NovaPay

додаток 2 до наказу
від 20.12.2023 № 2183

Інструкція (рекомендації)
про порядок забезпечення захисту ключів КЕП на клієнтському місці системи дистанційного обслуговування рахунку у ТОВ «НоваПей» (далі Система)

Підписувач, який створює електронний документ з накладенням кваліфікованого електронного підпису (далі – КЕП), або накладає КЕП на вже створений документ, цим самим засвідчує, що ознайомився з усім текстом документа, повністю зрозумів його зміст, не має заперечень до тексту документа (або його заперечення внесені як окремий реквізит документа) і свідомо застосовував свій КЕП у контексті, передбаченому документом (підписав, затвердив, погодив, завізував, засвідчив, ознайомився).

1. Користувач повинен зберігати КЕП на з'ємному захищеному носії інформації (далі – носій) та не допускати зберігання КЕП на комп'ютері.

2. Термін дії ключів КЕП встановлюється Кваліфікованим надавачем електронних довірчих послуг, але Користувач має право самостійно виконувати позапланову зміну ключів КЕП.

3. Користувач не має права передавати носій інформації з ключами КЕП у користування третім особам та іншим уповноваженим особам, якщо у Користувача передбачено дві (або більше) груп підпису, залишати його без нагляду, повідомляти пароль або код розблокування від захищеного носія ключів КЕП третім особам, в тому числі працівникам ТОВ «НоваПей». Користувач самостійно відповідає за схоронність ключів КЕП.

Увага! Особистий ключ кваліфікованого електронного підпису переданий іншій особі, вважається скомпрометованим, тобто недійсним.

4. Необхідно використовувати стійкі паролі та коди розблокування до захищеного носія ключів КЕП.

Паролі та коди розблокування повинні:

- не містити особистих даних, які легко отримати третім особам (ім'я, дата народження, адреса проживання, тощо);
- не містити символи що знаходяться підряд на клавіатурі, наприклад qwerty, 12345;
- складатися з 8 – 9 символів та містити букви, цифри та спецсимволи, наприклад Vtnf,fyr20.

5. Рекомендується змінювати пароль не рідше ніж раз на місяць та не використовувати паролі, що застосовувались раніше.

6. Користувач повинен забезпечити використання ліцензійного програмного забезпечення в тому числі антивірусних програмних засобів та своєчасне оновлення баз вірусних сигнатур до останніх версій, на тих комп'ютерних станціях, з яких здійснюється робота в Системі.

7. Користувач повинен уникати виконання сумнівних програм, що маскуються під програми надавачів платіжних послуг та пропонують надати інформацію щодо ключа КЕП та паролю доступу до нього. Не натискати на посилання в підозрілих поштових повідомленнях, а також не надавати персональну інформацію на будь – яких сайтах, у надійності яких немає впевненості.

8. Користувач повинен уникати відвідування інтернет-сторінок розважального характеру, соціальних мереж з того комп'ютера, з якого здійснюється робота в Системі.

9. Користувач повинен уникати використання неліцензійного програмного забезпечення, оскільки такі програми можуть містити віруси.

10. Наполегливо рекомендується встановлювати надійні паролі на облікові записи користувачів комп'ютера.

11. Наполегливо рекомендується працювати з Системою з окремого комп'ютера виділеного виключно для цих цілей.

12. Користувач повинен уникати обслуговування ненадійними IT- спеціалістами комп'ютерних станцій, з яких Користувач працює в Системі.

13. Зберігати носій в добре захищеному місці (наприклад в сейфі), яке виключає можливість використання носія третіми особами.

14. Користувач повинен виймати носій з комп’ютера в моменти коли він безпосередньо не здійснює підписання документів в Системі. (При безконтрольному підключенні носія до комп’ютерної станції існує ризик, що зловмисник за допомогою зараження вірусом отримає віддалене управління комп’ютером і відповідно підключеним носієм і виконає шахрайські операції від імені Користувача).

15. Користувач повинен уникати випадків одночасного підключення до комп’ютера, з якого здійснюється робота в Системі, декількох носіїв, якщо у Користувача передбачено дві (або більше) груп підпису Електронних документів.

16. Користувач повинен уникати механічних пошкоджень носія, потрапляння вологи, сильного нагріву, дії сильних електромагнітних полів. Не прикладати надмірних зусиль при підключенні та відключенні носія від комп’ютера.

17. Рекомендується застосування Користувачем таких додаткових заходів безпеки як:

- збереження ключів КЕП здійснювати на захищених носіях інформації ;
- застосування ір-фільтрації;
- підтвердження електронних документів одноразовим паролем (SMS-повідомлення).

18. У разі втрати, викрадення носія, або виникнення підозр, що в Системі від імені Користувача було здійснено несанкціоновані операції, Користувач повинен негайно припинити роботу в Системі та повідомити про це ТОВ «НоваПей» телефоном через Контактний центр за № 0800304949 з подальшим наданням оригіналу такого повідомлення (листа), скріпленого підписом Уповноваженої особи Користувача і відбитком печатки (у разі її наявності).

19. На підставі повідомлення ТОВ «НоваПей» заблокує доступ Користувача до Системи (рахунків) та скомпрометований ключ Користувача для запобігання подальших шахрайських операцій. Користувачу необхідно звірити з ТОВ «НоваПей» останні платежі, отримані від Користувача засобами Системи, впевнитись в тому, що виконуються усі вимоги даної інструкції; змінити коди носія, на якому зберігалися скомпрометовані ключі КЕП; звернутися до надавача електронних довірчих послуг.