Затверджую

Заступник Генерального прокурора України
Ю.Ударцов

_____

«_____» _____ 2012 р.

Інструкція
щодо поводження з ключовими документами і носіями

Інструкція створена на виконання вимог Кримінального процесуального кодексу України та Положення про порядок ведення Єдиного реєстру досудових розслідувань, затвердженого Наказом Генерального прокурора України № 69 від 17.08.2012 року.

Посадові особи для роботи в ЄРДР повинні отримати ключі для накладення та перевірки електронного цифрового підпису (ЕЦП). Для накладення цифрового підпису генерується особистий ключ. Використання особистого ключа для накладення електронного цифрового підпису на електронний документ є аналогом особистого підпису на відповідному паперовому документі.

Особистий ключ після генерації зберігається в файловому контейнері (файл з розширенням .nctx). Для збереження ключа посадовець, для якого здійснюється генерація, отримує особистий службовий носій ключової інформації (наприклад, USB флеш диск). Для доступу до особистого ключа його власник під час генерації задає пароль. Для блокування ключа за телефоном користувач при реєстрації повідомляє адміністратору реєстрації секретну фразу-пароль.

Носій ключової інформації разом з особистим ключем є об'єктом суворого зберігання.

Посадова особа, яка є власником особистого ключа ЕЦП, несе персональну відповідальність за збереження цілісності ключового носія і відповідного ключа, а також за недопущення доступу до ключового носія інших осіб.

Ключовий носій повинен зберігатися у службовому сейфі посадової особи або належної користувачу чарунці сейфа, яка повинна надійно зачинятись та опечатуватись.

Власник має право зробити резервний запис паролю доступу до особистого ключа та фрази-паролю тільки на аркуші паперу, який буде зберігатись в

запечатаному конверті в тому ж сховищі, що й ключовий носій. Робити інші записи паролю доступу та фрази-паролю заборонено.

Під час генерації, крім особистого ключа, формується відповідний йому відкритий ключ ЕЦП, він поміщується в сертифікат відкритого ключа та слугує для перевірки справжності ЕЦП програмними засобами ЄРДР.

Сертифікат відкритого ключа має статус, який дозволяє управляти дозволом до використання особистого ключа. Статус може бути: дійсний, блокований чи скасований. Використання особистого ключа можливе тільки при статусі «дійсний».

Під час тимчасового припинення виконання своїх службових обов'язків посадовою особою – власником особистого ключа (у зв'язку з відпусткою, хворобою та ін.), він повинен подати в ЦСК або регіональний центр реєстрації заяву про блокування сертифікату (може бути подана усно за телефоном з використанням фрази-паролю).

Після повернення до виконання службових обов'язків посадовець подає у той же орган заяву про поновлення сертифіката.

Власник особистого ключа зобов'язаний:

- Вживати всіх заходів для забезпечення безпечного зберігання ключового носія;
- Зберігати в таємниці пароль доступу до особистого ключа та фразу-пароль для блокування сертифіката;
- Використовувати ключ тільки особисто та лише в службових цілях;
- Використовувати особистий ключ для накладення ЕЦП тільки якщо сертифікат, відповідний цьому ключу має статус «дійсний».

Категорично заборонено:

- Копіювати ключові дані з ключового носія на будь-які інші носії;
- Робити записи пароля доступу до ключа та фрази-паролю, крім передбаченого цією Інструкцією;
- Залишати без нагляду ключовий носій;
- Передавати ключовий носій іншим особам, включаючи осіб, яким реєстратор чи користувач підпорядкований;
- Зберігати на ключовому носії будь-які дані, крім файлу-контейнеру свого особистого ключа;
- Вводити пароль доступу до особистого ключа у спосіб, що порушує його конфіденційність.

УВАГА!

Розголошення пароля (умисне, випадкове, за необачністю і т.п.), а також втрата ключового носія з особистим ключем або потрапляння до інших осіб, або обґрунтована підозра у доступі до нього інших осіб є фактом компрометації особистого ключа.

У цьому випадку користувач зобов'язаний:

- **Негайно звернутись з усною заявою про блокування сертифікату, що йому належить:**
    - **у робочі дні з 8-00 до 20-00 - у регіональний Центр приймання дзвінків;**
    - **у робочі дні з 20-00 до 8-00 - до чергового оператора приймання дзвінків ЦСК;**
    - **у вихідні дні цілодобово - до чергового оператора приймання дзвінків ЦСК;**
- **Доповісти безпосередньому керівнику про факт компрометації ключа;**
- **Не пізніше наступного робочого дня подати письмову заяву на скасування сертифіката, що йому належить, безпосередньо Адміністратору який здійснював реєстрацію;**
- **У встановленому порядку отримати новий особистий ключ.**

Адреса сайту ЦСК: ca.gp.gov.ua

Телефон чергового оператора приймання дзвінків ЦСК зазначений на сайті.

Телефони регіональних Центрів приймання дзвінків зазначений на сайті.

Начальник відділу –
начальник Центру сертифікації ключів
Генеральної прокуратури України О.Атерлей

Згоден

Начальник управління
інформатизації та зв'язку
Генеральної прокуратури України О.Уманський