



Уважаемые клиенты АКБ «ФОРА-БАНК» (АО), напоминаем Вам о необходимости соблюдать правила безопасности при использовании системы ДБО «BS-Client»:

- Для доступа к системе ДБО необходимо использовать выделенный (не используемый для иных целей) компьютер. Ограничьте круг лиц, имеющих доступ к компьютеру.

- Работу с системой ДБО необходимо проводить с использованием учетных записей, не имеющих административные привилегии в операционной системе.

- Используйте на компьютере только лицензионное программное обеспечение (ПО).

ПОМНИТЕ, помимо того, что Вы несете уголовную ответственность за пользование нелегальным программным обеспечением в соответствии со статьей 146 УК РФ, использование подобного программного обеспечения может нанести вред Вашему компьютеру.

- Используйте лицензионное антивирусное программное обеспечение на компьютере, с которого осуществляется доступ к системе ДБО.

- Регулярно производите установку обновлений операционной системы, обновляйте антивирусные базы и антивирусное программное обеспечение, прикладное ПО. Производите обновление только из доверенных источников, гарантирующих отсутствие вредоносных программ и целостность получаемых файлов обновлений.

- Регулярно (не реже 1 раза в неделю) проводите полную антивирусную проверку компьютера на наличие вирусов.

- Используйте межсетевой экран (брандмауэр, firewall), разрешающий доступ с компьютера только к системе ДБО Банка.

- Не устанавливайте на компьютер, который используется для взаимодействия с системой ДБО, постороннее программное обеспечение (например, программы автоматического переключения раскладки клавиатуры, различные дополнения к браузерам и т.п.).

- Не подключайте к компьютеру непроверенные на наличие вирусов внешние носители (USB-флеш-накопители, внешние жесткие магнитные диски, ...).

- Никогда не записывайте логины и пароли на бумаге, мониторе или клавиатуре, не сохраняйте логины и пароли в файлах на компьютере. При составлении пароля используйте прописные и строчные буквы, цифры, а также различные символы (например: ! / { } [] < >). **Регулярно** (не реже 1 раза в 3 месяца) проводите смену паролей.

- Перед вводом своего пароля убедитесь, что Вы установили соединение с легальным сайтом. Проверьте правильность указания адреса сайта <https://dbo.forabank.ru/>, наличие сертификата безопасности. В случае обнаружения подозрительных web-сайтов, доменные имена (адреса) и стиль оформления которых сходны с именами и оформлением официальных сайтов АКБ «ФОРА-БАНК» (АО), незамедлительно сообщите об этом в Банк.

- Не сообщайте посторонним лицам, а также кому бы то ни было, логины и пароли доступа к компьютеру, с которого осуществляется подключение к системе ДБО, логины и пароли доступа к системе ДБО, историю операций, контактные и учетные данные, так как эти данные могут быть перехвачены злоумышленниками и использованы для получения доступа к Вашим счетам.

- Присоединяйте USB-носитель с секретными ключами к компьютеру непосредственно перед началом работы с системой ДБО, по окончании работы извлекайте USB-носитель из компьютера.

- USB-носитель с секретными ключами необходимо тщательно оберегать от несанкционированного доступа. Не оставляйте USB-носитель без присмотра. Не храните USB-носитель в местах, где к нему может получить доступ кто-либо кроме Вас.

- При увольнении ответственного сотрудника, имевшего доступ к секретным ключам, сообщите об этом в Банк и проведите смену ключей.

- При возникновении любых подозрений на компрометацию секретных ключей или компрометацию среды исполнения (наличие в компьютере вредоносных программ) обязательно сообщите об этом в Банк и заблокируйте ключи.

- Не позволяйте третьим лицам производить за Вас генерацию секретных ключей.

- Если Вы получили на электронную почту письмо, содержащее просьбу обновить или предоставить какую-либо информацию со ссылкой на какой-либо сайт или телефон (в том числе – сайт Банка), перезвоните в Службу технической поддержки по телефону +7 (495) 775-65-55 доб.1220, 1232, 1255 или +7 (499) 245-44-79 и сообщите о письме.

ПОМНИТЕ, Банк никогда не просит передать конфиденциальные данные по электронной почте. Банк никогда не просит провести тестовые переводы в системе ДБО.

- При обнаружении подозрительных действий на компьютере, с которого осуществляется подключение к системе ДБО (компьютер не включается, нет доступа к системе ДБО, наличие на сайте информации о проведении технических работ, замедление работы компьютера, самопроизвольное движение мышки по экрану, ...), необходимо извлечь USB-носитель с секретными ключами из компьютера и незамедлительно сообщить о данном факте в Банк.

- При обнаружении несанкционированных действий со средствами, находящимися на Ваших счетах, необходимо незамедлительно сообщить о данном факте в Банк.