

ЗАТВЕРДЖЕНО

*Рішення виконкому
районної у місті ради
від 17 травня 2017 року № 207*

**ПОРЯДОК
застосування електронної цифрової печатки виконкомом
районної у місті ради**

I. Визначення термінів

1.1. У даному Порядку терміни вживаються у такому значенні:

1.1.1 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. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа;

1.1.2 електронна цифрова печатка - вид печатки, отриманої внаслідок криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати установу. Електронний цифровий печатка накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа;

1.1.3 особистий ключ – параметр криптографічного алгоритму формування електронної печатки;

1.1.4 посилений сертифікат відкритого ключа для забезпечення застосування електронної печатки (далі - сертифікат ключа електронної печатки) - сертифікат ключа електронної печатки, який відповідає вимогам Закону України «Про електронний цифровий підпис», виданий акредитованим центром сертифікації ключів;

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

1.1.6 блокування сертифікату ключа електронної печатки - тимчасове зупинення чинності сертифіката ключа;

1.1.7 підписувач – особа, яка на законних підставах використовує електронну печатку, накладає її під час створення електронного документа.

1.2. Інші терміни застосовуються у значенні, наведеному в законах України «Про електронний цифровий підпис», «Про електронні документи та електронний документообіг», інших нормативно-правових актах.

II. Загальні положення

2.1. Даний Порядок поширюється на працівників відділу бухгалтерського обліку виконкому районної у місті ради, які при виконанні своїх службових обов'язків використовують ЕЦП, електронну цифрову печатку.

2.2 Електронний фінансовий документообіг з органом Казначейства здійснюється з використанням всіма його суб'єктами послуг одного акредитованого центру сертифікації ключів Державної казначейської служби України (АЦСК ДКСУ, далі - центр сертифікації ключів).

2.3. Електронна цифрова печатка призначена для забезпечення діяльності виконкому районної у місті ради, яка здійснюється з використанням електронних фінансових документів.

2.4. Електронна цифрова печатка використовується для засвідчення печаткою справжності електронного підпису голови районної у місті ради, його заступника та підтвердження цілісності даних в електронній формі.

2.5. Використання ЕЦП та електронної цифрової печатки не змінює порядку підписання договорів та інших документів, встановленого законом для вчинення правочинів у письмовій формі.

2.6. Виконком районної у місті ради не застосовує ЕЦП та електронної цифрової печатки:

2.6.1 для складання електронних документів, які не можуть бути оригіналами у випадках, передбачених законодавством (наприклад, номерні бланки тощо);

2.6.2 для складання електронних документів, які згідно із законодавством можуть бути створені лише в одному оригінальному примірнику;

2.6.3 для вчинення правочинів на суму, що перевищує 1 млн. гривень.

2.7. Електронний фінансовий документообіг виконкому районної у місті ради з іншими установами й організаціями здійснюється за умови використання ними надійних засобів ЕЦП, електронної цифрової печатки та наявності у них посилених сертифікатів відкритих ключів.

2.8. Виконком районної у місті ради застосовує електронний цифровий підпис та печатку лише за умови використання надійних засобів електронного цифрового підпису та печатки, що повинне бути підтверджено сертифікатом відповідності або позитивним експертним висновком за результатами державної експертизи у сфері криптографічного захисту інформації, отриманим на ці засоби від Адміністрації Держспецзв'язку, та наявності посилених сертифікатів відкритих ключів.

III. Організація та контроль

3.1. Застосування електронної цифрової печатки для електронних фінансових документів у виконкомі районної у місті ради забезпечує відділ бухгалтерського обліку виконкому районної у місті ради.

3.2. Відділ бухгалтерського обліку виконкому районної у місті ради письмово повідомляє відділ інформатизації виконкому районної у місті ради

та центр сертифікації ключів про формування, блокування, скасування посиленних сертифікатів відкритих ключів електронної печатки.

3.3. Електронна цифрова печатка проставляється на фінансових документах, що створені в електронному вигляді та підлягають передачі до органів податкової та казначейської служби, а саме:

3.3.1 Криворізької Північної об'єднаної державної податкової інспекції Головного управління Державної фіскальної служби у Дніпропетровській області;

3.3.2 Управління Державної казначейської служби України у м. Кривому Розі Дніпропетровської області;

3.3.3 Державної служби статистики.

3.4. Відділ інформатизації виконкому районної у місті ради забезпечує:

3.4.1 ведення обліку засобів електронних цифрових печаток, що використовуються в установі для роботи з електронними фінансовими документами;

3.4.2 ведення обліку носіїв особистих ключів;

3.4.3 зберігання документів, на підставі яких було сформовано посилені сертифікати відкритих ключів електронних печаток;

3.5. Контроль за використанням засобів електронних цифрових печаток здійснює завідуючий відділом бухгалтерського обліку – головний бухгалтер виконкому районної у місті ради.

IV. Порядок організації електронного фінансового документообігу з іншими установами та організаціями

4.1. Здійснення електронного фінансового документообігу з органом казначейської, податкової служби та іншими установами та організаціями можливе за умов використання ними посиленних сертифікатів відкритих ключів.

4.2. Сторони можуть укладати між собою угоду, якою передбачатимуть здійснення спільного електронного фінансового документообігу, порядок підписання електронних фінансових документів, обміну такими документами між собою, конфіденційність та інше.

4.3. Для отримання сертифікатів відкритих ключів сторони електронного фінансового документообігу використовують відкритий каталог посиленних сертифікатів на технологічному ресурсі акредитованого центру сертифікації ключів.

4.4. У разі якщо сторона електронного фінансового документообігу відмовилася від публікації своїх сертифікатів відкритих ключів, вона зобов'язана надати їх за допомогою електронної пошти або особисто через представників.

4.5. Для уникнення непорозумінь та для точного визначення моменту підписання електронного фінансового документа сторони зобов'язані при його підписанні використовувати позначку часу.

V. Умови застосування електронної цифрової печатки та ведення електронного фінансового документообігу з казначейською та податковою службами

5.1. Генерація особистого та відкритого ключів здійснюється безпосередньо в центрі сертифікації ключів (регіональному пункті реєстрації), що обслуговує виконком районної у місті ради.

5.2. У посиленому сертифікаті відкритого ключа електронної печатки зазначаються основні атрибути (інформаційний текст), які внесено в сертифікат згідно з електронною заявкою, а саме: ім'я підписувача – виконком Саксаганської районної у місті ради; ЄДРПОУ - 05410872; область - Дніпропетровська; місто- Кривий Ріг.

5.3. Електронні документи повинні зберігатися на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність на цих носіях.

5.4. Строк зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері.

5.5. Право проставлення електронної печатки на електронних документах надається працівникам відділу бухгалтерського обліку виконкому районної у місті ради даним рішенням виконкому районної у місті.

5.6. Оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з ЕЦП автора та електронною цифровою печаткою.

5.7. У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації, кожний з електронних примірників вважається оригіналом електронного документа.

5.8. Справжність електронної цифрової печатки, накладеної на електронний документ або інші електронні дані, та цілісність цього документа (даних) перевіряється з дотриманням таких вимог:

5.8.1 під час перевірки повинен використовуватися посилений сертифікат ключа, чинний на момент накладення електронної цифрової печатки;

5.8.2 особистий ключ повинен відповідати відкритому ключу, зазначеному у сертифікаті;

5.8.3 на час перевірки повинен бути чинним посилений сертифікат відкритого ключа центру сертифікації ключів та/або посилений сертифікат відкритого ключа відповідного засвідчувального центру.

5.9. Перевірка цілісності електронного документа проводиться шляхом перевірки електронного цифрового підпису та печатки.

5.10. Електронний фінансовий документ, що не відповідає вищезазначеним вимогам, не приймається до розгляду. Відправник такого електронного документа повідомляється про відмову в прийнятті та розгляді документа із зазначенням підстави відмови.

5.11. Датою та часом підписання електронних документів ЕЦП та

засвідчення підписів електронною печаткою вважається дата та час, що зазначені в позначці часу.

5.12. Підписувач зобов'язаний:

5.12.1 дотримуватися вимог чинного законодавства України щодо застосування ЕЦП та електронної печатки;

5.12.2 використовувати надійні засоби для формування та перевірки;

5.12.3 застосовувати позначку часу для підтвердження наявності електронних фінансових документів на певний момент часу;

5.12.4 вести архів надісланих та отриманих електронних документів з ЕЦП та електронною печаткою;

5.12.5 зберігати особистий ключ у таємниці, не допускати використання особистого ключа іншими особами;

5.12.6 негайно інформувати відділ інформатизації виконкому районної у місті ради та центр сертифікації ключів про події, що трапилися до закінчення строку чинності сертифіката, а саме: втрату або компрометацію особистого ключа; виявлену неточність або зміну даних, зазначених у сертифікаті.

VI. Використання, зберігання та знищення особистого ключа (електронна цифрова печатка)

6.1. Використання особистого ключа (електронна цифрова печатка):

6.1.1 підписувач несе відповідальність за зберігання особистого ключа;

6.1.2 підписувач зобов'язаний зберігати пароль доступу до особистого ключа у таємниці;

6.1.3 для забезпечення конфіденційності пароля доступу до особистого ключа підписувач має право систематично змінювати пароль з використанням програмного забезпечення;

6.1.4 копіювання особистих ключів та/або передача їх іншим особам забороняється;

6.1.5 у приміщенні, де знаходяться або до якого мають доступ інші особи, забороняється залишення надійних засобів особистого ключа з введеним особистим ключем у відсутності підписувача.

6.2. Зберігання особистого ключа (електронна цифрова печатка):

6.2.1 особистий ключ зберігають у спосіб, що унеможлиблює її компрометацію (в особистому сейфі, спеціально обладнаному приміщенні тощо);

6.2.2 підписувач, якому надано право накладення електронної печатки на електронних фінансових документах, згідно з цим рішенням несе відповідальність за зберігання особистих ключів, паролів та кодів доступу до них.

6.3. Знищення особистого ключа (електронна цифрова печатка):

6.3.1 після скасування сертифікату відкритого ключа, завідуючий відділом бухгалтерського обліку-головний бухгалтер виконкому районної у

місті ради, зобов'язаний письмово повідомити та передати їх до відділу інформатизації виконкому районної у місті ради разом з метою знищення особистого ключа методом, що не допускає можливості його відновлення;

6.3.2 у зв'язку з неможливістю розшифрування файлів при знищенні особистого ключа, перед знищенням особистого ключа завідуючий відділом бухгалтерського обліку-головний бухгалтер виконкому районної у місті ради, зобов'язаний перевірити наявність чи відсутність електронних фінансових документів, зашифрованих цим ключем. У випадку наявності таких документів, при необхідності, здійснюється їх перешифрування на діючий ключ;

6.3.3 про знищення особистих ключів відповідальна особа відділу інформатизації виконкому районної у місті ради, робить відповідний запис в журналі реєстрації особистих ключів із зазначенням дати, точного часу, прізвища, ім'я по батькові та посади особи, яка знищила ключ.

VII. Блокування, поновлення та скасування посиленого сертифіката відкритого ключа електронної печатки

7.1. Блокування та поновлення сертифіката відкритого ключа електронної печатки:

7.1.1 у разі компрометації або обґрунтованої підозри щодо компрометації особистого ключа (електронна цифрова печатка), підписувач зобов'язаний терміново повідомити про це завідуючого відділом бухгалтерського обліку-головного бухгалтера виконкому районної у місті ради, який готує заяву на блокування сертифіката відкритого ключа електронної печатки та безпосередньо звертається до відділу інформатизації виконкому районної у місті ради та центру сертифікації ключів (регіонального пункту реєстрації заявників);

7.1.2 підставами для блокування посиленого сертифіката відкритого ключа електронної печатки підписувача є:

7.1.2.1 подання заяви власника ключа або його уповноваженого представника;

7.1.2.2 за рішенням суду, що надрало законної сили;

7.1.2.3 у разі компрометації особистого ключа (електронної печатки).

7.2. Скасування сертифіката відкритого ключа електронної печатки:

7.2.1 сертифікат відкритого ключа електронної печатки скасовується у разі:

7.2.1.1 припинення діяльності юридичної особи – власника ключа;

7.2.1.2 закінчення строку чинності сертифіката ключа;

7.2.1.3 подання заяви власника ключа або його уповноваженого представника;

7.2.1.4 подання заяви про блокування та/або скасування сертифіката у зв'язку з підтвердженням факту компрометації особистого ключа;

7.2.1.5 зміна даних, внесених до посиленого сертифіката відкритого ключа цифрової печатки.

7.2.2 відділ інформатизації виконкому районної у місті ради:

7.2.2.1 у разі припинення діяльності виконкому районної у місті ради повідомляє центр сертифікації ключів про необхідність скасування сертифікатів відкритих ключів електронної печатки із зазначенням дати такого скасування;

7.2.2.2 у разі компрометації особистого ключа терміново повідомляє центр сертифікації ключів та надає заяву на скасування сертифіката відкритого ключа електронної печатки.

Керуюча справами виконкому
районної у місті ради

О. Дуванова