

**Інструкція щодо забезпечення захисту ключів Кваліфікованого ЕП на клієнтському місці**

Всі терміни, що використовуються у тексті цієї Інструкції щодо забезпечення захисту ключів Кваліфікованого ЕП на клієнтському місці (далі – Інструкція) мають значення, викладені у Договорі комплексного банківського обслуговування.

1. Клієнт повинен генерувати та зберігати Особистий ключ Кваліфікованого ЕП чи Печатки виключно у Засобі Кваліфікованого ЕП чи Печатки, наданому Банком, а у разі укладення між Банком та Клієнтом відповідної угоди — на власному з’ємному носію інформації (далі — Носій), у разі якщо таке зберігання дозволене законодавством у сфері електронних довірчих послуг та не допускати зберігання Особистого ключа Кваліфікованого ЕП чи Печатки на комп’ютері.
2. Клієнт не має права надавати Носій з ключами Кваліфікованого ЕП у користування третім особам та іншим уповноваженим особам, якщо у Клієнта передбачено дві (або більше) груп підпису, залишати його без нагляду, повідомляти пароль (PIN-код) або код розблокування Носія, або логін, пароль та ПІН-код доступу до Особистого ключа Кваліфікованого ЕП чи Печатки, що зберігається у HSM третім особам, у тому числі працівникам Банку.
3. Клієнт самостійно відповідає за схоронність ключів Кваліфікованого ЕП і повинен зберігати Носій в добре захищеному місці (наприклад, в сейфі), яке виключає можливість використання Носія сторонніми особами.
4. Забезпечити використання виключно засобів Кваліфікованого ЕП чи Печатки для генерації Особистих та Відкритих ключів, формування та перевірки Кваліфіконого ЕП чи Печатки. Інші засоби можуть використовуватись лише у разі, якщо використання таких засобів дозволено законодавством у сфері електронних довірчих послуг.
5. Використовувати Особистий ключ виключно за його призначенням, визначеним в Сертифікаті відповідного Відкритого ключа, а також додержуватися інших вимог використання Особистого ключа, визначених Регламентом КНЕДП.
6. Забезпечити зберігання Особистого ключа у таємниці та у спосіб, що унеможливлює його використання іншими особами.
7. Забезпечити використання Особистих ключів та паролів доступу в спосіб, що унеможливлює ознайомлення із ним інших осіб.
8. Забезпечити конфіденційність своїх автентифікаційних даних доступу до Особистого ключа у HSM КНЕДП, у спосіб, що унеможливлює ознайомлення із ними інших осіб.
9. Не розголошувати та не повідомляти іншим особам пароль доступу до Особистого ключа.
10. Забезпечити виконання Підписувачами умов щодо нерозголошення іншим особам коду доступу до захищеного носія Особистого ключа та парольної фрази голосової аутентифікації.
11. Негайно інформувати КНЕДП про компрометацію Особистого ключа, втрату контролю щодо Особистого ключа через компрометацію пароля, коду доступу до нього, фізичне пошкодження або втрату носія тощо, виявлену неточність або зміну даних, зазначених у Сертифікаті.
12. Клієнт повинен виймати Носій з комп’ютера у моменти, коли він безпосередньо не здійснює підписання документів в Системі (при безконтрольному підключенні Носія до комп’ютера існує ризик, що зловмисник за допомогою вірусних програм отримає віддалене управління комп’ютером, і відповідно підключеним Носієм, і виконає шахрайські операції від імені Клієнта).
13. 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.
14. 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.
15. У 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, у тому числі, але не виключно, засобами Системи та/або телефонним зв’язком, з подальшим наданням оригіналу такого повідомлення (листа), скріпленого підписом Уповноваженої особи Клієнта і відбитком печатки (у разі її наявності).
16. На підставі повідомлення Банк заблокує доступ Користувача до Рахунків та скомпрометований ключ Кваліфікованого ЕП Клієнта для запобігання подальших шахрайських операцій. Клієнту необхідно звірити з Банком останні платежі, отримані Банком від Клієнта засобами Системи, і впевнитися у тому, що виконуються усі вимоги даної інструкції; змінити коди Носія (PIN-код і код розблокування), на якому зберігалися скомпрометовані ключі Кваліфікованого ЕП; провести позапланову генерацію скомпрометованого ключа Кваліфікованого ЕП; змінити ім’я Користувача (Логін).
17. Термін дії ключів Кваліфікованого ЕП встановлюється Банком/кваліфікованим надавачем електронних довірчих послуг, але Клієнт має право самостійно виконувати позапланову зміну ключів Кваліфікованого ЕП у порядку, визначеному Договором.
18. Наполегливо рекомендується встановлювати надійні паролі на облікові записи користувачів комп’ютера, коди Носія ключів Кваліфікованого ЕП і не використовувати їх для інших цілей — електронної пошти, соцмереж, кодів авторизацій, тощо.
19. Паролі та коди Носія повинні:
	* не містити особистих даних, які легко отримати третім особам (ім’я, особисті дати, адреси, тощо);
	* не містити символи, що знаходяться підряд на клавіатурі, наприклад qwerty, 12345;
	* складатися з 8 – 9 символів та містити букви великі і малі, цифри та спецсимволи, наприклад @GasDeng1.
20. Рекомендується регулярно змінювати паролі та не використовувати паролі, що застосовувалися раніше.
21. Клієнт повинен відключити у Інтернет-браузері функцію запам’ятовування або автозаповнення пароля.
22. Наполегливо рекомендується працювати з Системою з окремого комп’ютера, виділеного виключно для цих цілей.
23. Клієнт повинен уникати відвідування інтернет-сторінок (окрім інтернет-сторінок Банку і Системи), соціальних мереж, завантаження файлів, з того комп’ютера, з якого здійснюється робота в Системі, а також не використовувати при роботі з Системою незахищені Wi-Fi з‘єднання (в кафе, готелях, офісах, інших громадських місцях).
24. Клієнт повинен використовувати ліцензійне програмне забезпечення з підтримкою і регулярно оновлювати його до актуальних версій, у тому числі антивірусних програмних засобів, на тих комп’ютерах, з яких здійснюється робота в Системі. Регулярне оновлення сигнатурних баз антивірусних засобів і сканування комп’ютерів є обов’язковим!
25. Клієнт повинен уникати виконання будь-яких програм, що маскуються під банківські та пропонують надати інформацію щодо ключа Кваліфікованого ЕП та паролю доступу до нього. Не натискати на посилання у підозрілих поштових повідомленнях, а також не надавати персональну інформацію на будь – яких сайтах, у надійності яких немає впевненості.
26. Клієнт повинен здійснювати доступ до Системи виключно з інтернет-сторінки Банку, попередньо перевіривши надійність з’єднання (значок «колодка»  біля адреси сторінки, що свідчить про використання https-сертифікату).
27. Клієнт повинен уникати обслуговування ненадійними ІТ- спеціалістами комп’ютерів, з яких Клієнт працює в Системі.
28. Рекомендується застосування Клієнтом таких додаткових заходів безпеки як:
* застосування ІР-фільтрації на комп’ютері, з якого здійснюється робота з Системою;
* використання додаткової автентифікації (підтвердження електронних документів одноразовим паролем;
* послуга інформування про руш коштів по рахунках.