Правила информационной безопасности при использовании Клиентом Системы дистанционного банковского обслуживания клиентов IFOBS

С целью недопущения мошеннических действий в отношении денежных средств Клиента при использовании Системы дистанционного банковского обслуживания клиентов «IFOBS» (далее – Система) должны соблюдаться следующие меры безопасности:

1. Внимательно **изучите пользовательскую документацию** по использованию Системы (доступна по ссылке https://ibank.sbrf.com.ua/ifobsClient в разделе *Полезные ссылки*).

2. **Не разглашайте персональные данные**, используемые Вами для работы в Системе (логин[1] и пароль), посторонним лицам, даже получив по электронной почте, телефону или через SMS-сообщения запрос от лиц, представляющихся сотрудниками Банка.

3. **Храните ключи ЭЦП только на сменных носителях** (USB-токен, USB-флэш накопитель, токен, пр.), обеспечивайте их сохранность и не записывайте на сменные носители с ключом ЭЦП другую информацию. Не храните логины и пароли для доступа в Систему, ключи ЭЦП и пароли для их наложения на жестких дисках персональных компьютеров (далее – ПК) или общих сетевых ресурсах.

4. **Подключайте носитель с ключом ЭЦП только на время подписи документов в Системе**, немедленно их отключайте после окончания работы с платёжными документами. Ни в коем случае **не оставляйте носители с ЭЦП подключенными к ПК после осуществления операций**.

5. На ПК, с которых осуществляется работа в Системе, **используйте только лицензионные операционные системы и антивирусные программы. Регулярно**, не менее 1 раза в день, **обновляйте вирусные базы**, и периодически проводите полную проверку ПК на наличие вирусов и шпионских программ. Также **регулярно обновляйте операционную систему** (в первую очередь это касается обновлений безопасности). В случае обнаружения любого вредоносного программного обеспечения (вирусы, троянские программы и т.д.) на ПК, с которого осуществлялся вход в Систему, обязательно осуществите вход в Систему с гарантированно незараженного ПК и смените пароль доступа к Системе.

6. При повседневной работе на ПК **не используйте учетную запись с правами локального администратора** (используйте пользовательскую учетную запись).

7. **Установите на ПК**, который используется для работы с Системой, **специальное программное обеспечение (межсетевой экран/брандмауэр)** для исключения возможности внешнего подключения злоумышленников к компьютеру. Воздерживайтесь от использования этого ПК для развлечений и подключений к другим ресурсам сети Интернет, ограничьте к нему физический и сетевой доступ посторонних лиц. Данный ПК рекомендуется использовать только для работы в Системе.

8. **Периодически изменяйте пароль доступа в Систему**.

9. **Своевременно обновляйте клиентское программное обеспечение Системы** (периодически предлагается Системой при аутентификации пользователя).

10. **В случаях компрометации или подозрения на компрометацию ключей ЭЦП** (копирование, ознакомление, кража), увольнения сотрудника, которому принадлежал ключ ЭЦП, необходимо срочно сообщить в Банк для выполнения блокировки ключей ЭЦП, провести процедуру генерирования и регистрации новых ключей ЭЦП в Системе с предоставлением в Банк оригиналов сертификатов ЭЦП, заверенных Вашей подписью.

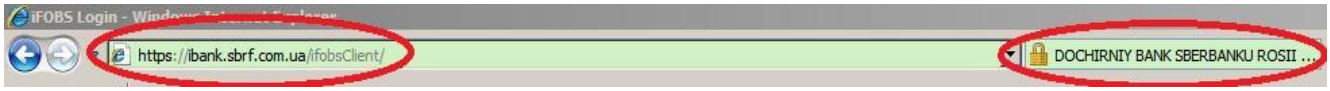
---

[1] За исключением случаев непосредственного обращения в Банк по Вашей инициативе (для оказания технической поддержки в телефонном режиме сотрудник банка может попросить назвать логин для однозначной идентификации клиента).

11. **Перед началом работы с Системой через WEB-интерфейс** (модуль iFOBS.Web) и вводом персональных данных на странице авторизации **убедитесь, что Вы находитесь именно на странице банка**: адрес начинается с https://ibank.sbrf.com.ua/ifobsClient (оставшаяся часть адреса в зависимости от типа подключения и используемого носителя для хранения ЭЦП).

Обязательно проверьте, чтобы адрес начинался с https, где буква «s» указывает на признак защищенного соединения.

Убедиться, что Вы 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, который откроется, Вы сможете убедиться, кому он был выдан. Правильный сертификат будет содержать информацию: «Кому выдан: ibank.sbrf.com.ua». **Используйте для работы с Системой последние версии веб-браузеров**. **Фон адресной строки должен отображаться зеленым** и содержать название организации: «DOCHIRNIY BANK SBERBANKU ROSII PAT».



12. **Не открывайте сайт Системы по ссылкам: баннерным или полученным по электронной почте** и т.п. 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 окончанию 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 т.п.

Для повышения безопасности при работе с Системой Банк дополнительно предлагает:

- Использовать защищенные носители (токены) для хранения ключей ЭЦП, которые не позволяют злоумышленникам их копировать.
- Установить ограничение на доступ к Системе только с определенных, указанных Вами, IP-адресов.
- Организовать работу в Системе с использованием 2-х рук (подписание проводок 2-мя лицами).
- Подключить услугу SMS-информирования о движениях по счетах.

Для подключения вышеуказанных дополнительных опций Вам необходимо обратиться к персональному менеджеру.