

ПАМ'ЯТКА

користувачу Єдиних та Державних реєстрів Міністерства юстиції України щодо підвищення рівня безпеки під час користування ними.

Для запобігання можливному доступу сторонніх осіб до інформації Єдиних та Державних реєстрів Міністерства юстиції України (далі - Реєстри) за Вашими особистими атрибутами відповідно до рекомендацій фахівців у сфері захисту інформації та правоохоронної діяльності необхідно дотримуватися наведених нижче рекомендацій.

1. Для проведення реєстраційних дій у Реєстрах використовувати окремий спеціально налаштований комп'ютер за можливості з фіксованою IP- адресою без доступу до мережі WI-FI.
2. Для роботи з Реєстрами використовувати захищений носій особистих ключів з вбудованими програмно-апаратними засобами, що має позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.
3. Не використовувати сторонні носії інформації (флеш-носії, карти пам'яті, диски тощо) на комп'ютері, призначеному для роботи з Реєстрами.
4. Регулярно змінювати паролі доступу до Реєстрів та особистого ключа ЕЦП з використанням багатосимвольних комбінацій з прописних і строкових літер, цифр та спеціальних символів.
5. Не розголошувати ідентифікатори доступу до системи, а також пароль доступу до особистого ключа, не залишати без нагляду та не передавати захищений носій ключової інформації іншим (навіть довіреним) особам. За необхідності фіксування паролів на паперових носіях, зберігати останні у сейфі (сховищі).
6. Використовувати виключно ліцензійне програмне забезпечення (операційна система, офісні програми тощо). Не встановлювати додаткових програмних засобів на комп'ютерному робочому місці, призначеному для роботи з Реєстрами, окрім тих, що необхідні для роботи.
7. Встановити пароль на вхід до операційної системи.
8. Вимкнути функції віддаленого доступу та автоматичного завантаження сторонніх програм, що дозволяють віддалене управління комп'ютером.
9. Створити окремий обліковий запис в операційній системі Windows без прав адміністратора для роботи з Реєстрами та документами.
10. Використовувати виключно ліцензійне антивірусне програмне забезпечення, що має чинний позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації, з актуальними анти вірусними базами даних.
11. Періодично та при підозрі зараження здійснювати антивірусну перевірку комп'ютера.
12. Не використовувати засоби електронного поштового листування на комп'ютерному робочому місці, призначеному для роботи з Реєстрами. Взагалі, під час користування електронною поштою, не відкривати електронні листи від невідомих адресатів, особливо з прикріпленими файлами, не переходити за наведеними в них посиланнями.

13. Не залишати носії з ключами ЕЦП у комп'ютері, а також відкриті сесії роботи з Реєстрами у разі необхідності тимчасового залишення робочого місця.

14. Не залишати фахівця з налаштування комп'ютерної техніки сам на сам з комп'ютером, на якому встановлено програмне забезпечення для роботи з Реєстрами, та не надавати йому паролі і ключі