

## ІНФОРМАЦІЙНИЙ ЛИСТ

### Основні положення Регламенту. Обов'язки підписувача. Правила та способи роботи з ЕЦП.



#### Основні положення Регламенту АЦСК

АЦСК «MASTERKEY» працює відповідно до *Регламенту* (детально можна ознайомитись на [www.masterkey.com.ua](http://www.masterkey.com.ua)) — документа, яким визначається порядок і правила функціонування акредитованого центру сертифікації ключів (у подальшому Центр сертифікації ключів або ЦСК), та згідно з чинним законодавством України в галузі електронного цифрового підпису.

Відповідно до Регламенту та чинного законодавства під час використання електронного цифрового підпису (ЕЦП) підписувач може зіткнутися з:

- компрометацією особистого ключа;
- блокуванням Сертифіката відкритого ключа;
- відновленням Сертифіката відкритого ключа;
- анулюванням Сертифіката відкритого ключа.

**Компрометація** — це втрата контролю над особистим ключем ЕЦП. Розрізняють два види компрометації: явну і неявну.

До подій явної компрометації особистого ключа ЕЦП відносяться:

- втрата носія ключової інформації;
- порушення правил зберігання і знищення особистого ключа ЕЦП;
- компрометація пароля доступу до особистого ключа ЕЦП;
- випадки, коли ключовий носій вийшов з ладу.

До подій неявної компрометації особистого ключа ЕЦП відносяться:

- виникнення підозри витоку інформації, яку містить особистий ключ;
- тимчасова втрата контролю за зберіганням носія ключової інформації. Подальше використання особистого ключа можливе лише за умови беззаперечної переконаності підписувача щодо відсутності факту компрометації.

#### Блокування Сертифіката відкритого ключа

У разі неявної компрометації особистого ключа ЕЦП підписувач повинен блокувати (припинити дію) Сертифіката відкритого ключа на період з'ясування характеру можливої компрометації. Заблокувати Сертифікат відкритого ключа можна одним з наступних способів:

- за допомогою програмного забезпечення «Програмний комплекс користувача ЦСК»;
- шляхом здійснення телефонного дзвінка в Центр сертифікації ключів;
- при особистому зверненні до Центру сертифікації ключів.

Блокування проводиться Центром сертифікації ключів протягом 2 годин з моменту надходження заяви власника особистого ключа ЕЦП з внесенням відповідних відомостей до реєстру Сертифікатів відкритих ключів. Сертифікат відкритого ключа блокується на строк не менше 10 днів. Протягом подальших 7 днів необхідно відвідати Центр сертифікації ключів і подати заяву про підтвердження блокування (термін блокування визначається власником особистого ключа, але не перевищує термін дії договору). У разі неподання в зазначені терміни письмового підтвердження блокування Сертифіката відкритого ключа по закінченні 10 календарних днів він анулюється.

#### Відновлення Сертифіката відкритого ключа

Після з'ясування виду компрометації та підтвердження або спростування цього факту власник особистого ключа ЕЦП може відновити дію Сертифіката відкритого ключа шляхом подання до ЦСК або його відокремленого пункту реєстрації абонентів письмової заяви. Дія Сертифіката відкритого ключа в цьому випадку поновлюється.

#### Анулювання Сертифіката відкритого ключа

У разі виявлення фактів, що підтверджують явну компрометацію особистого ключа ЕЦП, власникові ключа необхідно подати письмову заяву про анулювання Сертифіката відкритого ключа до Центру сертифікації ключів або його відокремленого пункту реєстрації абонентів. Сертифікат відкритого ключа анулюється протягом 2-х годин з моменту подання заяви.

#### Обов'язки підписувача

Відповідно до Регламенту та чинного законодавства України в галузі електронного цифрового підпису підписувач зобов'язаний:

- надавати достовірні відомості та інформацію, що вимагаються Регламентом ЦСК;
- виконувати вимоги, які передбачені Регламентом ЦСК;
- застосовувати особистий ключ відповідно до його призначення, а також дотримуватися інших вимог щодо його використання, визначених Регламентом ЦСК;
- зберігати особистий ключ у таємниці, не допускати використання особистого ключа іншими особами;
- застосовувати надійні засоби електронного цифрового підпису для генерації особистого та відкритого ключів, формування і перевірки електронного цифрового підпису;
- негайно інформувати ЦСК про такі події:
  - втрату або компрометацію особистого ключа;
  - втрату контролю щодо особистого ключа через компрометацію пароля або коду доступу до нього;
  - виявлені неточності або зміну даних, зазначених у посиленому сертифікаті відкритого ключа;
- не використовувати особистий ключ у разі його компрометації.

#### Правила та способи роботи з ЕЦП

При роботі з ЕЦП можливе використання програмного забезпечення «Програмний комплекс користувача ЦСК» або іншого спеціалізованого програмного забезпечення, в яке інтегровано надійні засоби електронного цифрового підпису.

Програмне забезпечення «Програмний комплекс користувача ЦСК» входить до складу пакета підписувача та дозволяє проводити наступні операції:

- Підписання файлів електронним цифровим підписом.
- Перевірку електронного цифрового підпису файлів.
- Шифрування файлів.
- Розшифрування файлів.

Більш детальну інформацію про функціонування програмного забезпечення і принципи його роботи можна отримати на вкладці «Допомога», яку містить програмне забезпечення «Програмний комплекс користувача ЦСК», або натиснувши клавішу F1 під час роботи з ним.