

Памятка по обеспечению безопасности при использовании Системы ДБО

Для безопасной работы в сервисе придерживайтесь следующих правил:

- ☑ Храните носители ключей (смарт-ключи, USB-флеш, CD) в месте, недоступном посторонним лицам. Исключите хранение ключей на жёстком диске, в сетевых каталогах и прочих общедоступных ресурсах, либо используйте крипто-контейнеры.
- ☑ Подключайте ключевой носитель к компьютеру только на время подписи документов. Не держите ключевые носители постоянно подключенными к компьютеру.
- ☑ Храните в тайне пароль доступа к ключу, исключите запись пароля на стикерах, носителях ключей и т.п., никому не сообщайте пароль по телефону, даже сотрудникам банка.
- ☑ Меняйте пароль для доступа в систему ДБО не реже одного раза в три месяца.
- ☑ Подключите email или SMS/PUSH-уведомления об отправке платежей и при обнаружении подозрительных операций незамедлительно обращайтесь в банк!
- ☑ Используйте встроенные средства блокировки и разблокировки мобильного телефона (логин/пароль для входа в ОС, логин/PIN-код/отпечаток пальца).

Соблюдайте общие правила безопасности, применяющиеся для защиты данных, хранящихся на компьютерах:

- ☑ Используйте только доверенные компьютеры с лицензионными программами, установленным антивирусом. Регулярно проверяйте компьютер на вирусы, обновляйте операционную систему, браузеры и антивирусные базы.
- ☑ При работе с электронной почтой не открывайте письма, полученные от неизвестных отправителей, и вложения к ним, не переходите по ссылкам из таких писем.
- ☑ Не используйте права администратора без крайней необходимости. В повседневной практике входите в систему, как пользователь без прав администратора.
- ☑ При работе в Интернет не соглашайтесь на установку дополнительных программ. По возможности используйте выделенный компьютер только для работы с Интернет-банком.
- ☑ Не сохраняйте логин и пароль на общедоступных компьютерах/терминалах.
- ☑ Храните в тайне номер банковской карты, срок ее действия, CVV/CVC/batch коды.