1. Внимательно изучите пользовательскую документацию по использованию системы (доступна по ссылке https://ibank.sbrf.com.ua/ifobsClient в разделе «Полезные ссылки»).
2. Не сообщайте персональные данные, которые вы используете для работы в системе (логин и пароль авторизации) посторонним лицам даже в случае получения по электронной почте, телефону или через SMS-сообщение запроса от лиц, представляемых сотрудниками Банка.
3. Храните ключи КЭП только на сменных носителях (USB-флэш накопитель, токен, др.), Обеспечивайте их сохранение и не записывайте на сменные носители с ключом КЭП другую информацию. Не храните логин и пароль авторизации для доступа в систему, ключи КЭП и пароли для их наложения на жестких дисках персональных компьютеров (далее - ПК) или общих сетевых ресурсах.
4. Подключайте носитель с ключом КЭП только на время подписи документов в системе. Немедленно их отключайте, после окончания работы с платежными документами. Ни в коем случае не оставляйте носители с КЭП подключенными к компьютеру после совершения операций.
5. На ПК, с которых осуществляется работа в системе, используйте только лицензионные операционные системы и антивирусные программы. Регулярно, не реже 1 раза в день, обновляйте вирусные базы и периодически проводите полную проверку компьютера на наличие вирусов и шпионских программ. Также регулярно обновляйте операционную систему (в первую очередь это касается обновлений безопасности). В случае выявления любого вредоносного программного обеспечения (вирусы, троянские программы и т.д.) на ПК, с которого осуществлялся вход в систему, обязательно выполните вход в систему с гарантированно незараженного ПК и смените пароль доступа к системе.
6. В повседневной работе на ПК не используйте учетную запись с правами локального администратора (используйте пользовательский акаунт).
7. Установите на ПК, который используется для работы с системой, специальное программное обеспечение (межсетевой экран / брандмауэр) для предотвращения внешнего подключения злоумышленников к компьютеру. Воздержитесь от использования этого ПК для развлечений и других неконтролируемых действий в сети Интернет, а также ограничьте к нему физический и сетевой доступ посторонних лиц.
8. Периодически меняйте пароль доступа к системе.
9. Своевременно обновляйте клиентское программное обеспечение системы (периодически предлагается системой, при аутентификации в системе пользователя).
10. В случаях компрометации или подозрения на компрометацию ключей КЭП (копирование, ознакомления, кража), увольнение сотрудника, которому принадлежал ключ КЭП, необходимо срочно сообщить Банк для выполнения блокировки ключей КЭП, провести процедуру генерации и регистрации новых ключей КЭП в системе с предоставлением в Банк оригиналов сертификатов КЭП, заверенных вашей подписью.
11. Перед началом работы с системой через WEB- интерфейс (модуль iFOBS.Web) и введением персональных данных на странице авторизации, убедитесь, что вы находитесь именно на странице Банка: адрес начинается с https://ibank.sbrf.com.ua/ifobsClient (часть адреса, оставшаяся в зависимости от типа подключения и используемого носителя для хранения КЭП).
Обязательно проверьте, чтобы адрес начинался с https, где буква «s» указывает на признак защищенного соединения.
Убедиться, что вы находитесь на правильной странице, можно проверив сертификат, с помощью которого осуществляется защищенное соединение. Отметка, определяющая защищенное соединение, чаще всего выглядит как «замок». В окне свойств сертификата, которое откроется, вы сможете убедиться кому он был выдан. Правильный сертификат должен содержать информацию: «Кому выдан ibank.sbrf.com.ua». Используйте для работы с системой последние версии веб-браузеров.
12. Не открывайте сайт системы по ссылкам: баннерным или полученным по электронной почте и так далее. Для удобства использования введите адрес сайта системы самостоятельно и добавьте эту страницу в закладки браузера.
13. Не используйте функцию «запоминания пароля» веб-браузером или другим программным обеспечением, установленным на ПК.

14. По окончании работы с системой осуществляйте непосредственный выход, нажав соответствующую кнопку «Выход».
15. Не используйте для доступа к системе ПК, установленные в публичных местах, чужие компьютеры, ноутбуки, смартфоны и тому подобное.

Сразу обращайтесь в Банк в случае обнаружения несанкционированного доступа или изменения информации Клиента в системах дистанционного обслуживания.

Круглосуточная клиентская поддержка:
5595 (бесплатно с мобильного), +380 (44) 354-15-15 + 380 (50) 3 125 125 (чат) Viber / Telegram
e-mail: sbrf@sbrf.com.ua