Свой Банк

Меры безопасности при работе с системой «Клиент-Банк»

- Используйте USB токен для хранения ключа ЭЦП. Использование USB токена значительно повышает сохранность информации.
- Заведите в системе «Клиент-Банк» пользователя, отличного от системного. Задайте для этого пользователя пароль.
- Заведите пароль на доступ к контейнеру ключа ЭЦП.
- Ни при каких условиях не сообщайте информацию о ваших паролях никому, включая сотрудников Банка, родственников и иных третьих лиц.
- Ни в коем случае не сохраняйте информацию о ваших паролях на любых носителях, включая компьютер.
- Периодическая заменяйте пароли на доступ к системе ДБО и контейнеру ключа ЭЦП (например, в случае увольнения сотрудника, имевшего доступ к системе ДБО)
- Запрещается хранить ключи ЭЦП на жестком диске компьютера. Храните ключи ЭЦП только на USB токене и флеш-носителях в недоступном для посторонних месте (сейфы, закрываемые ящики).
- Ограничьте доступ сотрудников и посторонних лиц к носителям ключей ЭЦП и компьютерам с установленными системами ДБО.
- Осуществляйте контроль за отправляемыми платежными документами при работе с системой ДБО.
- После окончания работы в системе ДБО обязательно закройте окно системы и извлеките из компьютера USB токен или другой носитель, на котором хранится ключ ЭЦП.
- Убедитесь, что ваш компьютер не заражен вирусами. Установите и активизируйте антивирусное ПО. Регулярно обновляйте антивирусные базы.
- Используйте лицензионное программное обеспечение из проверенных и надежных источников. Выполняйте регулярные обновления операционной системы и прикладного программного обеспечения (браузер, программы для работы с документами и т.д.).
- При обнаружении попыток несанкционированного доступа или в случае мотивированных опасений, что такие попытки могут быть осуществлены, а также в случае компрометации ключей ЭЦП, незамедлительно сообщите об этом в Банк.

При возникновении вопросов обращаетесь в службу поддержки клиентов:

- тел.: 8 800 101 03 03
- email: info@svoi.ru