Правила користування Засобами дистанційного обслуговування

1. **Правила безпечної роботи з Засобами дистанційного обслуговування**

1.1. Уникайте використання Системи «Клієнт-Банк» та/або Мобільного застосунку (далі - Система) з комп'ютерів/мобільних пристроях в громадських місцях, а також з пристроїв, налаштування яких знаходиться поза Вашим контролем. Якщо це можливо, для роботи з Системою використовуйте окремий пристрій з обмеженим доступом, з якого не здійснюється відвідування Інтернет сайтів, та на якому встановлено тільки необхідне для роботи Системи апаратне та ліцензійне програмне забезпечення. Регулярно відслідковуйте появу та по можливості встановлюйте всі виправлення з безпеки від виробників програмного забезпечення, що встановлено на Робочому місці.

1.2. Не відповідайте на листи з проханням вислати секретний ключ Електронного підпису (далі - ЕП), пароль та інші Ваші конфіденційні дані. Банк ніколи не надсилає запит на отримання у клієнтів конфіденційної інформації через електронну пошту, Сайт Банку або будь-яким іншим способом.

1.3. Не допускайте до Робочих місць Системи не уповноважених осіб.

1.4. Не встановлюйте і не зберігайте підозрілі файли, отримані з сумнівних джерел, завантажені з невідомих сайтів, надіслані електронною поштою або отримані на форумах. У випадку необхідності завантаження файлу, обов'язково перевірте його за допомогою антивірусу. Відмовтесь від відвідування сайтів сумнівного змісту.

1.5. Використовуйте на Робочому місці ліцензійні засоби антивірусного захисту відомих виробників. Регулярно оновлюйте антивірусні бази. Застосовуйте спеціалізовані програмні засоби безпеки: персональні фаєрволи, анти-шпигунське програмне забезпечення і т.п. з максимально можливими налаштуваннями безпеки.

1.6. Якщо це можливо, не працюйте на Робочому місці з правами адміністратора операційної системи.

1.7. Регулярно перевіряйте наявність оновлень програмного забезпечення Системи засобами Системи.

1.8. Використовуйте найновіші версії Системи.

1.9. Використовуйте для введення логінів/паролів віртуальну клавіатуру, що вбудована в нові версії програмного забезпечення Системи.

2. **Правила використання ключа ЕП і пароля доступу до ключа ЕП**

2.1. Використовуйте для зберігання файлів з секретними ключами ЕП окремі носії: CD/DVD, USB флеш-накопичувачі та інші. Не зберігайте секретні ключі ЕП на жорсткому диску.

2.2. Від'єднуйте носії з ключами ЕП, якщо вони не використовуються для роботи з Системою та зберігайте їх в сейфі або столі, що зачиняється на ключ.

2.3. Не розповсюджуйте паролі до секретних ключів, не записуйте їх та не зберігайте разом з носієм ЕП.

2.4. Вимоги до складності паролів:

- пароль не повинен співпадати з логіном користувача або бути його часткою;
- не використовуйте як пароль особисті дані і змістові значення (імена, назви, дати, словникові слова);
- якщо це можливо використовуйте довільні сполучення літерних символів різних регістрів, цифр та/або спеціальних символів (без лапок): ")", "(", "*", "%", "`", ".", "!" , "@", ",", "#", ";", ":", "$", "^", "&", "+", "-", і пропуск;
- довжина паролю - не менше 8-ми символів;
- повинен включати і літери і цифри; як мінімум одна літера у верхньому регістрі;

2.5. Замініть ключ ЕП у разі звільнення відповідального працівника, який мав доступ до ключа ЕП.

2.6. У разі виникнення будь-яких підозр на компрометацію (копіювання, втрату) секретних ключів ЕП або компрометацію середовища виконання (наявність в комп'ютері шкідливих програм) – обов'язково зверніться в Банк стосовно генерації нового ключа ЕП або його блокування.

2.7. Звертаємо Вашу увагу, що Банк не має доступу до Ваших секретних ключів і можливості підписання платіжних документів ЕП від імені Вашого імені. У Банку зберігається відкритий ключ Вашого ЕП, який використовується виключно для перевірки ЕП на підписаних Вашим секретним ключем електронних платіжних документах. Банк не несе відповідальності за збереження секретних ключів ЕП, які знаходяться у Вас, і можливі фінансові втрати у випадку виконання фальшивих платіжних документів, адже Ви - єдиний власник ЕП.

3. Клієнт ознайомлений та добре розуміє, що перелік, правил користування Засобами дистанційного обслуговування, не є вичерпним. Клієнт має право, на власний розсуд, застосовувати інші заходи, які на його погляд, є ефективними та забезпечують більш високий рівень безпеки користування Засобами дистанційного обслуговування.