Памятка пользователю системы ДБО

Уважаемые Клиенты!

В целях предотвращения несанкционированного доступа к Вашим средствам со стороны злоумышленников и компрометации Вашей ключевой информации рекомендуем Вам соблюдать **следующие меры предосторожности** при использовании систем ДБО:

1. В качестве места хранения ключевой информации используйте только отчуждаемые носители (съемные USB-носители). Использование в качестве места хранения ключевой информации реестра или жесткого диска компьютера резко увеличивает риск компрометации ключевой информации.
2. Ключевой носитель информации должен быть подключен к компьютеру только во время работы с системой ДБО. В остальное время ключевой носитель информации должен храниться в месте, где доступ посторонних лиц к нему исключен.
3. Рекомендуется оформлять право второй подписи, например, на главного бухгалтера предприятия. В этом случае для совершения операций с Вашим счетом через систему ДБО потребуется наличие двух подписей под электронным платежным документом, что снижает риск неправомерных операций.
4. Своевременно обновляйте операционную систему и используемое для работы в сети Интернет программное обеспечение (браузеры - Explorer, Opera, Firefox; почтовые клиенты - Outlook, The Bat, Thunderbird и т.д.).
5. Установите на компьютере и регулярно обновляйте лицензионное антивирусное программное обеспечение (Антивирус Касперского, Norton Antivirus, Avast и прочее).
6. Антивирусное программное обеспечение должно быть запущено постоянно с момента загрузки компьютера. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов.
7. При работе с электронной почтой не открывайте письма и прикрепленные к ним файлы, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.
8. Используйте сетевые экраны (firewall), разрешив доступ только к доверенным ресурсам сети Интернет и только для доверенных приложений.
9. При работе в Интернет не соглашайтесь на установку каких-либо дополнительных программ с неизвестных Вам сайтов.
10. На компьютере, используемом для работы в системе ДБО, не должно быть учетных записей (пользователей) с пустыми паролями. Выбирая пароль для учетной записи, постарайтесь сделать его сложным.
11. Система ДБО не должна запрашивать отдельный ввод ключевых данных для "проверки" и других несвойственных функций. В случае подозрений на нештатное поведение системы ДБО обратитесь за консультацией к сотрудникам службы поддержки клиентов Банка.
12. Осуществляйте информационное взаимодействие с Банком только с использованием средств связи (стационарные телефоны, интерактивные Web-сайты/порталы, электронная почта), реквизиты которых оговорены в документах, получаемых непосредственно в Банке.
13. В случае компрометации или подозрения на компрометацию следует немедленно произвести замену ключевой информации. В качестве события, рассматриваемого как компрометация ключа, может выступать не только хищение ключевой

информации, но и потеря ключевого носителя (даже с последующим обнаружением), увольнение или смена лиц, допущенных к ключевой информации.

Обращаем Ваше внимание, что в случае использования системы ДБО с публичных компьютеров (библиотека, Интернет-кафе) риск хищения и последующего неправомерного использования ключевой информации значительно возрастает.

Просим Вас незамедлительно обращаться в Банк при возникновении следующих ситуаций:

- В выписке обнаружены несанкционированные Вами расходные операции.
- Утерян или похищен носитель ключевой информации или компьютер, на котором была установлена система ДБО.
- У Вас не работает система ДБО по неизвестным причинам.

Телефон контакт-центра:
8-800-700-3000

Обращаем Ваше внимание, что соблюдение указанных правил и своевременное обращение в Банк при угрозе потери конфиденциальности Ваших ключей помогут существенно снизить угрозу мошенничества с Вашими средствами с использованием систем ДБО.