

### **Меры безопасности при работе с ЭП:**

- Храните ЭП в недоступном для посторонних лиц месте.
- В случае, если на клиента зарегистрировано две и более ЭП, желательно хранить каждую ЭП на отдельном отчуждаемом носителе, при этом не использовать данный носитель для других целей.
- Пароль доступа следует хранить отдельно от ЭП.
- Не осуществлять письменную запись ЭП и/или пароля на доступных другим лицам источниках (в записных книжках, в памяти телефона, на этикетке дискеты или диска и т.п.).
- В случае хранения ЭП и/или пароля на компьютере, обеспечить дополнительный контроль доступа к данному компьютеру (установить систему личных паролей для входа в компьютер для каждого пользователя).
- Закончив работу в Системе ДБО или прервав ее (даже на несколько минут), не забудьте вынуть внешний носитель из устройства чтения и убрать его в место, недоступное посторонним лицам.
- Придерживаться стандартных правил безопасности работы в интернете, таких как использование антивирусов, firewall-ов, и ограничение посещения подозрительных интернет — ресурсов.
- Не передавайте ЭП никому даже на короткое время.
- В случае, если носитель с ЭП утерян, или у Вас имеется подозрение, что ЭП оказалась у посторонних лиц, незамедлительно блокируйте технические средства, используемые для работы в системе ДБО и сообщите об этом факте в НКО любыми доступными из нижеперечисленных способами:
  - при Вашем личном обращении (Вашего представителя) в НКО
  - путем информирования сотрудников НКО по телефону: +7 (815-2) 607-494, 994-495.

В случае обращения в НКО по телефону и/или по адресу электронной почты Вам необходимо указать следующую информацию:

- Наименование Вашей организации;
  - Номер Счета Вашей организации;
  - Блокировочное слово;
  - Причину обращения в НКО.
- Заменяйте ключи ЭП во всех случаях увольнения или смены лиц, обладающих правом подписи или допущенных к этим ключам, а также руководителей, которые подписывали решения (доверенности) о допуске пользователей к ключам ЭП.
  - Срок действия ЭП составляет 2 года. Для замены Сертификата вам необходимо заблаговременно, до истечения срока действия текущей ЭП, сгенерировать новый ключ ЭП.
  - По возможности воздержитесь от использования системы Интернет-Банк в интернет кафе, а так же там, где вы не уверены в безопасности компьютеров.

### **Меры по защите компьютера, с которого осуществляется работа в Системе ДБО:**

- Доступ к компьютеру должны иметь только доверенные лица.
- Контролируйте действия сотрудников IT-подразделений при обслуживании компьютера, на котором установлена система.
- Должны быть установлены все обновления безопасности, рекомендуемые производителем операционной системы, установленной на компьютере.

- На компьютере должно быть установлено антивирусное программное обеспечение с **регулярно обновляемыми базами.**
- На компьютере должны запускаться программы, полученные из источников которым можно доверять (особую опасность могут представлять программы, полученные по электронной почте или из сети Интернет).
- Желательно установить на компьютер персональный Firewall.
- При необычном поведении программного обеспечения или работы системы обратитесь в техническое подразделение НКО за разъяснением. Данные изменения могут быть вызваны работой программы-шпиона. В этом случае необходимо заблокировать ЭП.

#### **Меры по противодействию мошенникам в интернете.**

- Не сообщать пароль даже если Вам пришло письмо с такой просьбой из НКО.
- Не вводить пароль заходя на сайт НКО с присланных по почте ссылок.
- Контролировать состояние отправленных в НКО ЭД. При обнаружении в системе ДБО несанкционированного ЭД, направленного от имени Вашей организации, незамедлительно связаться с сотрудниками НКО.