1. Уважно вивчіть призначену для користувача документацію з використання 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 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 КЕП тільки на змінних носіях (USB-флеш накопичувач, токен, ін.), забезпечуйте їх збереження і не записуйте на змінні носії з ключем КЕП іншу інформацію. Не зберігайте логіни і пароль авторизації для доступу в систему, ключі КЕП і паролі для їх накладення, на жорстких дисках персональних комп'ютерів (далі - ПК) або загальних мережевих ресурсах.
4. Підключайте носій з ключем КЕП тільки на час підпису документів у системі. Негайно їх відключайте, після закінчення роботи з платіжними документами. Ні в якому разі не залишайте носії з КЕП 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 до системи, обов'язково здійсніть вхід у систему з гарантовано незараженого ПК і змініть пароль доступу до системи.
6. У 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 та інших неконтрольованих дій у 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 у системі користувача).
10. У випадках компрометації або підозри на компрометацію ключів КЕП (копіювання, ознайомлення, крадіжка), звільнення співробітника, якому належав ключ КЕП, необхідно терміново повідомити Банк для виконання блокування ключів КЕП, провести процедуру генерування і реєстрації нових ключів КЕП у системі з наданням у Банк оригіналів сертифікатів КЕП, 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 КЕП).
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. Після закінчення 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.

Одразу звертайтесь до Банку в разі виявлення несанкціонованого доступу або зміни інформації Клієнта в системах дистанційного обслуговування.

Цілодобова клієнтська підтримка:
5595 (безкоштовно з мобільного), +380 (44) 354-15-15
+380 (50) 3 125 125 (чат) Viber/ Telegram
e-mail: sbrf@sbrf.com.ua