого сертифіката відкритого ключа

1. Адміністратор ІТС ЦЗО формує кваліфіковані сертифікати відкритих ключів юридичних осіб або фізичних осіб – підприємців, що мають намір надавати кваліфіковані електронні довірчі послуги, надавачам, які відповідають вимогам, встановленим частинами першою, другою та третьою статті 23 Закону, та забезпечує цілодобовий доступ до інформації про дату та час зміни статусу кваліфікованих сертифікатів відкритих ключів.

2. Формування кваліфікованого сертифіката відкритого ключа надавача здійснюється на підставі заяв про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу, визначених у додатку 2 (для надавача – юридичної особи) та у додатку 3 (для надавача – фізичної особи – підприємця) до цього Регламенту, що подаються до Адміністратора ІТС ЦЗО.

3. Заява про формування кваліфікованого сертифіката відкритого ключа подається до Адміністратора ІТС ЦЗО в електронній формі з накладенням кваліфікованого електронного підпису керівника юридичної особи чи його уповноваженої особи або фізичної особи – підприємця, шляхом надсилання її на електронну пошту Адміністратора ІТС ЦЗО: support.its@czo.gov.ua.

Під час прийому заяви про формування сертифіката відкритого ключа здійснюються ідентифікація, перевірка обсягу цивільної правоздатності та дієздатності представника юридичної особи або фізичної особи – підприємця (або його уповноваженої особи) шляхом перевірки ідентифікаційних даних особи з документів, що надаються заявником, та даних, одержаних з інформаційних систем органів державної влади, в тому числі в Єдиних та державних реєстрах.

4. Разом із заявою про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого

сертифіката електронного підпису чи печатки на електронну пошту Адміністратора ІТС ЦЗО надсилаються з накладенням кваліфікованого електронного підпису керівника юридичної особи чи його уповноваженою особою такі документи:

запит на формування сертифіката;

договір про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки.

5. Вимоги до запиту:

запит подається у форматі згідно зі специфікацією синтаксису запиту на сертифікацію (PKCS#10), що визначена RFC 2986 "PKCS #10: CertificationRequestSyntaxSpecification";

запит має містити інформацію про відкритий ключ надавача, що подає такий запит. Зазначена інформація визначається атрибутом "Інформація про відкритий ключ надавача" (subjectPublicKeyInfo), формат якого має відповідати технічним вимогам до технічних засобів та процесів їх використання у сфері електронних довірчих послуг, засобів криптографічного захисту інформації, процесів їх створення та функціонування у складі інформаційно-телекомунікаційних систем, які встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг та спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв’язку та захисту інформації, відповідно до Постанови.

Запит, крім обов’язкових реквізитів надавача в запиті на формування сертифіката ключа, що визначені таблицею 1 додатка 1 до цього Регламенту, та послуг надавача, може містити інші ідентифікаційні дані фізичних або юридичних осіб, необов’язкові додаткові спеціальні атрибути, визначені у стандартах для кваліфікованих сертифікатів відкритих ключів. Ці атрибути не мають впливати на інтероперабельність і визнання кваліфікованих електронних підписів.

Зазначені необов’язкові додаткові спеціальні атрибути визначаються атрибутом "Розширений запит" (extensionRequest), який має такий вигляд:

extensionRequest ATTRIBUTE : : = {

WITH SYNTAX ExtensionRequest

SINGLE VALUE TRUE

ID pkcs-9-at-extensionRequest

}

ExtensionRequest : : = Extensions.

6. Розгляд заяви про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу становить не більше двох робочих днів від дати прийняття заяви.

Під час розгляду заяви про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу здійснюється перевірка:

відповідності даних, внесених до заяви, документам надавача, отриманим від Мінцифри відповідно до встановленого порядку ведення Довірчого списку;

унікальності відкритого ключа послуги за відомостями реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

належності надавачу відповідного особистого ключа послуги шляхом перевірки удосконаленого електронного підпису чи печатки у запиті;

відповідності запиту вимогам, зазначеним у пункті 6 цієї глави.

7. У разі успішної перевірки Адміністратор ІТС ЦЗО формує кваліфікований сертифікат відкритого ключа надавача. У разі непроходження перевірки надавачу надається вмотивована відмова у формуванні сертифіката ключа та повертається заява про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу разом з додатками до неї.

8. Формування кваліфікованих сертифікатів відкритих ключів надавачів здійснюється адміністратором сертифікації під контролем адміністратора безпеки та аудиту.

9. Під час формування кваліфікованого сертифіката відкритого ключа додаткові розширення, що можуть міститись у запиті, встановлюються у кваліфікованому сертифікаті відкритого ключа надавача за умови, що вони були визначені як некритичні, а об’єктні ідентифікатори таких розширень зареєстровані у встановленому порядку.

2. Надання сформованого кваліфікованого сертифіката відкритого ключа надавачу

1. Після формування кваліфікованого сертифіката відкритого ключа надавача Адміністратор ІТС ЦЗО надсилає на електронну пошту надавача, зазначену в Довірчому списку та в електронному реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів, документи в електронній формі з накладенням кваліфікованого електронного підпису уповноваженої особи Адміністратора ІТС ЦЗО, а саме:

сформований/ні кваліфікований/ні сертифікат/ сертифікати надавача;

акт наданих послуг (для кожного із сертифікатів) про формування кваліфікованого сертифіката;

договір про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу.

2. За результатами проведеного формування та передавання кваліфікованого сертифіката відкритого ключа надавача Адміністратор ІТС ЦЗО надає уповноваженій особі надавача підписаний договір про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу та акт наданих послуг.

3. Умови використання кваліфікованих сертифікатів відкритих ключів та особистих ключів надавачів

1. Надавачі використовують пари ключів (особистих та відкритих) за призначенням (сферою використання) відповідно до технічних вимог до технічних засобів та процесів їх використання у сфері електронних довірчих послуг, засобів криптографічного захисту інформації, процесів їх створення та функціонування у складі інформаційно-телекомунікаційних систем, які встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг та спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв’язку та захисту інформації, відповідно до Постанови.

2. Під час надання послуг надавачі повинні використовувати пари ключів (особистих та відкритих) з такими параметрами:

зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;

зі ступенем розширення основного поля еліптичної кривої не менше 256 для алгоритму ECDSA згідно з ДСТУ ETSI EN 119 312:2015;

з довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI EN 119 312:2015.

3. Для обчислення значення геш-функції використовуються алгоритми, визначені до технічних вимог до технічних засобів та процесів їх використання у сфері електронних довірчих послуг, засобів криптографічного захисту інформації, процесів їх створення та функціонування у складі інформаційно-телекомунікаційних систем, які встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг та спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв’язку та захисту інформації, відповідно до Постанови.

4. Надавачі використовують особисті ключі тільки за призначенням (сферою використання) в період чинності відповідних кваліфікованих сертифікатів відкритих ключів, сформованих відповідно до цього Регламенту, та за умови, що цей сертифікат не був заблокований або скасований.

5. Надавачі забезпечують використання кваліфікованих сертифікатів відкритих ключів та особистих ключів тільки за призначенням (сферою використання), зазначених у пункті 2 глави 1 розділу IV цього Регламенту.

6. Під час надання кваліфікованих електронних довірчих послуг надавачі забезпечують обов’язковість перевірки строку чинності та статусу сформованих Адміністратором ЦЗО сертифікатів відкритих ключів.

7. Перед використанням будь-якого сертифіката відкритого ключа має забезпечуватись перевірка:

чинності кваліфікованого сертифіката відкритого ключа надавача на момент накладення кваліфікованого електронного підпису чи створення електронної печатки на документ або кваліфікованого електронного підпису чи печатки на документі;

чинності кваліфікованої електронної печатки ЦЗО, що була додана до кваліфікованого сертифіката відкритого ключа надавача за допомогою самопідписаного сертифіката ключа ЦЗО, чинного на момент формування кваліфікованого сертифіката відкритого ключа надавача;

статусу кваліфікованого сертифіката відкритого ключа надавача у режимі реального часу, якщо перевірка здійснюється на момент чинності цього сертифіката ключа або за СВС.

8. Під час перевірки статусу кваліфікованого сертифіката відкритого ключа надавача за СВС здійснюється перевірка автентичності, цілісності та терміну дії СВС.

4. Обставини та порядок зміни статусу (скасування, блокування, поновлення) кваліфікованого сертифіката відкритого ключа

1. Скасування кваліфікованого сертифіката відкритого ключа надавача:

1) скасування кваліфікованих сертифікатів відкритих ключів надавачів здійснюється у випадках, передбачених частинами першою, другою та третьою статті 25 Закону, на підставі заяви про скасування кваліфікованого сертифіката відкритого ключа надавача;

2) форми заяв про скасування кваліфікованого сертифіката відкритого ключа надавача, що подаються до Адміністратора ІТС ЦЗО, визначені у додатку 4 (для надавача – юридичної особи) та у додатку 5 (для надавача – фізичної особи – підприємця) до цього Регламенту;

3) заява про скасування кваліфікованого сертифіката відкритого ключа подається надавачем до Адміністратора ІТС ЦЗО в електронній формі, з накладенням кваліфікованого електронного підпису керівника юридичної особи чи його уповноваженої особи;

4) під час прийому заяви про скасування кваліфікованого сертифіката відкритого ключа здійснюється встановлення особи керівника юридичної особи – надавача (фізичної особи – підприємця, що є надавачем) або його уповноваженої особи та перевіряється достатність обсягу цивільної правоздатності і дієздатності шляхом перевірки ідентифікаційних даних особи з документів, що надаються заявником, та даних, одержаних з інформаційних систем органів державної влади, в тому числі в Єдиних та державних реєстрах;

5) не приймаються до розгляду заяви та документи, що не дають змоги однозначно тлумачити зміст, якщо кваліфікований електронний підпис не пройшов перевірку;

6) опрацювання заяви на скасування кваліфікованого сертифіката відкритого ключа та інформування Адміністратором ІТС ЦЗО надавача про скасування сертифіката ключа його послуги здійснюються протягом двох годин від моменту отримання заяви Адміністратором ІТС ЦЗО;

7) скасування кваліфікованого сертифіката відкритого ключа надавача здійснюється адміністратором сертифікації під контролем адміністратора безпеки та аудиту;

8) скасування кваліфікованого сертифіката відкритого ключа надавача набирає чинності з дати та часу здійснення цієї операції;

9) серійний номер скасованого кваліфікованого сертифіката відкритого ключа надавача вноситься до СВС із зазначенням дати та часу здійснення цієї операції.

2. Блокування кваліфікованого сертифіката відкритого ключа надавача:

1) блокування кваліфікованих сертифікатів відкритих ключів надавачів здійснюється у випадках, передбачених частинами шостою та сьомою статті 25 Закону.

У разі блокування кваліфікованого сертифіката відкритого ключа надавача на підставі його заяви такі заяви подаються до Адміністратора ІТС ЦЗО за формами, визначеними у додатку 6 (для надавача – юридичної особи) та у додатку 7 (для надавача – фізичної особи – підприємця) до цього Регламенту;

2) заява про блокування кваліфікованого сертифіката відкритого ключа подається надавачем до Адміністратора ІТС ЦЗО в електронній формі з накладенням кваліфікованого електронного підпису керівника юридичної особи чи його уповноваженої особи;

3) під час прийому заяви про блокування кваліфікованого сертифіката відкритого ключа здійснюється встановлення особи керівника юридичної особи – надавача (фізичної особи – підприємця, що є надавачем) або його уповноваженої особи та перевіряється достатність обсягу цивільної правоздатності і дієздатності шляхом перевірки ідентифікаційних даних особи з документів, що надаються заявником, та даних, одержаних з інформаційних систем органів державної влади, в тому числі в Єдиних та державних реєстрах;

4) не приймаються до розгляду заяви та документи, що не дають змоги однозначно тлумачити зміст, якщо кваліфікований електронний підпис не пройшов перевірку;

5) кваліфікований сертифікат відкритого ключа надавача блокується не пізніше ніж протягом двох годин від моменту отримання заяви про блокування кваліфікованого сертифіката відкритого ключа Адміністратором ІТС ЦЗО;

6) блокування кваліфікованого сертифіката відкритого ключа надавача здійснюється адміністратором сертифікації під контролем адміністратора безпеки та аудиту;

7) блокування кваліфікованого сертифіката відкритого ключа надавача набирає чинності з дати та часу здійснення цієї операції;

8) серійний номер заблокованого кваліфікованого сертифіката відкритого ключа надавача вноситься до СВС із зазначенням дати та часу здійснення цієї операції.

3. Поновлення кваліфікованого сертифіката відкритого ключа надавача:

1) поновлення кваліфікованих сертифікатів відкритих ключів надавачів здійснюється у випадках, передбачених частинами десятою, одинадцятою статті 25 Закону, на підставі заяв про поновлення кваліфікованого сертифіката відкритого ключа за формами, визначеними у додатку 8 (для надавача – юридичної особи) та у додатку 9 (для надавача – фізичної особи – підприємця) до цього Регламенту, що подаються до Адміністратора ІТС ЦЗО;

2) заява про поновлення кваліфікованого сертифіката відкритого ключа подається до Адміністратора ІТС ЦЗО в електронній формі з накладенням кваліфікованого електронного підпису керівника юридичної особи чи його уповноваженої особи;

3) під час прийому заяви про поновлення кваліфікованого сертифіката відкритого ключа здійснюється встановлення особи керівника юридичної особи – надавача (фізичної особи – підприємця, що є надавачем) або його уповноваженої особи та перевіряється достатність обсягу цивільної правоздатності і дієздатності шляхом перевірки ідентифікаційних даних особи з документів, що надаються заявником, та даних, одержаних з інформаційних систем органів державної влади, в тому числі в Єдиних та державних реєстрах;

4) не приймаються до розгляду заяви та документи, що не дають змоги однозначно тлумачити зміст, якщо кваліфікований електронний підпис не пройшов перевірку;

5) заблокований кваліфікований сертифікат відкритого ключа надавача поновлюється не пізніше ніж протягом двох годин від моменту отримання заяви про поновлення кваліфікованого сертифіката відкритого ключа Адміністратором ІТС ЦЗО;

6) поновлення кваліфікованого сертифіката відкритого ключа надавача здійснюється адміністратором сертифікації під контролем адміністратора безпеки та аудиту;

7) поновлення кваліфікованого сертифіката відкритого ключа надавача набирає чинності з дати та часу здійснення цієї операції;

8) відомості щодо поновлення кваліфікованого сертифіката відкритого ключа надавача вносяться до СВС із зазначенням дати та часу здійснення цієї операції.

4. Розповсюдження інформації про зміну статусу кваліфікованих сертифікатів відкритих ключів надавачів:

1) розповсюдження інформації про статус кваліфікованих сертифікатів відкритих ключів надавачів здійснюється за допомогою публікації повного та часткового СВС на офіційному вебсайті ЦЗО та забезпечення можливості перевірки статусу сертифіката ключа в режимі реального часу через телекомунікаційні мережі загального користування;

2) публікація наступного СВС здійснюється з періодичністю, зазначеною у пунктах 1 – 3 глави 2 розділу IV цього Регламенту;

3) Адміністратор ІТС ЦЗО під час формування СВС забезпечує такі умови:

у кожному СВС зазначається граничний термін його дії до видання наступного списку;

новий СВС може бути опублікований до настання граничного терміну його дії для видання наступного списку;

на СВС має бути накладена електронна печатка ЦЗО;

4) інформація про статус кваліфікованого сертифіката відкритого ключа надавача в режимі реального часу розповсюджується за протоколом визначення статусу сертифіката відповідно до технічних вимог до технічних засобів та процесів їх використання у сфері електронних довірчих послуг, засобів криптографічного захисту інформації, процесів їх створення та функціонування у складі інформаційно-телекомунікаційних систем, які встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг та спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації, відповідно до Постанови.

5. Закінчення строку чинності кваліфікованого сертифіката відкритого ключа надавача

1. Строк чинності кваліфікованого сертифіката відкритого ключа надавача становить не більше ніж п'ять років.

2. Початок строку чинності кваліфікованого сертифіката відкритого ключа надавача обчислюється з дати і часу формування сертифіката у ЦЗО, що відображається у сертифікаті.

3. Не пізніше закінчення половини строку чинності кваліфікованого сертифіката відкритого ключа надавача надавач отримує новий кваліфікований сертифікат відкритого ключа у порядку, визначеному у пунктах 1 – 8 глави 1 розділу V цього Регламенту.

VI. Надання адміністративної послуги внесення юридичних осіб та фізичних осіб – підприємців, які мають намір надавати електронні довірчі послуги, до Довірчого списку

1. Надання адміністративної послуги внесення юридичних осіб та фізичних осіб – підприємців, які мають намір надавати електронні довірчі послуги, до Довірчого списку здійснюється Мінцифри з урахуванням положень

Законів України «Про адміністративні послуги» та «Про електронні довірчі послуги».

2. На адміністративну послугу внесення юридичних осіб та фізичних осіб – підприємців, які мають намір надавати електронні довірчі послуги, до Довірчого списку Мінцифри затверджуються інформаційна і технологічна картки.

3. Інформаційна картка розміщується у місці здійснення прийому юридичних осіб та фізичних осіб – підприємців, які мають намір надавати електронні довірчі послуги, на офіційному вебсайті ЦЗО та на Єдиному державному вебпорталі електронних послуг.

4. Порядок подання юридичною особою або фізичною особою – підприємцем, що має намір надавати послуги, документів та їх розгляд ЦЗО визначено частиною другою статті 30 Закону, а також вимогами у сфері електронних довірчих послуг, затвердженими в установленому порядку.

5. Для набуття статусу надавача юридична особа або фізична особа – підприємець, що має намір надавати послуги, подає до ЦЗО заяву про внесення відомостей про неї до Довірчого списку та інші документи, визначені частиною другою статті 30 Закону.

6. Заява про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку та документи, що до неї додаються, можуть бути подані представником юридичної особи або фізичною особою – підприємцем, що має намір надавати кваліфіковані електронні довірчі послуги, в електронній формі через Єдиний державний вебпортал електронних послуг, у тому числі через інтегровану з ним інформаційну систему ЦЗО.

7. Ідентифікацію та автентифікацію заявників для внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку здійснюють посадові особи структурного підрозділу Мінцифри, відповідального

за етапи надання адміністративної послуги, які зазначаються у технологічній картці адміністративної послуги.

8. Розгляд документів, поданих юридичною особою або фізичною особою – підприємцем, що має намір надавати послуги, здійснюється у строк, визначений частиною четвертою статті 30 Закону.

9. Підставами для прийняття рішення про відмову у внесенні відомостей до Довірчого списку є:

подання не в повному обсязі документів, передбачених частиною другою статті 30 Закону;

виявлення в заявах про внесення до Довірчого списку та документах, що додаються до них, недостовірної інформації, пошкоджень, що не дають змоги однозначно тлумачити зміст, виправлень або дописок.

10. Форми заяв про внесення до Довірчого списку визначені у додатку 10 (для юридичної особи) та у додатку 11 (для фізичної особи – підприємця) до цього Регламенту.

11. Внесення відомостей до Довірчого списку, внесення змін, виключення надавача з Довірчого списку здійснюються відповідно до порядку ведення Довірчого списку, затвердженого в установленому порядку.

Директор директорату
функціонального розвитку
цифровізації **Анастасія ХАЛЄЄВА**