Інформаційний додаток
до Договору на розрахункове обслуговування за дистанційною системою

Інструкція про порядок забезпечення захисту ключів КЕП на клієнтському місці

Всі терміни, що використовуються у тексті цієї Інструкції про порядок забезпечення захисту ключів КЕП на клієнтському місці мають значення, викладені в Типових умовах та Договорі на розрахункове обслуговування за дистанційною системою.

Підписувач, який створює електронний документ з КЕП, 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. Клієнт повинен зберігати КЕП на з'ємному носії інформації (далі – носій) та не допускати зберігання Особистих ключів на комп'ютері.
2. Термін дії ключів КЕП встановлюється Акредитованим центром сертифікації ключів, але Клієнт має право самостійно виконувати позапланову зміну ключів КЕП.
3. Клієнт не має права передавати носій інформації з ключами КЕП у користування третім особам та іншим уповноваженим особам, якщо у Клієнта 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 Банку. Клієнт 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 та не використовувати паролі, що застосовувались раніше.
6. Клієнт 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. Клієнт повинен уникати виконання сумнівних програм, що маскуються під банківські 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. У разі виявлення сумнівних листів, програм чи будь-яких повідомлень Клієнт повинен проінформувати Банк офіційним листом.
9. Клієнт повинен уникати відвідування інтернет-сторінок розважального характеру, соціальних мереж з того комп'ютера, з якого здійснюється робота в Системі.
10. Клієнт повинен уникати використання неліцензійного програмного забезпечення, оскільки такі програми можуть містити віруси.
11. Наполегливо рекомендується встановлювати надійні паролі на облікові записи користувачів комп'ютера.
12. Наполегливо рекомендується працювати з Системою з окремого комп'ютера виділеного виключно для цих цілей.
13. Клієнт повинен уникати обслуговування ненадійними IT- спеціалістами комп'ютерних станцій, з яких Клієнт працює в Системі.
14. Зберігати носій в добре захищеному місці (наприклад в сейфі), яке виключає можливість використання носія третіми особами.
15. Клієнт 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 Клієнта).

16. Клієнт повинен уникати випадків одночасного підключення до комп'ютера, з якого здійснюється робота в Системі, декількох носіїв, якщо у Клієнта передбачено дві (або більше) груп підпису Електронних документів.
17. Клієнт 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.
18. Рекомендується застосування Клієнтом таких додаткових заходів безпеки як:
    - збереження ключів КЕП здійснювати на захищених носіях інформації ;
    - застосування ір-фільтрації;
    - підтвердження електронних документів одноразовим паролем (SMS-повідомлення).
19. В разі втрати, викрадення носія, або виникнення підозр, що в Системі від імені Клієнта було здійснено несанкціоновані операції, Клієнт повинен негайно припинити роботу в Системі та повідомити про це Банк будь-якими доступними засобами в тому числі, але не виключно засобами Системи та/або телефонним зв'язком та/або факсимільним зв'язком, з подальшим наданням оригіналу такого повідомлення (листа), скріпленого підписом Уповноваженої особи Клієнта і відбитком печатки (у разі її наявності).
20. На підставі повідомлення Банк заблокує доступ Користувача до Системи (рахунків) та скомпрометований ключ Клієнта для запобігання подальших шахрайських операцій. Клієнту необхідно звірити з Банком останні платежі, отримані Банком від Клієнта засобами Системи впевнитись в тому, що виконуються усі вимоги даної інструкції; змінити коди носія, на якому зберігалися скомпрометовані ключі КЕП; звернутися до надавача електронних довірчіх послуг.
21. Відповідно до "Положення про застосування електронного підпису та електронної печатки в банківській системі України ",постанова № 78 від 14.08.2017р. зі змінами та доповненнями, Підписувачу забороняється створювати кваліфікований ЕП, якщо кваліфікований сертифікат відкритого ключа підписувача є нечинним або одержати інформацію про його статус неможливо.