ЗАТВЕРДЖЕНО
Розпорядження голови
районної державної
адміністрації
27.03.2018 №142

ПОРЯДОК
застосування електронного цифрового підпису
у Пологівській районній державній адміністрації Запорізької області

I. Загальні положення

1. Цей Порядок поширюється на всіх посадових осіб райдержадміністрації, які під час виконання своїх посадових обов'язків використовують електронний цифровий підпис (далі – посадові особи).

2. Застосування електронного цифрового забезпечує відповідальна посадова особа, яка визначається розпорядженням голови райдержадміністрації (далі – відповідальний працівник).

3. Отримання електронних цифрових підписів для райдержадміністрації здійснюється в акредитованих центрах сертифікації ключів в установленому законодавством порядку.

4. Електронний цифровий підпис використовується для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

5. Використання електронного цифрового підпису не змінює порядку підписання договорів та інших документів, встановленого законом для вчинення правочинів у письмовій формі.

6. У разі, коли згідно із законодавством необхідно засвідчити справжність підпису на документах та відповідність копій документів оригіналам, а також для здійснення інформаційного обміну з іншими юридичними особами, посадові особи від імені установи застосовують спеціально призначений для таких цілей електронний цифровий підпис (далі – електронна печатка).

7. Перелік та облік електронних документів, до яких застосовується електронний цифровий підпис визначається інструкцією з діловодства райдержадміністрації.

8. Електронний документообіг райдержадміністрації з іншими установами і організаціями здійснюється за умови використання ними надійних

засобів електронного цифрового підпису та за наявності у них посилених сертифікатів відкритих ключів.

9. У цьому Порядку терміни вживаються у такому значенні:

електронний цифровий підпис (далі - ЕЦП) - вид електронного підпису, отриманого внаслідок криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. ЕЦП накладається за допомогою особистого ключа;

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

посилений сертифікат відкритого ключа - сертифікат відкритого ключа, який відповідає вимогам Закону України «Про електронний цифровий підпис», виданий акредитованим центром сертифікації ключів;

компрометація особистого ключа - будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа;

блокування посиленого сертифіката відкритого ключа - тимчасове зупинення чинності посиленого сертифіката відкритого ключа;

підписувач - зареєстрована в акредитованому центрі сертифікації ключів посадова особа райдержадміністрації, що має особистий ключ і для якої сформовано посилений сертифікат відкритого ключа, яка від свого імені накладає електронний цифровий підпис під час створення електронного документа.

Інші терміни вживаються у значеннях, наведених у Законах України «Про електронний цифровий підпис», «Про телекомунікації», Порядку акредитації центру сертифікації ключів, затвердженому постановою Кабінету Міністрів України від 13 липня 2004 року № 903.

II. Організація та контроль

1. Підставою для надання посадовій особі райдержадміністрації ЕЦП є розпорядження голови райдержадміністрації або наказ керівника апарату райдержадміністрації відповідно до вимог чинного законодавства та внутрішнього порядку роботи з документами.

2. Перелік працівників, яким надається право накладання електронної печатки визначається розпорядженням голови райдержадміністрації.

3. Здійснення заходів із забезпечення застосування ЕЦП та контролю за їх використанням покладається на відповідального працівника.

4. Відповідальний працівник здійснює:

ведення обліку, зберігання та знищення особистих ключів, а також подання до акредитованого центру сертифікації ключів інформації, необхідної для формування, скасування, блокування або поновлення посилених сертифікатів відкритих ключів підписувачів;

доступ користувачів до акредитованого центру сертифікації ключів зі своїх робочих місць;

збір, узагальнення, підготовку, перевірку та подання до акредитованого центру сертифікації ключів інформації, необхідної для формування посилених сертифікатів відкритих ключів підписувачів;

отримання в акредитованому центрі сертифікації ключів посиленого сертифіката відкритого ключа для забезпечення застосування електронної печатки, а також генерація відповідних ключів здійснюється в тому ж порядку, що й для електронного цифрового підпису;

надання допомоги посадовим особам райдержадміністрації при генерації особистих ключів підписувачів, підготовку заяв на формування посилених сертифікатів відкритих ключів підписувачів;

веде журнал обліку ЕЦП за формою, наведеною у додатку, в якому повинна відображатися інформація щодо згенерованих, виданих та знищених ЕЦП;

зберігання документів та їх електронних копій, на підставі яких отримано послуги, пов'язані з електронним цифровим підписом.

5. Надання акредитованому центру сертифікації ключів інформації (відповідних документів), необхідної для формування, скасування, блокування або поновлення посилених сертифікатів відкритих ключів підписувачів адміністрації здійснюється відповідальним працівником, за процедурами встановленими регламентом акредитованого центру сертифікації ключів.

6. Облік та знищення особистих ключів підписувачів здійснюється за формою, що додається.

7. Підписувач для виконання своїх посадових обов'язків не може використовувати одночасно кілька чинних посилених сертифікатів особистого відкритого ключа.

III. Використання, зберігання та знищення особистих ключів підписувачів

1. Використання особистого ключа ЕЦП:

1) підписувач несе відповідальність за зберігання особистого ключа;

2) використання особистого ключа підписувачем здійснюється на умовах конфіденційності. Підписувач зобов'язаний зберігати особистий ключ у таємниці та не допускати його використання іншими особами. Підписувач зобов'язаний зберігати пароль доступу до особистого ключа у таємниці;

3) копіювання особистого ключа та/або передача його іншим особам забороняється;

4) у приміщенні, де перебувають або до якого мають доступ інші особи, забороняється залишати надійні засоби ЕЦП з введеним особистим ключем за відсутності підписувача.

2. Зберігання особистого ключа ЕЦП:

особистий ключ підписувача зберігається у спосіб, що унеможливлює його компрометацію.

3. Знищення особистого ключа ЕЦП:

1) після скасування посилених сертифікатів відкритих ключів підписувачів відповідальний працівник зобов'язаний знищити особистий ключ методом, що не допускає можливості його відновлення;

2) про знищення особистого ключа відповідальний працівник, робить відповідний запис у журналі реєстрації особистих ключів ЕЦП із зазначенням дати, прізвища, ім'я, по батькові та посади особи, ключ якої знищили.

IV. Блокування, поновлення та скасування посиленого сертифіката відкритого ключа

1. Блокування та поновлення посиленого сертифіката відкритого ключа:

1) у разі компрометації або обґрунтованої підозри щодо компрометації особистого ключа підписувач зобов'язаний терміново повідомити про це відповідального працівника, який повинен підготувати заяву на блокування посиленого сертифіката відкритого ключа та безпосередньо звернутися до акредитованого центру сертифікації ключів або його відокремленого пункту реєстрації користувачів;

2) відповідальний працівник здійснює фіксування кожного випадку звернення про блокування та поновлення посиленого сертифіката відкритого ключа;

3) блокований посилений сертифікат відкритого ключа поновлюється:

у разі наявності заяви власника особистого ключа або його уповноваженого представника;

за рішенням суду, що набрало законної сили;

у разі встановлення недостовірності даних про компрометацію особистого ключа.

2. Скасування посиленого сертифіката відкритого ключа:

Посилений сертифікат відкритого ключа підписувача скасовується у разі:

припинення діяльності юридичної особи - власника особистого ключа;

смерті фізичної особи - підписувача або набрання законної сили рішенням суду про оголошення працівника померлим, визнання безвісно відсутнім, недієздатним, обмеження його цивільної дієздатності;

подання недостовірних даних про підписувача;

закінчення строку чинності посиленого сертифіката відкритого ключа;

подання заяви власника особистого ключа або його уповноваженого представника про скасування посиленого сертифіката відкритого ключа;

зміни даних про підписувача, що зазначені у посиленому сертифікаті відкритого ключа;

звільнення підписувача або переведення на іншу посаду;

відсторонення від виконання повноважень за посадою;
компрометації особистого ключа.

Керівник апарату
райдержадміністрації І.В. Браженко

Додаток
до Порядку застосування
електронного цифрового підпису

ЖУРНАЛ
обліку електронних цифрових підписів

№ з/п	Дата	Тип НКІ*	Заводський номер НКІ*	ПІБ підписувача, дата отримання та підпис	Відмітка про інструктаж**	Відмітка про знищення**
1	2	3	4	5	6	7
1.	дата (ДД.ММ.РРРР)		хххххххх		_____ (підпис) П.І.Б.	Знищено (ДД.ММ.РРРР), _____ (підпис) П.І.Б.

* - за наявності носія конфіденційної інформації для особистого електронного цифрового підпису.
** - інструктаж підписувача та знищення особистого цифрового підпису/носія конфіденційної інформації (НКІ) здійснюється відповідальним працівником.