Приложение № 5

РЕКОМЕНДАЦИИ
Клиенту по обеспечению безопасности информации
при использовании «Сервиса AltBank»

1. **Рекомендации по защитным мерам для работы в «Сервисе AltBank»**

1) Для работы в «Сервисе AltBank» рекомендуется использовать отдельное техническое устройство, доступ к которому имеют только уполномоченные лица Клиента, которым принадлежат ключи ЭП. Необходимо исключить возможность подключения такого технического устройства к личным почтовым ящикам, интернет системам обмена экспресс-сообщениями, а также сайтам социальных сетей.

2) Использовать технические устройства в помещениях с ограниченным доступом во избежание хищения Смарт-ключей, используемых для работы в «Сервисе AltBank».

3) Размещать технические устройства способом, не позволяющим производить визуальное наблюдение за экраном технического устройства и его клавиатурой, в том числе посредством системы видеонаблюдения и через оконные проемы.

4) Не рекомендуется подключать к техническим устройствам, на которых осуществляется работа в «Сервисе AltBank», внешние устройства, в том числе носители информации, не предусмотренные производственной необходимостью.

5) 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.

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

7) На техническом устройстве, с которого осуществляется работа в «Сервисе AltBank», необходимо использовать только лицензионное системное и прикладное ПО.

8) Рекомендуется своевременно проводить обновления системного и прикладного ПО.

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) Техническое устройство, с которого осуществляется доступ в «Сервис AltBank», по окончании рабочего дня рекомендуется выключать.

11) Для доступа в «Сервис AltBank» не используйте общедоступные компьютеры (например, установленные в интернет-кафе, гостинице).

2. Рекомендации по парольной защите

1) Длина пароля должна быть не менее 8 символов.

2) В пароле обязательно должны присутствовать заглавные и прописные (верхнего и нижнего регистра) буквы, 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 каждых 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) Не передавать Логин и Пароль одного Уполномоченного лица другому Уполномоченному лицу Клиента или иным лицам.

8) **Запрещено** произносить вслух, записывать и хранить в любом доступном посторонним лицам месте Пароли доступа в «Сервис AltBank» (например, на мониторе компьютера, под клавиатурой, на столе).

9) **Запрещено**: использовать временные пароли доступа в «Сервис AltBank», т.е. те, которые назначены по умолчанию, они должны быть незамедлительно изменены.

3. Рекомендации по эксплуатации и хранению Смарт-ключа

1) Смарт-ключ использовать только Уполномоченным лицом Клиента, которому принадлежит ключ ЭП, содержащийся на данном Смарт-ключе.

2) При первом использовании Смарт-ключа сменить установленные по умолчанию PIN-коды администратора и пользователя. Информация об управлении PIN-кодами Рутокена размещена в информационно-телекоммуникационной сети «Интернет» по адресу: https://dev.rutoken.ru/pages/viewpage.action?pageId=72451342

3) Не передавать Смарт-ключ одного Уполномоченного лица другому Уполномоченному лицу Клиента и иным лицам.

4) Хранить Смарт-ключи раздельно, в защищенном от несанкционированного доступа месте.

5) Не устанавливать Смарт-ключи в компьютеры, ноутбуки и иные устройства, не используемые для работы в «Сервисе AltBank».

6) Не оставлять Смарт-ключи установленными в технических устройствах после завершения сеанса работы в «Сервисе AltBank».

7) В нерабочее время хранить Смарт-ключи в сейфе (в железном или ином шкафу с прочными дверями и надежным замком). На двери сейфа (шкафа) необходимо предусмотреть возможность опечатывания для предотвращения несанкционированного вскрытия.

4. Рекомендации по работе в «Сервисе AltBank»

1) Вход в «Сервис AltBank» осуществляйте только с официального сайта РНКО в информационно-телекоммуникационной сети «Интернет» по адресу: https://altbank.com или непосредственно по адресу: https://dbo.altbank.ru.

РНКО никогда не помещает ссылки на страницу входа в «Сервис AltBank» в исходящей корреспонденции Клиентам.

Не входите в «Сервис AltBank» из источников в Интернете, т.к. мошенники часто фабрикуют фишинговые сайты (сайты-двойники). При обнаружении сайта-двойника немедленно сообщите об этом в службу технической поддержки РНКО и перешлите ссылку, с которой осуществлялся вход на него, для проведения расследования специалистами РНКО.

2) Обязательно контролируйте движение денежных средств по выписке, предоставляемой в «Сервисе AltBank».

3) Рекомендуется просматривать созданные и отправленные в течение дня ЭД/Простые ЭД в «Сервисе AltBank» на предмет отсутствия несанкционированных распоряжений на перевод денежных средств (платежных поручений). В случае обнаружения таких платежей незамедлительно обратитесь в РНКО.

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 РНКО.

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. РНКО 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. РНКО 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 РНКО и не переходите по ссылкам, указанным в сообщении.

«Сервис AltBank» имеет возможность обеспечения дополнительной защиты путем привязки к IP либо MAC адресам Вашего технического устройства, для включения этой возможности Вам необходимо вписать необходимые данные в Заявление на предоставление прав доступа уполномоченному лицу Клиента в «Сервисе AltBank» (Приложение № 2).