Додаток 10

Правила інформаційної безпеки при роботі з використанням системи «PRAVEXBANK BIZ»

1. Не передавати для роботи і/або збереження носії з особистими ключами електронного цифрового підпису (далі – ЕЦП) навіть тимчасово та не розголошувати паролі до них стороннім особам.

2. Забезпечувати збереження носіїв з ключами ЕЦП та, при наявності, їх копій в місцях недоступних для сторонніх осіб.

3. Уникати збереження та роботи з ключами ЕЦП при їх розташуванні на жорсткому диску комп'ютера.

4. При використанні змінних носіїв з електронними ключами не зберігати особисті електронні ключі безпосередньо на жорсткому диску машини.

5. Після закінчення роботи з системою «PRAVEXBANK BIZ» носії з електронними ключами повинні бути відокремлені від комп'ютера.

6. Уникати введення паролів до ключів ЕЦП та системи «PRAVEXBANK BIZ» в присутності сторонніх осіб.

7. При перегенерації ключа ЕЦП необхідно замінити до нього пароль, дотримуючись таких рекомендацій:

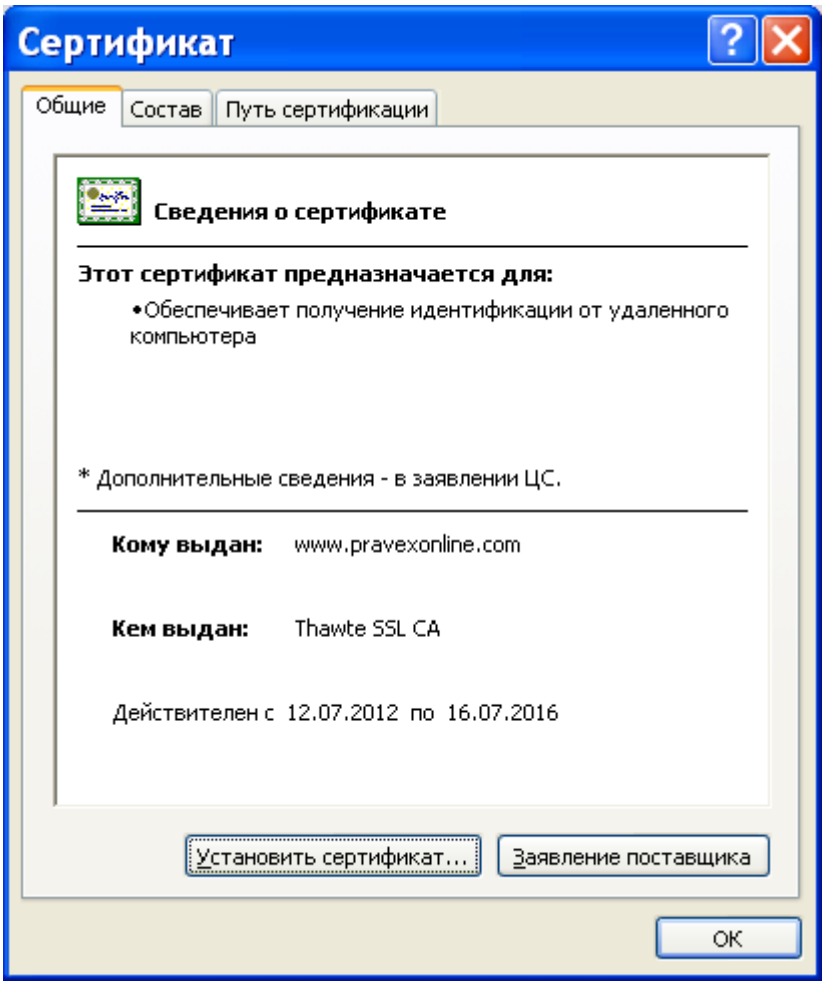
- при створенні паролю необхідно використовувати комбінації з великих та маленьких літер, цифр та спеціальних символів;
- не використовувати тривіальні (легкі для підбору) паролі та паролі, що пов'язані з Вашими персональними даними чи даними Ваших близьких;
- не використовувати функцію «запам'ятовування пароля» WEB-браузером чи іншим програмним забезпеченням, встановленим на Вашому ПК, ноутбуці тощо.

8. Тримати в таємниці інформацію (пароль, дані щодо рахунків тощо), що використовується Вами для входу та блокування системи «PRAVEXBANK BIZ», навіть отримавши усне чи письмове звернення від працівників Банку, та дотримуватись таких рекомендацій:

- не вводити цю інформацію на будь-яких інших WEB-сторінках, окрім робочої сторінки системи «PRAVEXBANK BIZ»;
- не зберігати цю інформацію на комп'ютері, з якого здійснюється робота з системою «PRAVEXBANK BIZ», а також, в будь-якому іншому вигляді (на паперових носіях, змінних носіях тощо), що може бути доступним стороннім особам;
- перед початком роботи із системою «PRAVEXBANK BIZ» та введенням персональних даних на сторінці авторизації необхідно впевнитись, що Ви знаходитесь на сторінці Банку https://www.pravexonline.com;
- обов'язково зверніть увагу на те, щоб адреса починалася з **https**, де літера «s» вказує на ознаку захищеного з'єднання з сервером Банку;
- бажано впевнитись, що Ви знаходитесь на сервері Банку, перевіривши електронний сертифікат, за допомогою якого здійснюється захищене з'єднання. Позначка, що визначає захищене з'єднання, в браузерах найчастіше зустрічається у вигляді «навісного механічного

замка». Натиснувши на дану позначку (наприклад для браузера Internet Explorer), можливо переглянути електронний сертифікат, яким захищений WEB-сервер Банку.

Електронний сертифікат, яким на даний час засвідчений WEB-сервер банку, має приведений нижче вигляд:



9. З метою надійної роботи комп'ютера та забезпечення інформаційної безпеки рекомендуємо використовувати антивірусне програмне забезпечення відомих виробників та своєчасно обновляти його антивірусні бази.

10. Не використовувати для роботи с системою «PRAVEXBANK BIZ» технічні засоби сторонніх осіб та ті, що встановлені у публічних місцях (інтернет-клуби, інтернет-кафе тощо).

11. Для запобігання зовнішніх вторгнень та виключення можливості підключення сторонніми особами ззовні, бажаним є застосування на обладнанні, що використовується для роботи із системою «PRAVEXBANK BIZ», мережевих екранів (брандмауерів).

12. Виконати налаштування щодо заборони доступу до комп'ютера з віддаленої машини.

13. Пам'ятайте, що будь-яка особа, яка має безпосередній доступ до технічних засобів, з яких ведеться робота із системою «PRAVEXBANK BIZ», має можливість встановити шкідливе програмне забезпечення та заволодіти Вашими персональними даними та електронними ключами, які в подальшому можуть бути використані для роботи в системі «PRAVEXBANK BIZ» від Вашого імені.

14. У разі зміни картки зі зразками підписів Клієнта, у випадку втрати носіїв або виникнення підозри щодо несанкціонованого копіювання секретних ключів необхідно негайно припинити обмін інформацією в системі.

15. За телефоном (044) 521-02-70 або 0800500450 необхідно проінформувати Банк про порушення секретності (компрометації) ключів ЕЦП та паролів користувачів, повідомивши при цьому:

- повне найменування клієнта (обов'язково);
- номер рахунку (якщо обслуговується декілька рахунків, то повідомляється рахунок, зазначений у Договорі та Анкеті-заяві);
- прізвище та ім'я особи, яка здійснює блокування;
- блокувальне слово (обов'язково);
- причину блокування.

Також Клієнту необхідно виконати позапланову зміну ключів ЕЦП.

Банк блокує роботу Клієнта в системі на основі отриманого телефонного повідомлення з вірно названим блокувальним словом.