РЕКОМЕНДАЦИИ
Клиенту по обеспечению безопасности информации при эксплуатации системы защиты информации

1. Рекомендации по организационному обеспечению безопасности систем защиты информации (далее - СЗИ):
   - в организации Клиента выделяются (определяются) должностные лица, ответственные за обеспечение безопасности информации и эксплуатации СЗИ;
   - в организации Клиента разрабатываются нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации СЗИ;
   - к работе с СЗИ допускаются сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации СЗИ.
2. Рекомендации по размещению СЗИ и режиму охраны:
   - помещения, в которых размещаются технические средства клиентского рабочего места со встроенными СЗИ, являются режимными и должны обеспечивать конфиденциальность проводимых работ;
   - размещение режимных помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств;
   - размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности;
   - входные двери режимных помещений должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время;
   - окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией;
   - размещение технических средств в режимном помещении должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых она отражается, через окна;
   - в режимные помещения допускаются руководители организации Клиента, сотрудники подразделения безопасности и исполнители, имеющие прямое отношение к обработке, передаче и приему конфиденциальных документов;
   - системные блоки компьютеров с СЗИ оборудуются средствами контроля вскрытия;
   - ремонт и/или последующее использование системных блоков осуществляется после удаления с них программного обеспечения СЗИ.
3. Рекомендации по обеспечению безопасности ключевой информации:
   - ключевые носители в организации Клиента берутся на поэкземплярный учет в выделенных для этих целей журналах;
   - учет и хранение ключей поручается руководством Клиента специально выделенным сотрудникам;
   - для хранения ключевых носителей выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации;
   - хранение ключей и дистрибутива клиентской части ИКБ с СЗИ допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное применение, не предусмотренное правилами пользования СЗИ;
   - ключевые носители хранятся раздельно с обеспечением условия невозможности их одновременной компрометации;
   - при транспортировке ключевых носителей с секретной ключевой информацией создаются условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию.
4. Рекомендации по выполнению следующих правил:
   - осуществление информационного взаимодействия с НКО только с использованием средств связи (мобильные и стационарные телефоны, факсы, интерактивные web-сайты/порталы, обычная и электронная почта и пр.), реквизиты которых оговорены в документах, получаемых непосредственно в НКО;
   - игнорирование поступающих на электронную почту сообщений или sms-сообщений, в которых под какими-либо предлогами (техническое перевооружение организации, обновление или сверка баз данных НКО и т.п.) предлагается ввести с клавиатуры компьютера персональную информацию (пароли, секретные ключи средств шифрования и АСП, персональные данные их

владельца и др.) в поля экранных форм в ходе имитируемых сеансов связи информационного взаимодействия с НКО;

- в случае отсутствия возможности подключения к Web-сайту НКО сообщать об этом в НКО по тел. (495) 223-95-10 или по адресу e-mail: admin@altbank.com;
- использование только лицензионного программного обеспечения на компьютере, с которого осуществляется доступ к ИКБ;
- использование ежедневно обновляемого антивирусного программного обеспечения, а также не реже одного раза в неделю установка обновлений, выпускаемых разработчиками операционных систем, web-браузеров;
- для защиты сетевого соединения на компьютере должен быть установлен и корректно настроен брандмауэр;
- лучшей практикой является отказ от использования ресурсов сети интернет, за исключением необходимых для работы ИКБ и обновления защиты, а также отказ от использования средств электронной почты. В случае, если отказаться от использования электронной почты невозможно, следует придерживаться следующих правил: Не открывать сообщения электронной почты, полученные от неизвестных отправителей. При получении таких писем рекомендуется их удалить без возможности восстановления (удаление с удержанием клавиши "shift");
- следует избегать использования каких-либо носителей информации, если эти носители получены из неизвестных или подозрительных источников или использовались на других компьютерах, возможно, незащищенных антивирусными средствами. В случае необходимости использования таких носителей необходимо предварительно провести их антивирусную проверку. Также следует отключить автозапуск сменных носителей в операционной системе;
- установка ключевого носителя в компьютер только при запросе системы и извлечение его сразу после выхода из ИКБ;
- в случае утраты ключевого носителя, невозможности входа в ИКБ, неожиданного отключения либо перезагрузки компьютера, при подозрении на "заражение" компьютерными вирусами следует незамедлительно прекратить использование ИКБ, извлечь ключевой носитель и обратиться в НКО для уточнения последних операций по счетам;
- ни при каких обстоятельствах не следует передавать носитель с ключевой информацией и не сообщать логин и пароль доступа к ИКБ посторонним лицам, даже представляющимися работниками НКО, а при наличии ключей 1-ой и 2-ой ЭЦП хранить их на разных носителях;
- немедленная замена Ключей в случаях их компрометации или подозрения на компрометацию, а также по истечении срока действия Ключа;
- исключение доступа к ИКБ с гостевых рабочих мест (Интернет-кафе и пр.).

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.