Памятка ОАО КБ «ИВАНОВО»
о мерах безопасного использования дистанционного банковского обслуживания для юридических лиц.

Защита устройства (персональный компьютер, ноутбук, планшет, смартфон и т.д.) с помощью которого осуществляется доступ к системе подключение к системе ДБО.

- Ограничьте доступ посторонних лиц к устройству, с которого осуществляется подключение к системе ДБО.
- Для повседневного использования создайте отдельную учетную запись с ограниченными правами пользователя.
- Установите пароли на учетные записи для входа в операционную систему.
- Используйте только лицензионное программное обеспечение.
- Установите себе решение для защиты от информационных угроз (антивирус, защита от шпионских программ, сетевой экран).
- Не реже раза в сутки должны проверятся и устанавливаться обновления операционной системы и решений для защиты от информационных угроз.
- Должна быть отключена возможность удаленно подключиться к устройству.
- Не посещайте интернет-сайты сомнительного содержания.
- Не устанавливайте программы, скачанные из не доверенных источников.
- Не открывайте неизвестные файлы и ссылки, присланные по e-mail, соц. сетям и службам сообщений.
- Не нажимайте на всплывающие окна.

Защита соединения с системой ДБО

- Рекомендуем вам использовать набор ip-адресов согласованный с тех. поддержкой ДБО. В этом случае доступ в вашу учетную запись с других ip-адресов будет не доступен.
- Не используйте для доступа к системе ДБО общедоступные сети (компьютерный клуб, интернет-кофе, WiFi в общественных местах и т.д.)
- Доступ в систему ДБО осуществляется с доменного имени kbivanovo.ru если доменное имя изменено хотя бы на символ, то прекратите и свяжитесь с тех. поддержкой ДБО

Защита ключей ЭП

- Ключи ЭП хранятся на отчуждаемом носителе, который подключается только на момент работы с системой ДБО.
- Носители с ключами ЭП в момент, когда не производится работы с системой ДБО, должны храниться в местах, защищенных от проникновения посторонних лиц.
- Рекомендуется хранить ключи ЭП на защищенных носителях информации – токенах.
- При любых подозрениях на компрометацию ключа ЭП, незамедлительно воспользуйтесь карточкой компрометации.
- При смене ответственного лица имевшего доступ к ключам ЭП, незамедлительно воспользуйтесь карточкой компрометации.

Парольная защита

- Никогда и никому не сообщайте свой пароль.

- Старайтесь запомнить свой пароль, а не записывать его тем более в легкодоступных местах.
- Поменяйте свой пароль после первого же входа в систему ДБО.
- Периодически меняйте свой пароль. Чем чаще вы это делаете, тем меньше вероятность компрометации вашего пароля.
- При формировании пароля используйте различные символы, цифры, буквы различного регистра.
- При вводе пароля убедитесь, что никто не имеет возможности его увидеть (в том числе при помощи зеркала, камер видеонаблюдения и т.д.).

Телефон технической поддержки (4932) 32-78-31