АТ «КРИСТАЛБАНК»

Додаток 2
до Публічної пропозиції АТ «КРИСТАЛБАНК»
на укладання договору комплексного банківського
обслуговування юридичних та самозайнятих осіб

Вимоги Банку та рекомендації Клієнту щодо безпечної роботи з системою «Клієнт-Банк iFobs»/ CRYSTAL Business (далі – Система)

1. Негайно інформуйте Банк, звертаючись до відділення, де Ви обслуговуєтесь, щодо нештатних ситуацій або підозри на порушення безпеки робочого місця Системи, а саме:

1. в разі отримання SMS-повідомлення про платіж, який Ви не виконували (у випадку підключення такої послуги);
2. в разі виявлення у виписці за Вашим рахунком платіжних операцій, яких Ви не виконували;
3. якщо у Вас не працює Система з невідомих причин;
4. у випадку, навіть тимчасової, втрати контролю над ключовими носіями електронного підпису (далі – ЕП) та існування вірогідності того, що з носія особистого ключа ЕП може бути виготовлена копія (в разі використання удосконаленого ЕП з кваліфікованим сертифікатом (далі – УЕП) на незахищеному носії);
5. в разі будь-якої підозри, що ключ може бути скомпрометований;
6. у випадку несанкціонованого (коли Ви як керівник не контролювали таке використання) користування Системою з інших комп'ютерів (публічних бібліотек, Інтернет-кафе або з комп'ютера, до якого мають доступ інші співробітники підприємства (організації)).

2. Рекомендації щодо роботи з ключовими носіями електронного підпису:

1. Використовуйте захищені носії (токени) для зберігання особистих ключів ЕП.
2. В разі використання незахищеного носія:
   - використовуйте окремий, спеціально виділений змінний носій, попередньо відформатований та перевірений на відсутність вірусів;
   - не використовуйте ключовий носій для інших цілей (копіювання та/або зберігання файлів) окрім зберігання особистого ключа ЕП;
   - не робіть копію ключа ЕП.
3. Не зберігайте ключ ЕП на жорсткому диску комп'ютера.
4. Після генерації ключа ЕП уважно контролюйте місце зберігання носія.
5. Не передавайте нікому носій інформації з особистим ключем ЕП та пароль до нього, включаючи працівників Вашого підприємства (організації) – будь-який електронний документ, підписаний Вашим ЕП, вважається підписаним Вами особисто.
6. Підключайте ключовий носій з ЕП до комп'ютера лише на момент роботи з Системою, в усіх інших випадках, якщо Ви не працюєте в Системі, не залишайте ключовий носій підключеним до комп'ютера та зберігайте його в надійному, контрольованому місці.
7. Під час генерації особистого ключа використовуйте надійні паролі з дотриманням таких правил:
   - пароль має бути довжиною щонайменше 6 символів
   - пароль має містити великі та малі літери, спеціальні символи (!, -, ?, &, $ та інші) та цифр (1, 2, …9). При генерації нового ключа змінюйте пароль доступу до нього.

3. Завжди виконуйте перегенерацію (заміну) ключа ЕП у випадках:

1. виявлення вірусів на Вашому комп'ютері;
2. виявлення програм віддаленого доступу на Вашому комп'ютері;
3. виявлення змін у налаштуванні служб та засобів віддаленого управління Вашим комп'ютером.

4. Рекомендації щодо користування персональним комп'ютером, на якому встановлено Систему:

1. обмежте доступ працівників до комп'ютера, з якого виконуються платежі в Системі;
2. для роботи в Системі використовуйте окремий, призначений лише для роботи з цією системою комп'ютер;
3. використовуйте програмне забезпечення (далі – ПЗ), отримане лише з довірених джерел (ліцензійне ПЗ), відслідковуйте та своєчасно встановлюйте усі оновлення операційної системи, використовуйте актуальні версії антивірусного та системного ПЗ, Web-браузера, віртуальної Java-машини;
4. встановлюйте та використовуйте Систему лише після того, як будете впевнені, що
5. Ваш комп'ютер не заражений вірусами та на ньому відсутнє шкідливе ПЗ;
6. налаштовуйте систему антивірусного захисту на перевірку у режимі реального часу. Регулярно виконуйте оновлення антивірусного ПЗ;
7. категорично не рекомендується встановлення програм для дистанційного управління
8. (Microsoft Remote Assistant, Team Viewer, Radmin та ін.) на комп'ютері, на якому використовується Система;
9. категорично не рекомендується скачувати та встановлювати неперевірене ПЗ, відкривати неперевірені повідомлення та додатки до повідомлень (особливо від невідомих відправників);
10. встановіть персональний файрвол та налаштуйте його в максимально жорсткому режимі – на обмін лише з банківським сервером Системи;
11. регулярно тестуйте комп'ютер на відсутність вірусів та руйнівного ПЗ;
12. на комп'ютері не повинно бути облікових записів користувачів з пустими паролями. При створені паролю для облікового запису або ключа ЕП дотримуйтесь таких правил:
    - пароль має бути довжиною щонайменше 6 символів;
    - пароль має містити великі та малі літери, спеціальні символи (!, -, ?, &, $ та інші) та цифр (1, 2, …9);
13. не рекомендується працювати під технологічними обліковими записами, наприклад: Адміністратор, а також під обліковими записами, що мають права адміністратора.

5. Додаткові рекомендації - регулярно контролюйте рух коштів та залишки на Ваших рахунках.

!!! Пам'ятайте, що лише своєчасне звернення до Банку дозволить вжити негайні заходи щодо попередження шахрайства та повернення коштів, які були несанкціоновано списані з Вашого рахунку.

З рекомендаціями Банку, щодо безпечної роботи з Системою, ознайомлений і зобов'язуюсь їх виконувати.

Я розумію, що невиконання вищезазначених рекомендацій може потягти за собою несанкціоноване списання коштів з мого рахунку.