

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ЗАТВЕРДЖУЮ
Ректор НТУ «ХПІ»

_____ Євген СОКОЛ

«__» _____ 2024 р.

**РЕГЛАМЕНТ РОБОТИ
НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ У
НАЦІОНАЛЬНОМУ ТЕХНІЧНОМУ УНІВЕРСИТЕТІ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

ЗАТВЕРДЖЕНО
ВЧЕНОЮ РАДОЮ НТУ «ХПІ»
Голова Вченої ради

_____ / Леонід ТОВАЖНЯНСЬКИЙ

Протокол _____ № _____

від «05» _____ червня _____ 2023р.

Харків 2024 р.

ЗМІСТ

ВСТУП.....	5
ТЕРМІНИ ТА ВИЗНАЧЕННЯ.....	6
ПОЗНАЧКИ ТА СКОРОЧЕННЯ.....	8
СТАТУС РЕГЛАМЕНТУ.....	9
ПОРЯДОК ВНЕСЕННЯ ЗМІН ТА ДОПОВНЕНЬ ДО РЕГЛАМЕНТУ.....	10
1 ЗАГАЛЬНІ ВІДОМОСТІ ПРО НЕДП.....	11
1.1 Ідентифікаційні дані НЕДП.....	11
2 ПЕРЕЛІК ІНФОРМАЦІЇ, ЩО РОЗМІЩУЄТЬСЯ НА ВЕБ-САЙТІ НЕДП.....	12
3 ПЕРЕЛІК ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ, НАДАННЯ ЯКИХ ЗАБЕЗПЕЧУЄ НЕДП.....	13
4 ОПИС ФУНКЦІЙ АДМІНІСТРАТОРА (ОПЕРАТОРА) РЕЄСТРАЦІЇ, АДМІНІСТРАТОРА СЕРТИФІКАЦІЇ, СИСТЕМНОГО АДМІНІСТРАТОРА, АДМІНІСТРАТОРА БЕЗПЕКИ.....	14
4.1 Працівники НЕДП.....	14
4.2 Керівник НЕДП.....	15
4.3 Адміністратор реєстрації.....	16
4.4 Оператор реєстрації.....	18
4.5 Адміністратор сертифікації.....	19
4.6 Системний адміністратор.....	20
4.7 Адміністратор безпеки.....	22
5. ПОЛІТИКА СЕРТИФІКАТА.....	25
5.1 Перелік сфер, в яких дозволяється використання сертифікатів ключів, сформованих НЕДП.....	25
5.2 Обмеження, щодо використання сертифікатів ключів, сформованих НЕДП.....	25
5.3 Час і порядок публікації сертифікатів ключів та списків відкликаних сертифікатів.....	26
5.4 Механізм підтвердження володіння особистим ключем, відповідно якому відкритий ключ надається для формування сертифіката ключа.....	27
5.5 Умови ідентифікації, автентифікації та верифікації клієнта НЕДП.....	27
5.5.1 Фізична особа.....	27
5.5.2 Іноземці.....	28
5.5.3 Юридична особа та представник юридичної особи.....	28
5.6 Механізм автентифікації підписувачів, які мають чинний сертифікат ключа, сформований НЕДП.....	29
5.7 Механізм ідентифікації, автентифікації, верифікації підписувачів під час обробки заяв на блокування, скасування або поновлення сертифіката.....	29

ключа.....	
5.8 Процедурний контроль.....	30
5.9 Порядок ведення журналів аудиту подій.....	30
5.10 Порядок ведення, збереження (із зазначенням строків зберігання), резервування, відновлення, захисту даних, пов'язаних із формуванням та обслуговуванням НЕДП сертифікатів ключів.....	31
5.11 Порядок та умови генерації, зберігання, використання пар ключів НЕДП.....	31
5.12 Порядок та умови резервного копіювання особистого ключа НЕДП, збереження, доступу та використання резервних копій.....	33
5.13 Генерація ключів користувачів.....	34
5.14 Процедури отримання користувачем особистого ключа в результаті надання електронної довірчої послуги її надавачем.....	35
5.15 Механізм надання відкритого ключа користувача надавачу для формування сертифіката відкритого ключа.....	36
6 ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК.....	37
6.1 Процес подання запиту на формування сертифіката ключа.....	37
6.2 Порядок надання сформованого сертифіката відкритого ключа користувачу.....	37
6.3 Порядок та умови публікації сформованого сертифіката ключа клієнта на Веб-сайт НЕДП.....	38
6.4 Умови використання сертифіката ключа користувача та його особистого ключа.....	38
6.5 Процедура подачі запиту на формування сертифіката ключа для користувачів, які мають чинний сертифікат ключа, сформований НЕДП.....	39
6.6 Порядок та умови скасування (блокування, поновлення) сертифіката ключа підписувача.....	39
6.6.1 Процедура подання заяви на скасування (блокування, поновлення) сертифіката ключа.....	42
6.6.2 Порядок та умови блокування, поновлення, скасування сертифікатів ключів користувачів, які є співробітниками НТУ «ХП».....	42
6.7 Порядок та умови надання інформації про статус сертифіката ключів, сформованих НЕДП.....	43
6.8 Строки дії сертифікатів ключів, сформованих НЕДП.....	43
7 ПРОЦЕДУРА ТА ПРОЦЕСИ, ЯКІ ВИКОНУЮТЬСЯ ПІД ЧАС НАДАННЯ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ, ЩО НЕ ПЕРЕДБАЧАЮТЬ ФОРМУВАННЯ ТА ОБСЛУГОВУВАННЯ СЕРТИФІКАТІВ ВІДКРИТИХ КЛЮЧІВ.....	44

7.1. Надання засобів електронного підпису чи печатки.....	44
7.2. Надання електронної довірчої послуги формування, перевірки та підтвердження електронної позначки часу.....	44
ДОДАТКИ.....	45

ВСТУП

Даний Регламент є документом надавача електронних довірчих послуг Національного технічного університету “Харківський політехнічний інститут” (далі НЕДП НТУ “ХПІ”), який визначає організаційно-методологічні, технічні та технологічні умови діяльності НЕДП, під час надання ним електронних довірчих послуг (далі – Регламент).

Регламент розроблено відповідно чинного законодавства України у сфері електронних довірчих послуг.

Вимоги Регламенту є обов’язковими для виконання персоналом НЕДП та клієнтами НЕДП.

Суб’єктами правових відносин у сфері електронних довірчих послуг, що обумовлюються цим Регламентом є НЕДП і підписувач.

Будь-яка зацікавлена особа може ознайомитися з положеннями Регламенту на Веб-порталі (електронному інформаційному ресурсі) НЕДП та його відокремленому пункті реєстрації.

ТЕРМІНИ ТА ВИЗНАЧЕННЯ

Надавач	надавач електронних довірчих послуг Національний технічний університет “Харківський політехнічний інститут”;
Відкритий ключ	параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів;
База даних	база даних НЕДП, у якій зберігаються реєстр НЕДП, інформаційно-довідкова, технологічна та інша службова інформація, потрібна для функціонування програмно-технічного комплексу (далі – ПТК) НЕДП;
Електронна позначка часу	електронні дані, які пов’язують інші електронні дані з конкретним моментом часу для засвідчення наявності цих електронних даних на цей момент часу;
Електронний підпис	електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов’язуються і використовуються ним як підпис;
Надавач електронних довірчих послуг	юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа-підприємець, яка надає одну або більше електронних довірчих послуг, діяльність якої відповідає вимогам цього Закону та відомості про яку внесені до Довірчого списку;
Компрометація особистого ключа	будь-яка подія, що призвела або може призвести до несанкціонованого доступу до особистого ключа;
Особистий ключ	параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів;
Програмно-технічний комплекс	апаратні, апаратно-програмні та програмні засоби, що забезпечують виконання функцій, пов’язаних з наданням електронних довірчих послуг;

Сертифікат відкритого ключа	електронний документ, який засвідчує належність відкритого ключа фізичній або юридичній особі, підтверджує її ідентифікаційні дані та/або надає можливість здійснити автентифікацію веб-сайту;
Центр реєстрації	представництво (філія, підрозділ) центру сертифікації ключів, яке здійснює реєстрацію підписувачів;
Центр сертифікації ключів	організація, що надає послуги електронного підпису та засвідчила свій відкритий ключ у центральному засвідчувальному органі.

ПОЗНАЧКИ ТА СКОРОЧЕННЯ

НЕДП	– надавач електронних довірчих послуг;
ЕП	– електронний підпис;
ЕПЧ	– електронна позначка часу;
ПТК	– програмно-технічний комплекс;
БД	– база даних;
ЄДРПОУ	– єдиний державний реєстр підприємств та організацій України;
ІКС	– інформаційно-комунікаційна система;
ЄДДР	– єдиний державний демографічний реєстр;
УНЗР	– унікальний номер запису в ЄДДР;
ОС	– операційна система;
ПЗ	– програмне забезпечення;
РНОКПП	– реєстраційний номер облікової картки платника податків;
СВС	– список відкликаних сертифікатів;
ІКС	– інформаційно-комунікаційна система
ЦР	– центр реєстрації.

СТАТУС РЕГЛАМЕНТУ

Регламент роботи надавача електронних довірчих послуг Національний технічний університет “Харківський політехнічний інститут” (далі – НЕДП або Надавач) визначає організаційно-методологічні, технічні та технологічні умови діяльності надавача під час надання електронних довірчих послуг, включаючи політику сертифіката та положення сертифікаційних практик, встановлює порядок роботи та процедури НЕДП з надання електронних довірчих послуг.

Регламент розроблений відповідно до:

- Закону України від 05 жовтня 2017 року № 2155-VIII “Про електронні довірчі послуги”(зі змінами);
- Закону України від 22 травня 2003 року № 851 - IV “Про електронні документи та електронний документообіг” (зі змінами);
- Постанови Кабінету Міністрів України від 07.11.2018 № 992 “Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг”;
- Постанови Кабінету Міністрів України від 19.09.2018 р. № 749 “Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності”;
- інших нормативно-правових актів у сфері надання електронних довірчих послуг.

Норми цього Регламенту поширюються на:

- працівників надавача;
- заявників;
- підписувачів;
- створювачів електронної печатки.

Вимоги Регламенту є обов’язковими до виконання працівниками надавача.

Визнання вимог Регламенту заявниками, підписувачами та створювачами електронних печаток є обов’язковою умовою та підставою для надання електронних довірчих послуг.

Вимоги Регламенту засновані на принципах дотримання прав та виконання обов’язків суб’єктами надання та отримання електронних довірчих послуг, які наведено в Законі України “Про електронні довірчі послуги”.

Будь-яка зацікавлена особа може ознайомитися з положеннями Регламенту на офіційному веб-сайті надавача.

ПОРЯДОК ВНЕСЕННЯ ЗМІН ТА ДОПОВНЕНЬ ДО РЕГЛАМЕНТУ

Внесення змін та доповнень до Регламенту здійснюється надавачем відповідно до Вимог у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 07 листопада 2018 року № 992.

Про внесення змін та доповнень до Регламенту надавач повідомляє заявників, підписувачів, створювачів електронних печаток та інших зацікавлених осіб шляхом розміщення зазначених змін та доповнень на офіційному веб-сайті надавача.

Зміни та доповнення до Регламенту, що не пов'язані зі зміною чинного законодавства України, набувають чинності через 10 календарних днів з дня розміщення зазначених змін і доповнень на офіційному веб-сайті надавача.

Всі зміни та доповнення, що внесені до Регламенту у зв'язку зі зміною законодавства, набувають чинності одночасно зі вступом у дію відповідних нормативно-правових актів.

Якщо підписувач не погоджується із внесеними до Регламенту змінами та доповненнями, він має право припинити використання сертифіката.

1 ЗАГАЛЬНІ ВІДОМОСТІ ПРО НЕДП

1.1. Ідентифікаційні дані НЕДП

Повне найменування НЕДП: Надавач електронних довірчих послуг Національний технічний університет “Харківський політехнічний інститут”.

Скорочене найменування надавача: НЕДП НТУ “ХПІ”.

Юридична та фактична адреса надавача: Україна, 61002, м. Харків, вул. Кирпичова, 2.

Телефон: +380635891789; +380505225664 .

Код ЄДРПОУ: 02071180.

Електронна адреса веб-сайту надавача: **<https://ca.khpi.edu.ua>**

Адреса електронної пошти надавача: **ca@khpi.edu.ua**

Для надання електронних довірчих послуг на певній території надавач може створювати центри реєстрації.

Центрами реєстрації надавача є філії чи окремі підрозділи надавача, які здійснюють реєстрацію підписувачів з дотриманням вимог законодавства у сфері електронних довірчих послуг та захисту інформації.

2 ПЕРЕЛІК ІНФОРМАЦІЇ, ЩО РОЗМІЩУЄТЬСЯ НА ВЕБ-САЙТІ НЕДП

До інформації, вільний доступ до якої забезпечує надавач через офіційний веб-сайт, належать:

- відомості про надавача;
- дані про внесення відомостей про надавача до Довірчого списку;
- Регламент роботи надавача;
- сертифікати відкритих ключів надавача;
- перелік електронних довірчих послуг, які надає надавач;
- дані про засоби електронного підпису чи печатки, що використовуються під час надання електронних довірчих послуг;
- форми документів, на підставі яких надаються електронні довірчі послуги;
- реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів;
- відомості про обмеження під час використання сертифікатів відкритих ключів користувачами;
- дані про порядок перевірки чинності сертифіката відкритого ключа, у тому числі умови перевірки статусу сертифіката відкритого ключа;
- перелік актів законодавства у сфері електронних довірчих послуг.

На веб-сайті додатково може розміщуватись будь-яка інша інформація.

Надавач також забезпечує інформування користувачів про умови отримання електронних довірчих послуг шляхом розміщення відповідної інформації на офіційному веб-сайті надавача.

Інформація, що публікується на електронному інформаційному ресурсі надавача, є загальнодоступною.

3 ПЕРЕЛІК ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ, НАДАННЯ ЯКИХ ЗАБЕЗПЕЧУЄ НЕДП

Під електронними довірчими послугами розуміються послуги, які надаються для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють надавачу електронних довірчих послуг щодо надання такої послуги, зокрема надання у користування засобів ЕП, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги, визначені Законом України “Про електронні довірчі послуги” від 05 жовтня 2017 року № 2155-VIII.

Надавач забезпечує надання таких електронних довірчих послуг:

- електронна довірча послуга створення, перевірки та підтвердження електронного підпису чи печатки;
- електронна довірча послуга формування, перевірки та підтвердження чинності сертифіката електронного підпису чи печатки;
- електронна довірча послуга формування, перевірки та підтвердження чинності електронної позначки часу.

4. ОПИС ФУНКЦІЙ АДМІНІСТРАТОРА (ОПЕРАТОРА) РЕЄСТРАЦІЇ, АДМІНІСТРАТОРА СЕРТИФІКАЦІЇ, СИСТЕМНОГО АДМІНІСТРАТОРА, АДМІНІСТРАТОРА БЕЗПЕКИ

Організаційна структура НЕДП містить дві основні складові частини, що виконують адміністративні функції, технічні і технологічні функції.

До адміністративних функцій НЕДП належать:

- реєстрація підписувачів;
- надання підписувачам консультацій з питань, пов'язаних з використанням ЕП;
- розгляд заяв і скарг підписувачів.

До технічних і технологічних функцій НЕДП належать:

- створення і забезпечення функціонування ПТК НЕДП;
- забезпечення захисту інформації впродовж експлуатації ПТК НЕДП;
- генерування і зберігання ключів НЕДП та відповідальних осіб НЕДП;
- надання методологічно-консультативної допомоги під час генерування ключів підписувачів у разі потреби та вживати заходів щодо забезпечення безпеки інформації під час генерування ключів;
- установлення належності підписувачу особистого ключа та його відповідність відкритому ключу;
- формування сертифікатів ключів послуги інтерактивного визначення статусу сертифіката, відповідальних осіб НЕДП і підписувачів;
- ведення реєстру НЕДП;
- поширення сертифікатів ключів НЕДП і підписувачів у встановленому цим Регламентом порядку;
- блокування, скасування та поновлення сертифікатів ключів послуги інтерактивного визначення статусу сертифіката, відповідальних осіб НЕДП і підписувачів у випадках, передбачених цим Регламентом і законодавством України у сфері електронних довірчих послуг;
- надання підписувачам послуг фіксування часу;
- надання послуг визначення статусу сертифіката ключа;
- публікація на Веб-сайті НЕДП відкритої інформації;
- інші дії, пов'язані з технічною та технологічною підтримкою діяльності НЕДП.

4.1. Працівники НЕДП

НЕДП для надання довірчих послуг призначає розпорядчим актом працівників, які виконують функції:

- керівник НЕДП;
- адміністратор безпеки;
- адміністратор сертифікації;
- адміністратор реєстрації;
- системний адміністратор;
- оператор реєстрації.

4.2. Керівник НЕДП

Керівник НЕДП призначається та звільняється з роботи наказом ректора університету та підпорядкований безпосередньо ректору університету або особі, що виконує його обов'язки.

Керівник НЕДП керується в роботі Конституцією України, чинним законодавством України, регламентом НЕДП, наказами і розпорядженнями університету.

Функціональні обов'язки:

До функціональних обов'язків керівника НЕДП належить:

- виконання рішень, наказів ректора, інструкцій та положень, прийнятих в університеті;
- здійснення поточного управління (керівництво) НЕДП, забезпечення ефективного використання і збереження майна НЕДП, забезпечення виконання завдань передбачених регламентом НЕДП;
- контроль роботи відокремлених пунктів НЕДП;
- організація системи організаційних та технічних заходів збереження конфіденційної інформації НЕДП та університету;
- подання звітів про роботу НЕДП до Центрального засвідчувального органу (далі – ЦЗО) та Державної служби спеціального зв'язку та захисту інформації України (відповідно до вимог нормативної документації);
- вживання заходів для підвищення ефективності роботи працівників НЕДП та відокремлених пунктів;
- розгляд конфліктних ситуацій, що виникають в трудовому колективі НЕДП, відокремлених пунктів та застосування необхідних заходів для їх вирішення;
- організація впровадження нових прогресивних форм і методів управління НЕДП та відокремлених пунктів реєстрації заявників, створення організаційних і економічних умов для високопродуктивної праці у НЕДП;
- створення безпечних і сприятливих умов праці.

Повноваження:

До повноважень керівника НЕДП належить:

- видавати розпорядження та інші документи з питань діяльності НЕДП;
- погоджувати положення та інструкції, що приймаються в університеті та стосуються роботи НЕДП і його відокремлених пунктів;
- затверджувати внутрішні для НЕДП положення та інструкції, а також зміни до графіку роботи НЕДП у випадках пов'язаних з перенесенням робочих днів на загальнодержавні свята;
- подавати ректору університету клопотання про внесення змін до основного графіку роботи НЕДП, Регламенту, штату НЕДП, положень та інструкцій НЕДП університету при виникненні об'єктивної необхідності;
- доповідати ректору університету про необхідність застосування до співробітників НЕДП заходів дисциплінарного впливу;
- вносити на розгляд ректору університету або керівників структурних підрозділів питання, пов'язані з діяльністю НЕДП або його відокремлених пунктів;
- доводити до відома розробників програмно-технічного комплексу (ПТК) та постачальників іншого програмного та апаратного забезпечення, що застосовується в НЕДП, пропозиції та зауваження по роботі зазначених компонентів НЕДП;
- здійснювати оперативне управління майном НЕДП.

Додаткові повноваження визначаються довіреністю та наказами ректора університету.

4.3. Адміністратор реєстрації

Адміністратор реєстрації призначається та звільняється з роботи наказом ректора університету та підпорядкований безпосередньо керівнику НЕДП або особі, що виконує його обов'язки.

Адміністратор реєстрації здійснює свою діяльність на підставі Регламенту НЕДП.

Функціональні обов'язки:

До функціональних обов'язків адміністратора реєстрації належить:

- перевірка даних, обов'язкових для формування сертифіката, а також даних, які вносяться у сертифікат на вимогу підписувача;
- формування електронних заяв на формування, скасування, блокування та поновлення сертифікатів ключів на підставі письмових заяв підписувачів;
- надання допомоги підписувачам під час генерації особистих та відкритих ключів, у разі отримання від них відповідного звернення, а також

вживання заходів щодо забезпечення безпеки інформації під час генерації ключової інформації;

- перевірка законності звернень про блокування, поновлення та скасування сертифікатів;
- формування запитів на формування стартових та робочих сертифікатів відкритих ключів підписувачів, засвідчення коректності включених в них даних шляхом накладення на запит власного електронного цифрового підпису;
- видання сертифікатів відкритих ключів підписувачів за допомогою програмно-технічних засобів;
- формування електронних заяв на блокування та скасування сертифікатів ключів у випадках, передбачених Регламентом;
- перевірка законності звернень про блокування за процедурою, визначеною Регламентом;
- надання підписувачам консультацій щодо умов та порядку надання послуг ЕЦП;
- зберігання власного носія з особистим ключем;
- реєстрація внесення змін в реєстр користувачів з дозволу керівника ЦСК або особи, що його заміщує;
- передача особових справ заявника до архіву;
- вирішення спірних питань, що виникають під час роботи оператора реєстрації з клієнтами, доведення до керівника НЕДП про питання, які не можуть бути вирішені з власними повноваженнями;
- збереження конфіденційних відомостей та комерційної таємниці НЕДП та університету;
- суворе дотримання правил безпеки під час експлуатації ПЕОМ та електрообладнання.

Відповідальність:

Адміністратор реєстрації несе особисту відповідальність за:

- відповідність даних, включених в запит на формування сертифіката, який підписаний його ЕЦП, даним, що подані заявником в письмовій заяві та визначених Регламентом документах;
- повноту комплекту документів, відповідно переліку, визначеному Регламентом, та коректність засвідчення копій документів, якими заявник підтверджує дані для внесення в сертифікат;
- документально підтверджену законність заяв на зміну статусу сертифіката підписувача, які були ним сформовані та засвідчені особистим ЕЦП.

Під час відсутності оператора реєстрації адміністратор виконує його обов'язки та безпосередньо працює з клієнтами НЕДП.

Повноваження:

До повноважень адміністратора реєстрації належить:

- перевірка роботи операторів реєстрації;
- перевірка повноти та правильності наданої заявниками інформації;
- вимагання від заявників додаткових документів;
- відмова заявнику у реєстрації та формуванні, скасуванні, блокуванні та відновленні сертифікатів ключів, якщо форма та зміст відповідної заяви не відповідають вимогам регламенту та/або договору або якщо ці заяви подає не вповноважена на це особа;
- відмова заявнику в прийомі запиту на формування сертифіката, що виконаний в електронному вигляді, якщо засіб криптографічного захисту інформації використаний заявником для формування запиту на сертифікат не підтримується НЕДП;
- відмова заявнику в формуванні сертифіката, якщо ключова пара була сформована поза НЕДП та не проходить перевірку на відповідність відкритого та особистого ключів;
- відмова заявнику в прийомі заяви на блокування сертифіката по телефону, якщо деякі з названих даних не співпадають з тими, що є в реєстрі користувачів;
- перевірка роботи адміністраторів реєстрації відокремлених пунктів реєстрації заявників.

4.4. Оператор реєстрації

Оператор реєстрації призначається та звільняється з роботи наказом ректора університету та підпорядкований безпосередньо керівнику НЕДП або особі, що виконує його обов'язки та підконтрольний адміністратору реєстрації НЕДП.

Оператор реєстрації здійснює свою діяльність на підставі Регламенту.

Функціональні обов'язки:

До функціональних обов'язків оператора реєстрації належить:

- встановлення осіб, які звернулися до НЕДП з метою формування сертифіката;
- перевірка даних, обов'язкових для формування сертифіката, а також даних, які вносяться у сертифікат на вимогу підписувача;
- перевірка документів, наданих заявниками для ідентифікації їх особи;
- перевірка повноти комплексу документів, відповідно переліку, визначеному Регламентом, та коректність засвідчення копій документів, якими заявник підтверджує дані для внесення в сертифікат;

- вимагання від заявників додаткової інформації в документальній формі, якщо така інформація необхідна для їх реєстрації;
- заповнення електронних форм з даними Заявника, перевірка точності занесення даних, формування особової справи Заявника;
- формування запитів на формування стартових та робочих сертифікатів відкритих ключів підписувачів, засвідчення коректності включених в них даних шляхом накладення на запит власного електронного цифрового підпису;
- отримання від підписувачів письмових заяв на формування, скасування, блокування та поновлення сертифікатів ключів;
- перевірка законності звернень про блокування, поновлення та скасування сертифікатів;
- формування електронних заяв на блокування, поновлення та скасування сертифікатів ключів у випадках, передбачених Регламентом;
- 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 ключової інформації;
- надання підписувачам консультацій щодо умов та порядку надання послуг ЕЦП;
- доведення до адміністратора реєстрації про всі спірні питання, які виникли при реєстрації заявників;
- збереження конфіденційних відомостей та комерційної таємниці НЕДП та університету;
- суворе дотримання правил безпеки під час експлуатації електрообладнання.

Повноваження:

До повноважень оператора реєстрації належить:

- відмова заявнику у реєстрації, якщо форма та зміст заяви не відповідають вимогам Регламенту або якщо заяву подає не вповноважена на це особа;
- відмова в прийомі до розгляду документів, які мають підчистки, дописки, закреслені слова, інші незастережні виправлення або написи олівцем, а також мають пошкодження, внаслідок чого їх текст неможливо прочитати;
- вимагання від заявника надання документів та відомостей, які необхідні для з'ясування його особи та формування сертифікату.

4.5. Адміністратор сертифікації

Адміністратор сертифікації призначається та звільняється з роботи наказом

ректора університету та підпорядкований безпосередньо керівнику НЕДП або особі, що виконує його обов'язки.

Адміністратор сертифікації здійснює свою діяльність на підставі Регламенту.

Функціональні обов'язки:

До функціональних обов'язків адміністратора сертифікації належить:

- формування за допомогою особистого ключа НЕДП сертифікатів підписувачів, списків відкликаних сертифікатів та позначок часу;
- формування електронних заяв на блокування, поновлення та скасування сертифікатів ключів у випадках, передбачених Регламентом;
- збереження резервної копії особистого ключа НЕДП, резервних копій особистих ключів функціональних серверів;
- контроль своєчасності і коректності процесу формування СВС та розміщення їх на інформаційному ресурсі НЕДП;
- подання до ЦЗО даних, які необхідні для формування сертифіката та засвідчення відкритого ключа НЕДП;
- участь у резервному копіюванні особистого ключа НЕДП та особистих ключів функціональних серверів НЕДП, відновленні цих ключів, знищенні особистих ключів та їх резервних копій;
- збереження конфіденційних відомостей та комерційної таємниці НЕДП та університету;
- суворе дотримання правил безпеки під час експлуатації ПЕОМ та електрообладнання.

4.6. Системний адміністратор

Системний адміністратор призначається та звільняється з роботи наказом ректором університету та підпорядкований безпосередньо керівнику НЕДП або особі, що виконує його обов'язки.

Системний адміністратор здійснює свою діяльність на підставі Регламенту НЕДП.

Функціональні обов'язки:

До функціональних обов'язків системного адміністратора належить:

- організація експлуатації та технічного обслуговування інформаційно-комунікаційної системи НЕДП;
- ведення моніторингу функціонування інформаційно-комунікаційної системи НЕДП;
- відновлення інформаційно-комунікаційної системи НЕДП після збоїв та відмов;

- підтримка електронного інформаційного ресурсу НЕДП;
- участь у забезпеченні функціонування комплексної системи захисту інформації;
- формування та ведення резервних копій конфігурацій загальносистемного та спеціального програмного забезпечення програмно-технічного комплексу;
- контроль архівації та резервування бази даних сформованих сертифікатів та СВС;
- адміністрування антивірусного програмного забезпечення, забезпечення актуальності антивірусних баз;
- формування та зберігання резервних копій конфігураційних файлів загальносистемного та спеціального програмного забезпечення програмно-технічного комплексу;
- технічна підтримка підписувачів НЕДП по каналах зв'язку;
- ведення формуляру ІКС НЕДП;
- ведення журналів, що стосуються експлуатації ІКС ЦСК;
- збереження конфіденційних відомостей та комерційної таємниці НЕДП та університету;
- суворе дотримання правил безпеки під час експлуатації електрообладнання.

За системним адміністратором закріплюється в експлуатації ІКС НЕДП.

Відповідальність:

Системний адміністратор несе персональну відповідальність за безперебійне функціонування ІКС НЕДП та доступність для доступу користувачів інформаційного ресурсу НЕДП, а також за збереженість апаратури та майна ІКС НЕДП.

Повноваження:

До повноважень системного адміністратора належить:

- контролювати дотримання співробітниками політики безпеки та технології обробки інформації;
- отримати під час приймання чергування від чергового адміністратора реєстрації вичерпні відомості про стан процесу обробки інформації, апаратних та програмних засобів ІКС та КСЗІ;
- готувати пропозиції щодо забезпечення програмно-технічного комплексу ІКС НЕДП необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою з метою підвищення рівня захисту інформації;
- приймати участь в інвентаризації апаратури та майна НЕДП;

- доводити до відома розробників пропозицій та зауважень по роботі апаратних, програмних та апаратно-програмних засобів.
- програмних та апаратно-програмних засобів.

4.7. Адміністратор безпеки

Адміністратор безпеки призначається та звільняється з роботи наказом ректора університету та підпорядкований безпосередньо керівнику НЕДП.

В разі тимчасової відсутності керівника НЕДП, адміністратор безпеки виконує його обов'язки та підпорядковується безпосередньо ректору університету.

Адміністратор безпеки здійснює свою діяльність на підставі Регламенту.

Адміністратор безпеки не може суміщати декілька посад.

Функціональні обов'язки:

До функціональних обов'язків адміністратора безпеки належить:

- забезпечення повноти та якості виконання організаційно-технічних заходів із захисту інформації;
- забезпечення функціонування комплексної системи захисту інформації;
- розроблення розпорядчих документів, згідно з якими в НЕДП повинен забезпечуватися захист інформації, контроль за їх виконанням;
- своєчасне реагування на спроби несанкціонованого доступу до ресурсів програмно-технічного комплексу НЕДП, спроби порушення правил експлуатації засобів захисту інформації;
- участь у процедурах генерації особистого ключа НЕДП та особистих ключів функціональних серверів, резервного копіювання цих ключів та їх знищенні;
- участь у відновленні особистого ключа НЕДП та особистих ключів функціональних серверів;
- зберігання резервної копії особистого ключа НЕДП;
- контроль за зберіганням резервних копій особистих ключів функціональних серверів;
- генерація, контроль за зберіганням та використанням особистих ключів посадових осіб НЕДП і їх своєчасним та надійним знищенням;
- засвідчення електронних запитів на формування сертифікатів відкритих ключів посадових осіб НЕДП;
- формування електронних заяв на блокування, поновлення та скасування сертифікатів відкритих ключів посадових осіб НЕДП у випадках, передбачених Регламентом;

- формування електронних заяв на блокування, поновлення та скасування сертифікатів ключів у випадках, передбачених Регламентом;
- ведення контролю за процесом резервування сертифікатів ключів та списків відкликаних сертифікатів (далі – СВС), а також інших важливих ресурсів;
- передавання резервної копії бази даних сертифікатів ключів та СВС на зберігання до відокремленого сховища;
- організація розмежування доступу до ресурсів програмно-технічного комплексу НЕДП, зокрема розподілення між посадовими особами паролів, ключів, сертифікатів тощо;
- забезпечення спостереження за функціонуванням комплексної системи захисту інформації (реєстрація та аудит подій в програмно-технічному комплексі НЕДП, моніторинг подій тощо);
- забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування комплексної системи захисту інформації після збоїв, відмов або аварій;
- організація зберігання та оберту в межах ІКС НЕДП засобів криптографічного захисту інформації (далі – КЗІ);
- контроль ведення журналів аудиту подій, що реєструються засобами програмно-технічного комплексу НЕДП;
- контроль зберігання архівних і резервних копій реєстрів сертифікатів, журналів аудиту та конфігурацій програмного забезпечення та обладнання;
- контроль приймання та здавання чергування системним адміністратором та черговими адміністраторами реєстрації;
- ведення журналів, що стосуються заходів з забезпечення захисту інформації;
- збереження конфіденційних відомостей НЕДП та університету;
- суворе дотримання правил безпеки під час експлуатації електрообладнання.

Повноваження:

До повноважень адміністратора безпеки належить:

- вимагати від системного адміністратора та чергових адміністраторів безпеки звіту про стан процесу обробки інформації, апаратних та програмних засобів ІКС та КЗІ;
- вимагати від співробітників НЕДП негайної доповіді про факти скоєння (або навіть спроби) несанкціонованого доступу до інформації, що обробляється в ІКС НЕДП;

- проводити службові розслідування виявлених порушень політики безпеки, фактів або спроб несанкціонованого доступу до конфіденційної інформації;
- контролювати дотримання співробітниками політики безпеки;
- готувати пропозиції щодо забезпечення програмно-технічного комплексу ІКС НЕДП (КСЗІ) необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою з метою підвищення рівня захисту інформації;
- узгоджувати умови включення до складу програмно-технічного комплексу ІКС НЕДП нових компонентів та подавати керівництву пропозиції щодо заборони їхнього включення, якщо вони порушують прийняту політику безпеки або рівень захищеності ресурсів;
- надавати пропозиції безпосередньому керівництву щодо покращення умов праці.

5. ПОЛІТИКА СЕРТИФІКАТА

5.1. Перелік сфер, в яких дозволяється використання сертифікатів ключів, сформованих НЕДП

Сертифікати ключів, які формуються НЕДП, призначені для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів.

Електронний підпис, який перевіряється з використанням сертифікатів ключів, що формується НЕДП, використовується фізичними та юридичними особами – суб'єктами електронного документообігу – для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Перелік сфер, в яких дозволяється використання сертифікатів:

- автентифікації;
- перевірки кваліфікованого електронного підпису;
- перевірки кваліфікованої електронної печатки;
- узгодження ключів шифрування.

Для ідентифікації сфери використання відкритих ключів, під час формування сертифіката відкритого ключа надавач встановлює розширення сертифіката “Призначення відкритого ключа” (“keyUsage”), зазначені у табл. 5.1.

Таблиця 5.1

Сфера використання кваліфікованого сертифіката відкритого ключа	Призначення відкритого ключа ("keyUsage")
Автентифікація	digitalSignature + nonRepudiation або keyAgreement
Перевірка електронного підпису	digitalSignature + nonRepudiation
Перевірка електронної печатки	digitalSignature + nonRepudiation
Узгодження ключів шифрування	keyAgreement

5.2. Обмеження, щодо використання сертифікатів ключів, сформованих НЕДП

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

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

використання сертифіката ключа заноситься до сформованого сертифіката ключа у вигляді уточненого призначення ключа.

Не допускається використання сертифікатів відкритих ключів, сформованих надавачем для певної сфери використання, в інших сферах.

5.3. Час і порядок публікації сертифікатів ключів та списків відкликаних сертифікатів

Сертифікати відкритих ключів надавача публікуються одразу після їх отримання від Центрального засвідчувального органу.

Сертифікати відкритих ключів серверів ІКС надавача публікуються одразу після їх формування надавачем.

Сертифікати відкритих ключів підписувачів та створювачів електронної печатки, які надали згоду на їх публікацію, публікуються одразу після формування таких сертифікатів.

Надавач формує списки відкликаних сертифікатів у вигляді повного та часткового списків, які відповідають таким вимогам:

- у кожному списку відкликаних сертифікатів зазначається граничний строк його дії до видання нового списку;
- новий список відкликаних сертифікатів може бути опубліковано до настання граничного строку його дії до видання наступного списку;
- на список відкликаних сертифікатів повинен бути накладений кваліфікований електронний підпис надавача.

Публікація списків відкликаних сертифікатів відбувається в автоматичному режимі.

Час зміни статусу сертифікатів відкритих ключів синхронізований із Всесвітнім координованим часом (UTC) з точністю до однієї секунди.

Посилання на списки відкликаних сертифікатів вносяться до сертифікатів відкритих ключів підписувачів та створювачів електронної печатки.

Повний список відкликаних сертифікатів формується та публікується 1 раз на тиждень та містить інформацію про всі відкликані сертифікати ключів, які були сформовані надавачем.

Частковий список відкликаних сертифікатів формується та публікується кожні 2 години і містить інформацію про всі відкликані сертифікати, статус яких був змінений в інтервалі між часом випуску останнього повного списку відкликаних сертифікатів та часом формування поточного часткового списку відкликаних сертифікатів.

У випадку одночасного використання надавачем декількох діючих особистих ключів і відповідних до них сертифікатів надавач може вести декілька

списків відкликаних сертифікатів, підписаних різними особистими ключами. В такому разі всі вони публікуються на веб-сайті надавача у наведеному вище порядку.

5.4. Механізм підтвердження володіння особистим ключем, відповідно якому відкритий ключ надається для формування сертифіката ключа

Відкритий ключ заявника надається для формування сертифіката відкритого ключа виключно у вигляді самопідписаного запиту формату PKCS#10. Підтвердження володіння заявником особистим ключем, відповідний якому відкритий ключ надається для формування сертифіката відкритого ключа, забезпечується шляхом перевірки удосконаленого електронного підпису, створеного за допомогою особистого ключа заявника на запиті на формування сертифіката, за допомогою відкритого ключа, що міститься у цьому запиті.

Підтвердження володіння заявником особистим ключем здійснюється без розкриття особистого ключа.

5.5. Умови ідентифікації, автентифікації та верифікації клієнта НЕДП

Формування та видача сертифіката відкритого ключа без ідентифікації особи, ідентифікаційні дані якої міститимуться у сертифікаті відкритого ключа, не допускаються.

Заява для отримання сертифіката ключа підписувачем може мати електронний вигляд, у такому випадку вона повинна бути підписана кваліфікованим електронним підписом (КЕП) клієнта та надана адміністратору реєстрації НЕДП електронною поштою або на носії інформації. Заява, яка має електронний вигляд, приймається до розгляду лише у разі позитивної перевірки КЕП та ідентифікації особи клієнта.

5.5.1. Фізична особа

Ідентифікація фізичної особи, яка звернулася за отриманням електронної довірчої послуги формування, перевірки та підтвердження чинності сертифіката електронного підпису чи печатки, здійснюється виключно за умови її особистої присутності 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.

Допускається ідентифікація заявника надавачем електронних довірчих послуг за ідентифікаційними даними, що містяться у раніше сформованому ним

сертифікаті відкритого ключа, за умови чинності цього сертифіката.

При ідентифікації фізичної особи з'ясовують:

- прізвище, ім'я та по-батькові;
- реєстраційний номер облікової картки платника податків;
- серія та номер паспорта громадянина України або номер паспорта виготовленого у формі картки, що містить безконтактний електронний носій;
- унікальний номер запису в Єдиному державному демографічному реєстрі (за наявності).

5.5.2. Іноземці

Ідентифікація іноземців здійснюється відповідно до законодавства за умови наявності у заявника посвідки на проживання та національного паспорта іноземця або документа, що його замінює.

5.5.3. Юридична особа та представник юридичної особи

Під час перевірки цивільної правоздатності та дієздатності юридичної особи надавач електронних довірчих послуг зобов'язаний ознайомитися з інформацією про юридичну особу, що міститься в ЄДР, а також пересвідчитися, що обсяг її цивільної правоздатності та дієздатності є достатнім для формування та видачі сертифіката відкритого ключа.

Надавач електронних довірчих послуг під час формування та видачі сертифіката відкритого ключа здійснює ідентифікацію особи уповноваженого представника юридичної особи відповідно до вимог Закону України «Про електронні довірчі послуги», а також перевіряє обсяг його повноважень за документом або за даними з ЄДР, що визначають повноваження представника.

Якщо від імені юридичної особи діє колегіальний орган, надавачу електронних довірчих послуг подається документ, у якому визначено повноваження відповідного органу та розподіл обов'язків між його членами.

До розгляду не приймаються документи/копії документів, які мають підчистки, дописки, закреслені слова, інші виправлення або мають пошкодження, внаслідок чого їх текст (фото) неможливо прочитати (розпізнати).

Після позитивної ідентифікації адміністратор реєстрації приймає рішення про реєстрацію заявника.

Реєстрація здійснюється за особистої присутності заявника та є підставою для формування відповідних сертифікатів відкритих ключів.

5.6. Механізм автентифікації підписувачів, які мають чинний сертифікат ключа, сформований НЕДП

Автентифікація користувачів, які мають чинний сертифікат відкритого ключа, сформований надавачем, здійснюється у випадку подання в електронній формі заяв на формування, блокування та скасування сертифікатів відкритих ключів. Перевірка ідентифікаційних даних заявника, який звертається з заявою в електронній формі, а також законності такого звернення, здійснюється шляхом автентифікації підписувача за результатами перевірки кваліфікованого електронного підпису на заяві та встановлення чинності на момент подання заяви сертифіката ключа, що містить ідентифікаційні дані особи.

5.7. Механізм ідентифікації, автентифікації, верифікації підписувачів під час обробки заяв на блокування, скасування або поновлення сертифіката ключа

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

- при письмовому (паперовому) зверненні: лист за підписом підписувача;
- у разі звернення підписувача у електронній формі: за електронним підписом, створеним за допомогою особистого ключа підписувача (у разі чинності відповідного сертифіката ключа підписувача).

Підписувач має право подати до НЕДП заяви про блокування, скасування або поновлення сертифіката відкритого ключа відповідно табл. 5.2.

Таблиця 5.2

Тип операції (причина подання заяв)	Форма подання заяв
Блокування сертифіката відкритого ключа	У формі паперового документа
	У формі електронного документа
	У формі електронного документа з використанням діючого ключа КЕП
Скасування сертифіката відкритого ключа	У формі паперового документа
	У формі електронного документа
	У формі електронного документа з використанням діючого ключа КЕП
Поновлення сертифіката відкритого ключа	У формі паперового документа
	У формі електронного документа з використанням діючого ключа КЕП

5.8. Процедурний контроль

Працівники НЕДП несуть відповідальність за неналежне виконання своїх посадових обов'язків, недотримання вимог нормативно-правових актів у сфері електронних довірчих послуг, вимог внутрішньої організаційно-розпорядчої документації надавача та документації комплексної системи захисту інформації.

Працівники, які виконують функції, безпосередньо пов'язані із наданням електронних довірчих послуг, приступають до виконання таких функцій після ознайомлення із посадовими інструкціями.

5.9. Порядок ведення журналів аудиту подій

НЕДП забезпечує ведення журналів аудиту подій, в яких реєструються події таких типів:

- спроби створення, знищення, встановлення паролів, зміни прав доступу в ПТК НЕДП;
- генерація, використання, знищення особистих ключів НЕДП;
- формування, блокування, скасування та поновлення сертифікатів ключів формування СВС;
- спроби несанкціонованого доступу до ПТК НЕДП;
- надання доступу адміністраторам до ПТК НЕДП;
- помилки в роботі ПТК НЕДП.

Адміністратор безпеки НЕДП зобов'язаний вести журнали обліку, передбачені документацією на систему захисту інформації ПТК НЕДП.

Записи в журналах аудиту подій та журналах обліку повинні містити дату та час події, а також ідентифікувати суб'єкта, що здійснив або ініціював подію. Час, що використовується в журналах аудиту подій в електронній формі, повинен бути синхронізований із Всесвітнім координованим часом із точністю до секунди.

НЕДП забезпечує захист журналів аудиту подій від несанкціонованого перегляду, несанкціонованої модифікації та від знищення.

Адміністратор реєстрації, адміністратор сертифікації, системний адміністратор мають право переглядати журнали аудиту подій, пов'язані з виконанням їх функціональних обов'язків.

НЕДП забезпечує зберігання протягом п'яти років:

- журналів аудиту подій;
- журналів обліку, передбачених документацією на систему захисту інформації ПТК НЕДП.

5.10. Порядок ведення, збереження (із зазначенням строків зберігання), резервування, відновлення, захисту даних, пов'язаних із формуванням та обслуговуванням НЕДП сертифікатів ключів

НЕДП забезпечує зберігання документів, на підставі яких клієнтам надавалися електронні довірчі послуги та були сформовані, блоковані, поновлені, скасовані сертифікати ключів, усі сформовані сертифікати ключів, а також СВС протягом строків, встановлених Правилами застосування переліку документів, що утворюються в діяльності НТУ “ХПІ”, до передавання на архівне зберігання.

НЕДП зобов'язаний створити систему резервування та відновлення функціонування ПТК НЕДП, яка має забезпечити резервування інформації на основному майданчику та у віддаленому резервному пункті, із забезпеченням її захисту від несанкціонованого доступу.

5.11. Порядок та умови генерації, зберігання, використання пар ключів НЕДП

В ІКС надавача використовуються особисті та відповідні їм відкриті ключі за такими призначеннями (сферою використання) та з такими параметрами:

- особисті та відповідні їм відкриті ключі надавача для накладення та перевірки електронного підпису на сертифікатах відкритих ключів підписувачів та СВС зі ступенем розширення основного поля еліптичної кривої не менше 257 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 надавача, що використовуються для надання електронної довірчої послуги формування, перевірки та підтвердження електронної позначки часу, зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;
- особисті та відповідні їм відкриті ключі надавача для накладення та перевірки електронного підпису на даних про статус сертифікатів відкритих ключів підписувачів, 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 серверів обробки запитів, що використовуються для криптографічного захисту повідомлень, які передаються відкритими каналами зв'язку, зі ступенем розширення основного поля еліптичної

кривої не менше 257 згідно з ДСТУ 4145-2002;

- особисті та відповідні їм відкриті ключі посадових осіб, що використовуються для автентифікації посадових осіб та криптографічного захисту повідомлень, зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145- 2002;

- особисті та відповідні їм відкриті ключі надавача для накладення та перевірки електронного підпису на сертифікатах відкритих ключів підписувачів та CBC 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 надавача, що використовуються для надання електронної довірчої послуги формування, перевірки та підтвердження електронної позначки часу із використанням іменованої еліптичної кривої NIST P-256 (secp256r1) для алгоритму ECDSA згідно з ДСТУ ETSI TS 119 312:2015;

- особисті та відповідні їм відкриті ключі надавача для накладення та перевірки електронного підпису на даних про статус сертифікатів відкритих ключів підписувачів, 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 надавача для накладення та перевірки електронного підпису на сертифікатах відкритих ключів підписувачів та CBC з довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI EN 119 312:2015;

- особисті та відповідні їм відкриті ключі надавача, що використовуються для надання електронної довірчої послуги формування, перевірки та підтвердження електронної позначки часу, з довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI EN 119 312:2015;

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

Строк чинності особистого ключа дорівнює строку чинності відповідного сертифіката ключа.

Особисті ключі надавача для накладення та перевірки електронного підпису на сертифікатах відкритих ключів підписувачів та CBC, особисті ключі

надавача, що використовуються для надання електронної довірчої послуги формування, перевірки та підтвердження електронної позначки часу та ключі надавача для накладення та перевірки електронного підпису на даних про статус сертифікатів відкритих ключів підписувачів, що визначається в режимі реального часу, генеруються, зберігаються та застосовуються виключно у засобах електронного підпису чи печатки, що є апаратно-програмними пристроями і входять до складу ІКС надавача.

Ключі НЕДП зберігаються виключно у засобах електронного підпису чи печатки, що забезпечують захист записаних даних від несанкціонованого доступу.

Для застосування ключів НЕДП необхідно ввести паролі доступу до засобу електронного підпису чи печатки.

5.12. Порядок та умови резервного копіювання особистого ключа НЕДП, збереження, доступу та використання резервних копій

Адміністратор сертифікації НЕДП створює резервні копії особистих ключів НЕДП за участю адміністратора безпеки. Адміністратор безпеки реєструє факти створення резервних копій особистих ключів НЕДП у відповідному журналі обліку.

Резервні копії особистих ключів НЕДП зберігаються у засобах електронного підпису чи печатки, що забезпечують захист записаних даних від несанкціонованого доступу.

Особистий ключ НЕДП та всі його резервні копії після закінчення строку дії сертифіката ключа НЕДП знищуються способом, що унеможлиблює їх відновлення. Адміністратор сертифікації здійснює знищення особистих ключів НЕДП та їх резервних копій за участю адміністратора безпеки.

5.13. Генерація ключів користувачів

Особистий ключ підписувача або створювача електронної печатки може бути згенерований:

- на стаціонарному робочому місці підписувача (створювача електронної печатки) або на власному портативному обчислювальному пристрої;
- на робочій станції генерації ключів в офісі надавача або його відокремлених пунктів реєстрації;
- у «хмарному» сховищі ключів надавача.

Якщо пара ключів була згенерована заявником поза приміщенням надавача, ідентифікація такого заявника, перевірка достатності обсягу його цивільної правоздатності і дієздатності, формування та видача йому сертифіката відкритого

ключа здійснюється надавачем після перевірки факту володіння заявником особистим ключем, який відповідає відкритому ключу, наданому для формування сертифіката відкритого ключа, відповідно до пункту 5.4 цього Регламенту.

У разі генерації ключових даних підписувачем у «хмарному» сховищі надавача, яке являє собою засіб КЕП, що реалізує зберігання множини особистих ключів КЕП (наприклад, у мережному криптомодулі), така генерація ініціюється підписувачем самостійно після ідентифікації у «хмарному» сховищі на основі атрибутів захисту від доступу сторонніх осіб до використання особистого ключа (пароль, PIN-код, біометричні дані володільця особистого ключа тощо).

Генерацію та/або управління парою ключів від імені підписувача або створювача електронної печатки може здійснювати виключно надавач. Під час управління парою ключів підписувача або створювача електронної печатки надавач може здійснювати резервне копіювання особистого ключа підписувача або створювача електронної печатки з метою його зберігання за умови дотримання таких вимог:

- рівень безпеки резервної копії особистого ключа повинен відповідати рівню безпеки оригінального особистого ключа;
- кількість резервних копій не повинна перевищувати мінімального значення, необхідного для забезпечення безперервності послуги.

Для генерації особистих ключів використовуються засоби кваліфікованого електронного підпису чи печатки, які перебувають у власності користувачів або надаються надавачем.

Надання надавачем засобів кваліфікованого електронного підпису чи печатки здійснюється у порядку, наведеному у розділі 5.1 цього Регламенту. Згенерований особистий ключ підписувача чи створювача електронної печатки захищається за допомогою атрибутів захисту від доступу сторонніх осіб до параметрів особистого ключа (пароль, PIN-код, біометричні дані володільця особистого ключа тощо).

Під час надання кваліфікованої електронної довірчої послуги із створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток надавачем забезпечується:

- використання підписувачем або створювачем електронної печатки виключно засобу кваліфікованого електронного підпису чи печатки та кваліфікованого сертифіката електронного підпису чи печатки;
- захист обміну інформацією між підписувачем або створювачем електронної печатки та надавачем засобами телекомунікаційних мереж загального користування;
- допомога під час генерації пари ключів підписувача або створювача

електронної печатки у спосіб, що не допускає порушення конфіденційності та цілісності особистого ключа, а також ознайомлення із значенням параметрів особистого ключа та їх копіювання;

- унікальність пари ключів підписувача або створювача електронної печатки;
- зберігання особистого ключа підписувача або створювача електронної печатки;
- захист від доступу сторонніх осіб до параметрів особистого ключа підписувача або створювача електронної печатки під час використання засобу кваліфікованого електронного підпису чи печатки.

5.14. Процедури отримання користувачем особистого ключа в результаті надання електронної довірчої послуги її надавачем

Отримання користувачем особистого ключа у володіння в результаті надання електронної довірчої послуги її надавачем здійснюється за таких умов:

- отримання та використання особистого ключа на правах повного володіння засобом електронного підпису, у тому числі, носієм особистого ключа;
- отримання та використання особистого ключа на правах повного володіння або доступу на договірних засадах до частини ресурсу засобу електронного підпису, який реалізує зберігання множини особистих ключів електронного підпису чи печатки (наприклад, мережний криптомодуль).

Фактичне отримання користувачем особистого ключа відбувається у момент генерації особистого ключа особисто або у момент зміни атрибутів захисту від доступу сторонніх осіб до параметрів особистого ключа (пароль, PIN-код, біометричні дані володільця особистого ключа тощо) у випадку, коли ключові пари були попередньо створено надавачем. Не допускається формування надавачем сертифікатів відкритих ключів до моменту фактичного отримання особистого ключа користувачем.

5.15. Механізм надання відкритого ключа користувача надавачу для формування сертифіката відкритого ключа

Відкритий ключ надається для формування сертифіката відкритого ключа у складі запиту на формування сертифіката відкритого ключа, який являє собою запит формату PKCS#10, що містить відкритий ключ заявника і додаткову інформацію для формування сертифіката.

Запит формату PKCS#10 формується під час генерації особистого та відкритого ключів засобами електронного підпису чи печатки. Формування запиту передбачає створення удосконаленого електронного підпису за

допомогою особистого ключа з однієї пари з відкритим ключем.

Процес подання запиту на формування сертифіката відкритого ключа описаний у положеннях сертифікаційних практик цього Регламенту.

6 ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК

6.1. Процес подання запиту на формування сертифіката ключа

До переліку суб'єктів, уповноважених подавати запит на формування сертифіката відкритого ключа належать заявники.

Запит на формування сертифіката відкритого ключа приймається в обробку після приймання та реєстрації заяви на формування сертифіката, встановлення (ідентифікації) особи заявника та підтвердження володіння заявником особистим ключем, відповідний якому відкритий ключ надається для формування сертифіката відкритого ключа відповідно до вимог цього Регламенту.

Обробка запиту на формування сертифіката відкритого ключа здійснюється програмними засобами ІКС надавача за участю адміністратора сертифікації або автоматично.

Під час обробки запиту на формування сертифіката відкритого ключа засобами ІКС надавача здійснюється перевірка унікальності відкритого ключа в реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів та забезпечується унікальність серійного номера сертифіката електронного підпису чи печатки.

Строк оброблення запиту на формування сертифіката відкритого ключа, поданого разом із заявою на реєстрацію, становить не більше однієї години.

6.2. Порядок надання сформованого сертифіката відкритого ключа користувачу

Надання сформованого сертифіката відкритого ключа заявнику здійснюється в один із способів:

- шляхом запису файлу із сформованим сертифікатом відкритого ключа на носій інформації, наданий заявником;
- шляхом публікації сформованого сертифіката відкритого ключа на офіційному веб-сайті надавача.

Заявник повинен перевірити свої ідентифікаційні дані, внесені надавачем до сертифіката відкритого ключа. Надавач повинен надавати відповідні консультації щодо проведення такої перевірки. Заявник повинен використовувати особистий ключ для створення електронного підпису тільки після проведення перевірки. Використання підписувачем особистого ключа є фактом визнання ним сертифіката відповідного відкритого ключа.

У разі виявлення заявником невідповідності ідентифікаційних даних, внесених надавачем до кваліфікованого сертифіката відкритого ключа, його власник звертається до надавача для скасування сертифіката відкритого ключа та

формування нового сертифіката у порядку, встановленому цим Регламентом.

6.3. Порядок та умови публікації сформованого сертифіката ключа клієнта на Веб-сайт НЕДП

Кваліфіковані сертифікати відкритих ключів підписувачів та створювачів електронних печаток, які надали згоду на їх публікацію, публікуються одразу після формування сертифікатів.

Згода на публікацію кваліфікованих сертифікатів відкритих ключів надається заявниками під час подання заяв на формування сертифікатів.

6.4. Умови використання сертифіката ключа користувача та його особистого ключа

Сертифікати відкритого ключа підписувачів та створювачів електронної печатки використовуються у сферах та із обмеженнями, зазначеними у пунктах 5.1 та 5.2 цього Регламенту.

Користувачі електронних довірчих послуг зобов'язані дотримуватись умов використання особистих ключів та сертифікатів відкритих ключів в межах зобов'язань, передбачених у статті 12 Закону України «Про електронні довірчі послуги», а саме:

- забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа;
- невідкладно повідомляти надавача про підозру або факт компрометації особистого ключа;
- надавати достовірну інформацію, необхідну для отримання електронних довірчих послуг;
- своєчасно здійснювати оплату за електронні довірчі послуги, якщо така оплата передбачена договором між надавачем та користувачем електронних довірчих послуг;
- своєчасно надавати надавачу інформацію про зміну ідентифікаційних даних, які містить сертифікат відкритого ключа;
- не використовувати особистий ключ у разі його компрометації, а також у разі скасування або блокування сертифіката відкритого ключа.

Наслідками неправильного використання сертифіката відкритого ключа та особистого ключа можуть стати недостовірні автентифікація підписувача або створювача електронної печатки в інформаційних системах, заволодіння зловмисниками правами доступу користувача до інформації, підробка електронних документів, матеріальні та репутаційні втрати користувача.

6.5. Процедура подачі запиту на формування сертифіката ключа для підписувачів, які мають чинний сертифікат ключа, сформований НЕДП

Запит на формування нового сертифіката відкритого ключа для користувачів, які мають чинний сертифікат відкритого ключа, попередньо сформований надавачем, подається разом із заявою про формування нового сертифіката відкритого ключа.

Програмні засоби ІКС надавача із інтегрованими засобами електронного підпису чи печатки, розміщені на офіційному веб-сайті надавача, забезпечують:

- перевірку чинності попереднього сертифіката відкритого ключа користувача;
- автоматичне формування заяви про формування нового сертифіката відкритого ключа із використанням ідентифікаційних даних, внесених до попереднього сертифіката;
- створення електронного підпису чи печатки до цієї заяви із використанням попереднього особистого ключа;
- створення запиту на формування сертифіката відкритого ключа у форматі PKCS#10 на згенеровану нову ключову пару;
- передачу запиту на формування нового сертифіката відкритого ключа разом із заявою про формування нового сертифіката відкритого ключа на обробку до ІКС надавача.

Створення заяви про формування нового сертифіката відкритого ключа, запиту на формування нового сертифіката відкритого ключа та їх передача на обробку до ІКС надавача здійснюється із забезпеченням цілісності та конфіденційності інформації за допомогою засобів електронного підпису чи печатки, та засобів криптографічного захисту, які мають позитивний експертний висновок за результатами їх державної експертизи у сфері КЗІ.

6.6. Порядок та умови скасування (блокування, поновлення) сертифіката ключа підписувача

До переліку суб'єктів, уповноважених подавати запит на скасування (блокування та поновлення) сертифіката відкритого ключа формування сертифіката відкритого ключа належать фізичні та юридичні особи, які подають до надавача заяви або надають інформацію, що підтверджує підстави для зміни статусу сертифіката, передбачені статтею 25 Закону України “Про електронні довірчі послуги”.

Перелік підстав для зміни статусу сертифіката із зазначенням суб'єктів подання запитів на зміну статусу та форм підтвердження підстав наведено у таблиці 6.1.

Таблиця 6.1

Підстави для зміни статусу сертифіката	Скасування	Блокування	Поновлення	Підтвердження підстав
подання користувачем електронних довірчих послуг заяви	+	+	+	Заява користувача
смерть фізичної особи - підписувача	+			Документальне підтвердження
припинення діяльності створювача електронної печатки	+			Документальне або технічне (отримання інформації в електронному вигляді з ЄДР) підтвердження
зміни ідентифікаційних даних користувача електронних довірчих послуг	+			Документальне або технічне (отримання інформації в електронному вигляді з ЄДР) підтвердження
надання користувачем електронних довірчих послуг недостовірних ідентифікаційних даних	+			Документальне підтвердження
факт компрометації особистого ключа користувача електронних довірчих послуг, виявлений самостійно користувачем або контролюючим органом під час здійснення заходів державного нагляду (контролю) за дотриманням	+			Документальне підтвердження
вимог законодавства у сфері електронних довірчих послуг				

Підстави для зміни статусу сертифіката	Скасування	Блокування	Поновлення	Підтвердження підстав
повідомлення користувачем електронних довірчих послуг або контролюючим органом про підозру в компрометації особистого ключа користувача електронних довірчих послуг		+		Заява користувача або документальне підтвердження
повідомлення про встановлення недостовірності інформації щодо факту компрометації особистого ключа користувачем електронних довірчих послуг або контролюючим органом, який раніше повідомив про цю підозру			+	Заява користувача або документальне підтвердження
набрання законної сили рішенням суду	+	+	+	Документальне підтвердження
порушення користувачем електронних довірчих послуг істотних умов договору про надання електронних довірчих послуг		+		Документальне підтвердження

Заява про скасування (блокування, поновлення) сертифіката електронного підпису чи печатки подається надавачеві у спосіб, що забезпечує підтвердження особи користувача.

Перелік та опис механізмів автентифікації користувачів з питань блокування, скасування або поновлення сертифіката відкритого ключа наведено у таблиці 5.2 цього Регламенту.

Надавач здійснює цілодобовий прийом та перевірку заяв підписувачів та створювачів електронних печаток про скасування, блокування та поновлення їхніх сертифікатів відкритих ключів в тому числі з використанням інформаційних каналів, відомості про які наведено на офіційному сайті надавача.

Сертифікати відкритих ключів скасовуються, блокуються та поновлюються надавачем не пізніше ніж протягом двох годин від моменту отримання підтвердження підстав для зміни статусу сертифіката та здійснення відповідної перевірки достовірності документальних повідомлень та автентифікації

заявників.

Надавач формує списки відкликаних сертифікатів у вигляді повного та часткового списків. Повний список відкликаних сертифікатів формується та публікується 1 раз на тиждень та містить інформацію про всі відкликані сертифікати ключів, які були сформовані надавачем. Частковий список відкликаних сертифікатів формується та публікується кожні 2 години та містить інформацію про всі відкликані сертифікати, статус яких був змінений в інтервалі між часом формування останнього повного списку відкликаних сертифікатів та часом формування поточного часткового списку відкликаних сертифікатів.

Крім списків відкликаних сертифікатів, розповсюдження інформації про статус сертифікатів електронного підпису чи печатки користувачів також здійснюється шляхом забезпечення можливості перевірки статусу сертифіката електронного підпису чи печатки користувача в режимі реального часу через комунікаційні мережі загального користування із використанням протоколу OCSP.

Посилання на сервіс перевірки статусу сертифіката електронного підпису чи печатки користувача в режимі реального часу вносяться до сертифікатів відкритих ключів підписувачів та створювачів електронної печатки.

6.6.1. Процедура подання заяви на скасування (блокування, поновлення) сертифіката ключа

Блокування сертифіката тимчасово припиняє дію сертифіката ключа. Сертифікат ключа, статус якого змінено на заблокований, у період блокування не використовується.

Скасування сертифіката припиняє дію сертифікату ключа. Скасовані сертифікати поновленню не підлягають.

Поновлення чинності сертифікату ключа можливе лише для сертифікатів, що заблоковані і строк дії, зазначений у сертифікаті ключа, не закінчився.

Підписувач зобов'язаний подавати заяви про блокування, поновлення, скасування сертифікатів ключів відповідно до вимог пункту 5.7 цього Регламенту.

6.6.2. Порядок та умови блокування, поновлення, скасування сертифікатів ключів користувачів, які є співробітниками НТУ «ХП»

Блокування сертифіката здійснюється НЕДП на підставі заяви, що надходить від підписувача установленим порядком в НЕДП в усній, паперовій формі чи у вигляді електронного документа або на підставі іншої причини, зазначеної у цьому Регламенті.

Сертифікат ключа вважається заблокованим з моменту зміни НЕДП статусу сертифіката ключа на заблокований.

Скасування сертифіката здійснюється НЕДП на підставі заяви, що надходить від підписувача установленим порядком в НЕДП в паперовій формі чи у вигляді електронного документа або на підставі іншої причини, зазначеної у цьому Регламенті.

Заява на скасування сертифіката засвідчується відповідно до цього Регламенту. Електронна заява подається до НЕДП за встановленою формою та засвідчується підписувачем (заявником) за допомогою свого особистого ключа (якщо відповідний сертифікат ключа є чинним) і електронною печаткою організації (в разі наявності і у випадку клієнта – юридичної особи).

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

Сертифікат ключа вважається скасованим з моменту зміни НЕДП статусу сертифіката ключа на скасований.

Поновлення чинності сертифікату ключа можливе лише для сертифікатів, що заблоковані і строк дії сертифіката не закінчився. Скасовані сертифікати поновленню не підлягають.

Поновлення чинності сертифіката здійснюється НЕДП на підставі заяви, що надходить встановленим порядком в НЕДП в паперовій формі або у вигляді електронного документа.

Сертифікат ключа вважається поновленим з моменту зміни НЕДП статусу сертифіката ключа на чинний.

НЕДП здійснює прийом та перевірку заяв підписувачів про скасування, блокування, поновлення сертифікатів ключів підписувачів тільки в робочий час, відповідно до розпорядку роботи НЕДП. НЕДП скасовує, блокує та поновлює сертифікати ключів клієнтів не пізніше ніж протягом двох годин від часу реєстрації заяв про скасування, блокування, поновлення сертифікатів ключів підписувачів.

6.7. Порядок та умови надання інформації про статус сертифіката ключів, сформованих НЕДП

НЕДП поширює інформацію про статус сертифіката ключа:

- за запитом підписувача у реальному часі (OCSP-запити) з використанням OCSP-сервера НЕДП;
- шляхом поширення СВС.

Якщо одержати інформацію про статус сертифіката ключа підписувача тимчасово неможливо, то потрібно відмовитися від використання ключа.

6.8. Строки дії сертифікатів ключів, сформованих НЕДП

Строк дії сертифікатів відкритих ключів користувачів становить не більше двох років.

Дата та час початку та закінчення строку дії сертифіката відкритого ключа користувача зазначається у сертифікаті із точністю до однієї секунди.

Після закінчення строку дії сертифіката такий сертифікат відкритого ключа вважається нечинним.

7 ПРОЦЕДУРА ТА ПРОЦЕСИ, ЯКІ ВИКОНУЮТЬСЯ ПІД ЧАС НАДАННЯ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ, ЩО НЕ ПЕРЕДБАЧАЮТЬ ФОРМУВАННЯ ТА ОБСЛУГОВУВАННЯ СЕРТИФІКАТІВ ВІДКРИТИХ КЛЮЧІВ

7.1. Надання засобів електронного підпису чи печатки

Для надання електронних довірчих послуг надавачем використовуються засоби електронного підпису чи печатки, які мають позитивний експертний висновок за результатами їх державної експертизи у сфері КЗІ.

Надання надавачем засобів електронного підпису чи печатки у вигляді апаратно-програмних засобів та їх технічна підтримка і обслуговування здійснюється на договірних засадах.

Надання надавачем засобів електронного підпису чи печатки може здійснюватися шляхом надання доступу до відповідних сервісів через Веб-сайт НЕДП.

Надання надавачем засобів електронного підпису чи печатки у вигляді окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків, може здійснюватись шляхом передачі цих засобів на носіях інформації безпосередньо підписувачу або створювачу електронної печатки або шляхом надання доступу через офіційний веб-сайт надавача.

Допомога при генерації ключів здійснюється адміністратором реєстрації або працівником відокремленого пункту реєстрації, на якого покладено обов'язки з реєстрації користувачів, та який виконує функції адміністратора реєстрації.

7.2. Надання електронної довірчої послуги формування, перевірки та підтвердження електронної позначки часу

Електронна довірча послуга з формування, перевірки та підтвердження електронної позначки часу надається користувачам в режимі реального часу за протоколом TSP.

Електронна довірча послуга формування, перевірки та підтвердження електронної позначки часу включає:

- формування електронної позначки часу;
- передачу електронної позначки часу користувачеві електронної довірчої послуги.

Електронна позначка часу має презумпцію точності дати та часу, на які вона вказує та цілісності електронних даних, з якими ці дата та час пов'язані.

ЗАЯВА на проведення реєстрації та формування сертифіката відкритого ключа електронного підпису

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

Дані Підписувача для формування сертифіката відкритого ключа електронного підпису					
<i>Назва організації</i>					
<i>Прізвище</i>					
<i>Ім'я</i>					
<i>По батькові</i>					
<i>Посада*</i>					
<i>Роль в ЄРДР**</i>					
<i>Реєстраційний номер облікової картки платника податків</i>			<i>серія та номер паспорта/номер ID- картки</i>		
Засоби зв'язку (заповнюються обов'язково)					
<i>Телефон +38</i>	0		<i>E-mail:</i>		
<i>Ключова фраза голосової автентифікації</i>					
<i>Згода підписувача на оброблення персональних даних ***</i>		<i>ТАК</i> ☐ <i>НІ</i> ☐			

* – вказується посада (індекс підрозділу) відповідно до наказу про призначення (обов'язково для доступу в ЄРДР).

** - відповідно до ст. 3 КПК України.

*** – Підписувач надає НЕДП НТУ "ХПІ" згоду на оброблення (збирання, накопичення, зберігання) своїх персональних даних, зазначених у цій заяві та інших документах (заявах), які передбачені Регламентом НТУ "ХПІ" та необхідні для реєстрації його як Підписувача і формування сертифіката.

Підписавши цю Заяву, Ви засвідчуєте повне розуміння Регламенту НЕДП НТУ "ХПІ", значень термінів і всіх умов. Підписавши цю Заяву, Ви підтверджуєте достовірність та правильність зазначеної в ній інформації, погоджуєтесь на формування сертифіката відкритого ключа за вказаними даними та зобов'язуєтесь негайно повідомляти про зміну даних, зазначених у цій Заяві.

<i>Дата</i>	<i>Підпис Підписувача</i>	<i>Прізвище, ініціали Підписувача</i>
«___» _____ 20__ р.	_____	_____

Даний блок заповнюється адміністратором реєстрації

Адміністратор реєстрації _____ / _____ /

дата

підпис

ПІБ

ЗАЯВА

на проведення реєстрації та формування сертифіката відкритого ключа електронної печатки

Заповнюється українською мовою та приймається до розгляду, якщо немає
виправлень, дописок чи необумовлених зауважень

Дані Створювача для формування сертифіката відкритого ключа електронної									
Назва організації									
Код ЄДРПОУ									
Найменува ння									
Відомості про уповноважену посадову особу, відповідальну за застосування									
Прізвище									
Ім'я									
По батькові									
Посада									
Засоби зв'язку (заповнюються обов'язково)									
Телефон +38									
E-mail:									
Ключова фраза голосової									
Згода уповноваженої особи Створювача на оброблення персональних даних *							Відтиск печатки		
ТАК ☐ НІ ☐									
* – Уповноважена особа надає НЕДП НТУ “ХПІ” згоду на оброблення (збирання, накопичення, зберігання) своїх персональних даних, зазначених у цій заяві та інших документах (заявах), які передбачені Регламентом НЕДП НТУ “ХПІ” та необхідні для реєстрації Створювача електронної печатки і формування сертифіката.									
Дата	Підпис			Прізвище, ініціали					
«__» _____ 20__ р.									
Даний блок заповнюється адміністратором реєстрації									
Адміністратор реєстрації _____ / _____ /									

ЗАЯВА**про зміну статусу сертифіката відкритого ключа електронного підпису чи електронної печатки**

Заповнюється українською мовою та приймається до розгляду,
якщо немає виправлень, дописок чи необумовлених зауважень

Дані Підписувача (Створювача електронної печатки), які були зазначені при формуванні сертифіката			
Назва організації			
Код ЄДРПОУ*			
Прізвище			
Ім'я			
По батькові			
Посада			
Реєстраційний номер облікової картки платника податків		серія та номер паспорта/номер ID- картки	
Зміна статусу сертифіката (оберіть один із варіантів)			
Скасувати Заблокувати Поновити			
Причина скасування сертифіката електронного підпису чи електронної печатки (заповнюється обов'язково у разі необхідності скасування сертифіката):			
Підписавши цю Заяву, Ви підтверджуєте достовірність та правильність зазначеної вище інформації.			
Дата	Підпис	Прізвище, ініціали	
«__» _____ 20__ р.	_____	_____	

**- заповнюється при скасуванні електронної печатки*

Даний блок заповнюється адміністратором реєстрації

Адміністратор реєстрації

/

дата

/

підпис ПБ