П А М Я Т К А
О МЕРАХ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ СИСТЕМЫ ДБО

Для исключения несанкционированного доступа в Систему дистанционного банковского обслуживания КБ «Геобанк» (ООО) просим Вас внимательно ознакомиться с Памяткой о мерах безопасного использования Системы ДБО. Соблюдение нижеизложенных рекомендаций позволит обеспечить максимальную безопасность и контроль доступа к Вашим счетам, а также снизит возможные риски при совершении банковских операций через сеть Интернет.

Выделите отдельное рабочее место (компьютер) для работы в Системе ДБО. Определите порядок доступа сотрудников к выделенному компьютеру. Введите ограничения по обмену информацией по электронной почте с выделенного компьютера.

Используйте только лицензионное программное обеспечение и регулярно выполняйте его обновления, в особенности, приложения безопасности. Установите на свой компьютер антивирусное программное обеспечение и регулярно производите его обновление.

С целью контроля исходящего и входящего подозрительного трафика выделенный компьютер должен быть защищен от внешнего доступа программным или аппаратным средством межсетевого экранирования. Программные межсетевые экраны должны пресекать отправку в Интернет информации, инициированной программами, не имеющими соответствующих полномочий.

Для функционирования USB-ключа необходимо выполнить перечисленные ниже действия. Установить выданного Банком диска драйвер устройства или скачать драйвер с сайта Банка для Вашей операционной системы. Ссылка для скачивания: ***http://www.geobank.ru/DRVISB*.**

При первоначальном подключении USB-ключа к компьютеру Система предложит изменить пароль. Необходимо **ОБЯЗАТЕЛЬНО** произвести смену пароля **- работа с паролем «по умолчанию» не допускается!!!**

Пароль необходимо регулярно изменять (не реже 1 раза в три месяца). Длина пароля должна быть не менее 8 символов. Пароль должен состоять из цифр, больших и маленьких букв английского алфавита. Использование простых и легко угадываемых паролей (например, имена, фамилии, номера телефонов, даты рождения и т.п.) должно быть исключено.

Важно!

Количество попыток введения пароля ограничено: при вводе неверного пароля более 15 раз устройство будет заблокировано!

Никогда ни при каких обстоятельствах не передавайте средства доступа к Системе ДБО (логин, пароль, USB-ключ) третьим лицам, в том числе родственникам.

При получении просьбы, в том числе со стороны сотрудника Банка, о сообщении информации о средствах доступа к Системе ДБО, не сообщайте их. Всегда сообщайте в Банк о подобных фактах. Не отправляйте информацию о средствах доступа к Системе ДБО средствами SMS, почтой или электронной почтой. Помните, Банк, ни при каких условиях, не вправе потребовать от Вас конфиденциальную информацию. Не следуйте по «ссылкам», указанным в письмах (включая ссылки на сайт Банка), т.к. они могут вести на сайты-двойники.

В целях информационного взаимодействия с Банком рекомендуется использовать только реквизиты средств связи (мобильных и стационарных телефонов, факсов, интерактивных web-сайтов/порталов, обычной и электронной почты и пр.), которые указаны в документах, полученных непосредственно в Банке.

Избегайте работы с Системой в публичной среде, такой, как интернет-кафе, социальные точки доступа в интернет, компьютеры друзей и тому подобное.

После завершения работы с Системой ДБО, осуществляйте выход из системы, выбрав пункт меню «Выйти из системы» и всегда отключайте USB-ключ от компьютера по завершению работы с Системой.

В случае если имеются предположения об использовании средств доступа к Системе ДБО третьими лицами, позволяющими совершить неправомерные действия с Вашим банковским счетом, необходимо немедленно обратиться в Банк и следовать указаниям сотрудника Банка.

Рекомендуем Вам всегда иметь при себе контактные телефоны Банка на различных носителях информации: в записной книжке, мобильном телефоне и/или других носителях информации.

Для блокировки доступа в Систему ДБО Вы можете обратиться по телефонам:
+7 (495) 737-32-93 (круглосуточно)
+7 (495) 221-33-41 (по рабочим дням с 9-00 до 18-00)

Для получения дополнительной информации по техническим вопросам Вы можете ежедневно по рабочим дням с 9-00 до 18-00 обратиться:
Служба технической поддержки: (495) 221-33-41 доб.47-56, 47-13
По организационным вопросам: (495) 221-33-41 доб.47-22

Справочная информация:

Что такое *USB-ключ*?

USB-ключ - персональное средство аутентификации и хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной подписью.

Основное назначение:

Строгая двухфакторная аутентификация пользователей при доступе к защищенным ресурсам (компьютерам, сетям, приложениям);

Безопасное хранение ключа электронной подписи;

Аппаратное выполнение криптографических операций в доверенной среде (генерация ключей шифрования, формирование ЭП).

USB-ключ используется в Системе ДБО для усиления защиты. Ключ электронной подписи размещен в неизвлекаемой области памяти USB-ключа и устройство будет использовать ключ только внутри себя. Чтобы использовать это преимущество, всегда отключайте устройство от компьютера по завершению работы с системой.

USB-ключ обеспечивает:

- строгую аутентификацию пользователя за счет использования криптографических методов;
- безопасное хранение ключей электронной подписи для доступа к защищенным корпоративным сетям и информационным ресурсам;
- безопасное использование - воспользоваться USB-ключом может только его владелец, ключ электронной подписи генерируется аппаратно и не может быть перехвачен;
- удобство работы - ключ выполнен в виде брелка и напрямую подключается к USB-портам, не требует специальных устройств для считывания.