Руководство
по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

1. Ключ электронной подписи при генерации необходимо записывать на отчуждаемые относительно рабочего места носители ключевой информации (USB-токен, флеш-накопитель)
При этом ключ электронной подписи на ключевом носителе должен защищаться паролем (ПИН-кодом). Ответственность за сохранение пароля (ПИН-кода) в тайне возлагается на владельца сертификата ключа электронной подписи. Не рекомендуется использовать одно и то же значение пароля (ПИН-кода) для защиты нескольких ключевых носителей.

2. Необходимые меры безопасности при подписании:
– подсоединять полученный носитель ключевой информации к компьютеру только непосредственно перед подписанием, и в обязательном порядке извлекать его из компьютера сразу после окончания работы;
– обеспечить безопасное хранение носителя - в сейфе или запираемом ящике стола;
– при уходе с рабочего места, проверить стол и компьютер, извлечь ключевые носители и обеспечить их надежное хранение.

3. Не допускается:
– снимать несанкционированные копии с ключевых носителей;
– знакомить или передавать ключевые носители лицам, к ним не допущенным;
– записывать на ключевой носитель с ключами электронной подписи постороннюю информацию.

4. Требуется повторное обращение к представителю удостоверяющего центра для смены ключевой пары в случае:
– окончания срока действия ключа сертификата ключа проверки электронной подписи (далее - СКП ЭП);
– изменения данных владельца сертификата, предоставленных при получении СКП ЭП.
– замены ответственного лица, которое имеет право подписи электронной подписью электронных документов (для юридических лиц);
– увольнения уполномоченных представителей организации - владельцев сертификатов ключей проверки электронной подписи (для юридических лиц);
– обнаружения фактов доступа неуполномоченных лиц к ключевой информации (в том числе при подозрении о таком доступе).

В обязательном порядке уведомлять Удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении.

5. Использование средств квалифицированной подписи
Владелец СКП ЭП обязан использовать для создания и проверки электронных подписей, создания ключей электронных подписей и ключей их проверки средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 06 апреля 2011г. N 63-ФЗ «Об электронной подписи».

6. Обращение со средствами криптографической защиты информации (СКЗИ)
– Хранить инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, носители ключевой информации в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение и потерю;
– Осуществлять эксплуатацию СКЗИ в соответствии с эксплуатационной документацией, предусмотренной Формуляром на соответствующее СКЗИ.

После того как Удостоверяющий центр передал владельцу сертификата ключа проверки электронной подписи ключи электронной подписи, содержащиеся на носителе ключевой информации, конфиденциальность полученных данных полностью зависит от того, насколько ответственно владелец сертификата ключа проверки электронной подписи отнесётся к их использованию и хранению.