Приложение № 5

РЕКОМЕНДАЦИИ
Клиенту по обеспечению безопасности информации при использовании системы «Интернет Клиент-Банк»

1. **Рекомендации по защитным мерам для персональной электронной вычислительной машины (ПЭВМ)**

1) Для работы с системой «Клиент-Банк» рекомендуется использовать отдельный компьютер, доступ к которому имеют только уполномоченные Клиентом Владельцы АСП.

2) Средствами BIOS компьютера следует исключить возможность загрузки операционной системы, отличной от установленной на жестком диске, т.е. должна быть отключена возможность загрузки с дискет, CD/DVD приводов, USB-flash дисков, загрузка по сети и т.п.

3) Доступ к изменению настроек BIOS должен быть защищен паролем.

4) ПЭВМ с системой «Интернет-Клиент-Банк» по окончании рабочего дня рекомендуется выключать.

5) Не рекомендуется подключать к ПЭВМ с системой «Интернет-Клиент-Банк» внешние устройства, в том числе носители информации, не предусмотренные производственной необходимостью.

6) На компьютере, с которого осуществляется работа в системе «Интернет-Клиент-Банк», необходимо использовать только лицензионное системное и прикладное ПО.

7) Рекомендуется своевременно проводить обновления системного и прикладного ПО.

8) На ПЭВМ с системой «Интернет-Клиент-Банк» должна быть установлена только одна операционная система.

9) В обязательном порядке должно быть установлено и регулярно обновляться антивирусное ПО (отдавайте предпочтение российским разработчикам). Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т.е. не требующий ответов пользователя при обнаружении вирусов и другого вредоносного ПО.

10) Разработайте и утвердите перечень программного обеспечения, разрешенного для установки и используемого на ПЭВМ. Стандартизировав ПО на ваших ПЭВМ, Вы значительно уменьшите потенциальные уязвимости на ПЭВМ.

11) По возможности следует принять меры, препятствующие несанкционированному вскрытию системных блоков ПЭВМ с системой «Интернет-Клиент-Банк». (защитные наклейки, пломбы и т.п.).

12) Рекомендуется полностью блокировать сетевой доступ к ресурсам ПЭВМ с системой «Интернет-Клиент-Банк».

13) На ПЭВМ с системой «Интернет-Клиент-Банк» рекомендуется ограничить использование сети Интернет пользователями системы «Интернет-Клиент-Банк», т.е. ограничить список доступных для соединения адресов, например, разрешить только соединение с сервером системы «Интернет-Клиент-Банк».

Категорически запрещено:

a. посещать социальные сети (Например, ВКонтакте, Одноклассники и др.) и другие ресурсы, не связанные с должностными обязанностями работника;

b. устанавливать и использовать программы мгновенного обмена сообщениями (Например, ICQ, QIP, Mail.ru agent, Miranda);

c. устанавливать и использовать ПО для облачного хранения данных (Например, GoogleDisk, YandexDisk, DropBox, Mail cloud и др.);

d. устанавливать и использовать программы, обеспечивающие голосовую и видео связь (Skype, Viber, Microsoft Lync и т.п.);

ВАЖНО: Возможность подключения к личным почтовым ящикам, интернет системам обмена экспресс-сообщениями, а также сайтам социальных сетей должна быть исключена.

14) Пользователи системы «Интернет-Клиент-Банк», работающие с системой, не должны обладать правами администратора на ПЭВМ с системой «Интернет-Клиент-Банк» с целью ограничения возможностей установки под этими учетными записями программного обеспечения на ПЭВМ. Доступ к файловым ресурсам компьютера, особенно на запись, должен быть ограничен минимально необходимыми правами. Пользователи должны запускать только те приложения, которые им разрешены.

15) **ЗАПРЕЩЕНО**: устанавливать, запускать, использовать на ПЭВМ с системой «Интернет-Клиент-Банк» ПО для удаленного управления (Например, RDP, TeamViewer, Radmin, Ammyy Admin, др.).

16) Для доступа к системе «Интернет-Клиент-Банк» не используйте общедоступные компьютеры (например, установленные в интернет-кафе, гостинице).

2. Рекомендации по парольной защите

Учетные записи операционной системы и системы «Интернет-Клиент-Банк» должны быть защищены паролями с учётом следующих параметров:

1) Длина пароля должна быть не менее 8 символов.

2) В пароле обязательно должны присутствовать заглавные и прописные (верхнего и нижнего регистра) символы, цифры, а также специальные символы (например, #, %, ^, * и т.п.). Примеры паролей (hjf#48dFt, 5$ma(fQ5er, %deR*2fvw2).

3) В качестве пароля не следует использовать имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе.

4) В качестве пароля не следует использовать повторяющуюся комбинацию из нескольких символов либо комбинацию символов, набираемых в закономерном порядке;

5) Пароль должен меняться не реже 180 дней, а также при компрометации (или подозрении в компрометации) пароля.

6) При смене пароля новый пароль не должен совпадать с ранее используемыми паролями.

7) **Запрещено** произносить вслух, записывать и хранить в любом доступном посторонним лицам месте пароли доступа к ПЭВМ и системе «Интернет-Клиент-Банк» (например, на мониторе компьютера, под клавиатурой, на столе).

8) **Запрещено**: использовать стандартные пароли доступа к системе «Интернет-Клиент-Банк», т.е. те, которые назначены по умолчанию, они должны быть незамедлительно изменены.

9) Блокировать операционную систему в случае перерыва в работе с ПЭВМ одним из двух нижеприведенных способов:

- блокировать операционную систему (одновременно нажав клавиши Ctrl+Alt+Del) и далее в диалоговом окне нажать «блокировать компьютер»;
- блокировать операционную систему (одновременно нажав клавиши «Windows» + L).

10) После 6 неудачных попыток получения доступа к ПЭВМ с системой «Интернет-Клиент-Банк» учетная запись пользователя должна быть заблокирована на 30 минут или до момента разблокировки учетной записи соответствующим администратором.

11) Принудительно завершайте сессию работы с системой «Интернет Клиент-Банк» выходом из системы.

12) Не храните логин и пароль в мобильном телефоне, смартфоне.

13) При отсутствии активности работника на ПЭВМ после авторизации, в течение 15 минут сеанс работы должен быть заблокирован или завершен.

3. Рекомендации по эксплуатации внешнего ключевого носителя (Рутокен 2.0)

1) Для повышения уровня безопасности хранения ключей ЭП используйте устройства строгой аутентификации и хранения данных, такие как Рутокен 2.0, полученные в НКО для работы в системе «Интернет Клиент-Банк». Это позволяет существенно снизить вероятность хищения ключей ЭП злоумышленниками.

2) Для надежной защиты ключа ЭП на Рутокен 2.0 рекомендуется установить надежный пароль согласно рекомендациям раздела 2 настоящего приложения.

3) Порядок хранения и использования внешнего ключевого носителя с ключом ЭП должен исключать возможность несанкционированного доступа к ним.

4) Внешние ключевые носители должны храниться только у тех лиц, которым они принадлежат (Владельцы АСП).

5) Внешний ключевой носитель должен быть установлен в ПЭВМ с системой «Интернет-Клиент-Банк» только при входе в систему для Интернет-Клиент-Банка, в момент подписания и при получении информации из НКО.

6) По окончании рабочего дня, а также вне времени сеансов связи с системой «Интернет-Клиент-Банк» внешний ключевой носитель должен храниться в сейфе.

4. Рекомендации по работе с системой «Интернет-Клиент-Банк»

1) Вход в систему «Интернет-Клиент-Банк» осуществляйте только с официального web-сайта НКО в сети Интернет по адресу: https://altbank.com.

НКО никогда не помещает ссылки на страницу входа в систему «Интернет-Клиент-Банк» в исходящей корреспонденции Клиентам.

Не входите в систему «Интернет-Клиент-Банк» из источников в Интернете, т.к. мошенники часто фабрикуют фишинговые сайты (сайты-двойники) для хищения Вашей аутентификационной (логин, пароль) и, как следствие, финансовой информации. При обнаружении сайта-двойника немедленно сообщите об этом в службу технической поддержки НКО и перешлите ссылку, с которой осуществлялся вход на него, для проведения расследования специалистами НКО.

2) Обязательно контролируйте движение денежных средств по выписке, предоставляемой по системе «Интернет-Клиент-Банк».

3) Рекомендуется просматривать созданные и отправленные в течение дня ЭД в системе «Интернет-Клиент-Банк» на предмет отсутствия несанкционированных распоряжений на перевод денежных средств (платежных поручений). В случае обнаружения таких платежей незамедлительно обратитесь в НКО.

4) Незамедлительно заблокируйте Вашу учетную запись, если обнаружили операции, которые Вы не совершали, успешные или неуспешные попытки входа с неизвестных Вам IP-адресов или в необычное для Вас время суток.

5) Для получения рекомендаций по настройке параметров безопасности Вы можете обратиться в службу технической поддержки НКО.

5. Работа с сообщениями

1) Не отвечайте на сообщения, требующие предоставить, подтвердить или уточнить Вашу конфиденциальную информацию: пароли, логины, фамилию, имя, отчество, паспортные данные, номер мобильного телефона. НКО никогда не связывается по телефону и не осуществляет рассылок сообщений по SMS или e-mail с таким запросом.

2) Не открывайте подозрительные файлы, поступившие Вам по электронной почте. НКО никогда не рассылает программы в своих электронных письмах и не связывается с просьбой установить или обновить программное обеспечение.

3) Не отвечайте на полученное подозрительное сообщение от имени НКО и не переходите по ссылкам, указанным в сообщении.

ИКБ имеет возможность обеспечения дополнительной защиты путем привязки к IP либо MAC адресам Вашего компьютера, для включения этой возможности Вам необходимо вписать необходимые данные в Заявление на подключение к ИКБ либо, если ИКБ у Вас уже имеется, направить в НКО письмо с указанием таких адресов.