Правила інформаційної безпеки при використанні Клієнтом Системи дистанційного банківського обслуговування клієнтів IFOBS

З метою недопущення шахрайських дій відносно грошових коштів Клієнта при використанні Системи дистанційного банківського обслуговування клієнтів «IFOBS»(далі - Система), Клієнти повинні дотримуватися наступних заходів безпеки:

1. Уважно **вивчіть призначену для користувача документацію** по використанню Системи (доступна за посиланням https://ibank.*sbrf.com.ua/*ifobsClient в розділі «*Полезные ссылки»*).

2. **Не розголошуйте персональні дані**, які Ви використовуєте для роботи в Системі (Логін[1] і Пароль авторизації), стороннім особам, навіть у разі отримання по електронній пошті, телефону або через SMS- повідомлення, запиту від осіб, що представляються співробітниками Банку.

3. **Зберігайте ключі ЕЦП тільки на змінних носіях** (USB флеш накопичувач, токен, ін.), забезпечуйте їх збереження і не записуйте на змінні носії з ключем ЕЦП іншу інформацію. Не зберігайте Логіни і Пароль авторизації для доступу в Систему, ключі ЕЦП і паролі для їх накладення, на жорстких дисках персональних комп'ютерів (далі - ПК) або загальних мережевих ресурсах.

4. **Підключайте носій з ключем ЕЦП тільки на час підпису документів в Системі**. Негайно їх відключайте, після закінчення роботи з платіжними документами. Ні в якому разі **не залишайте носії з ЕЦП підключеними до ПК після здійснення операцій**.

5. На ПК, з яких здійснюється робота в Системі, **використайте тільки ліцензійні операційні системи і антивірусні програми**. **Регулярно**, не менше 1 разу на день, **оновлюйте вірусні бази**, і періодично, проводьте повну перевірку ПК на наявність вірусів і шпигунських програм. Також, **регулярно оновлюйте операційну систему (**в першу чергу це стосується оновлень безпеки). У разі виявлення будь-якого шкідливого програмного забезпечення (віруси, троянські програми тощо) на ПК, з якого здійснювався вхід в Систему, обов'язково здійсніть вхід в Систему з гарантовано незараженого ПК і змініть пароль доступу до Системи.

6. При повсякденній роботі на ПК **не використовуйте обліковий запис з правами локального адміністратора (**використайте призначений для користувача обліковий запис).

7. **Встановіть на ПК**, який використовується для роботи з Системою, **спеціальне програмне забезпечення (міжмережевий екран/брандмауер)** для унеможливлення зовнішнього підключення зловмисників до комп'ютера. Утримуйтеся від використання цього ПК для розваг і інших неконтрольованих дій в мережі Інтернет, а також обмежте до нього фізичний і мережевий доступ сторонніх осіб.

8. **Періодично змінюйте пароль доступу до Системи**.

9. **Своєчасно оновлюйте клієнтське програмне забезпечення Системи (**періодично пропонується Системою, при Аутентифікації в Системі користувача).

10. **У випадках компрометації або підозри на компрометацію ключів ЕЦП** (копіювання, ознайомлення, крадіжка), звільнення співробітника, якому належав ключ ЕЦП, необхідно терміново повідомити Банк для виконання блокування ключів ЕЦП, провести процедуру генерування і

[1] За винятком випадків безпосереднього звернення у Банк за Вашою ініціативою (для надання технічної підтримки в телефонному режимі співробітник Банку може попросити назвати Логін для однозначної ідентифікації Клієнта).

реєстрації нових ключів ЕЦП в Системі з наданням у Банк оригіналів сертифікатів ЕЦП, завірених Вашим підписом.

11. **Перед початком роботи з Системою через WEB- інтерфейс** (модуль iFOBS.Web) і введенням персональних даних на сторінці авторизації, **переконаєтеся, що Ви знаходитеся саме на сторінці банку**: адреса починається з https://ibank.sbrf.com.ua/ifobsClient (частина адреси, що залишилася, залежно від типу підключення і використовуваного носія для зберігання ЕЦП).

Обов'язково перевірте, щоб адреса починалася з https, де буква «s» вказує на ознаку захищеного з'єднання.

Переконатися, що Ви на правильній сторінці, можна, перевіривши сертифікат, за допомогою якого здійснюється захищене з'єднання. Відмітка, що визначає захищене з'єднання, найчастіше виглядає як «замок». У вікні властивостей сертифікату, яке відкриється, Ви зможете переконатися, кому він був виданий. Правильний сертифікат міститиме інформацію: «Кому виданий: ibank.sbrf.com.ua». **Використовуйте для роботи з Системою останні версії веб-браузерів**.

12. **Не відкривайте сайт Системи за посиланнями: банерним або отриманим по електронній пошті** тощо. Для зручності використання, введіть адресу сайту Системи самостійно і додайте цю сторінку в закладки браузеру.

13. **Не використовуйте функцію «запам'ятовування пароля» веб-браузером** або іншим програмним забезпеченням, встановленим на ПК.

14. **По закінченню роботи з Системою, здійснюйте безпосередній вихід**, натиснувши відповідну кнопку «Вихід».

15. **Не використовуйте** для доступу до Системи ПК, встановлені в публічних місцях, **чужі комп'ютери**, ноутбуки, смартфони тощо.

Для підвищення безпеки при роботі з Системою Банк додатково пропонує:

- Використати захищені носії (токени) для зберігання ключів ЕЦП, які не дозволяють зловмисникам їх копіювати.
- Встановити обмеження на доступ до Системи тільки з визначених, вказаних Вами, IP- адрес.
- Організувати роботу в Системі з використанням 2-х рук(підписання проводок 2-ма особами).

Для підключення вищезгаданих додаткових опцій Вам необхідно звернутися до персонального менеджера.