«УТВЕРЖДАЮ»

Директор ОБУ «Информационно-технический центр»

_____ А.А. Вахтин

«29» декабря 2012 г.

ИНСТРУКЦИЯ

пользователям по обеспечению безопасности использования электронной подписи

Электронная подпись представляет собой реквизит электронного документа, который позволяет установить отсутствие искажения информации в этом документе с момента формирования электронной подписи и определить лицо, подписывающее электронный документ. Значение реквизита получается в результате криптографического преобразования информации с использованием ключа электронной подписи, записанного на ключевой носитель.

Электронная подпись является полноценной заменой (аналогом) собственноручной подписи в случаях, предусмотренных действующим законодательством Российской Федерации.

При работе с электронной подписью должны выполняться требования настоящей Инструкции и иных документов, регламентирующих порядок обращения с информацией ограниченного распространения.

Пользователи, работающие с носителями ключевой информации, обязаны:

- Обеспечивать конфиденциальность ключей электронной подписи, принимать все возможные меры для предотвращения его хищения, потери, раскрытия, искажения и несанкционированного использования.
- 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.
- Не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.
- Для защиты ключа электронной подписи от несанкционированного использования установить на ключевой носитель пароль условно-постоянного действия длиной не менее шести буквенно-цифровых символов.
- Обеспечить условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц.
- Исключить бесконтрольное проникновение и пребывание в помещениях, в которых размещаются технические средства формирования электронной подписи, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в указанных помещениях. В случае необходимости присутствия таких лиц в указанных помещениях должен быть обеспечен контроль за их действиями.
- Применять для формирования электронной подписи только действующий ключ электронной подписи, т.е. не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован (отозван), срок действия которого истек или действие которого приостановлено.

- Использовать электронную подпись в соответствии с ограничениями, содержащимися в сертификате ключа проверки электронной подписи (если такие ограничения установлены).
- При наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена, не использовать ключ электронной подписи и немедленно обратиться в Удостоверяющий центр, выдавший сертификат, для прекращения действия этого сертификата.
- Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на аннулирование (отзыв) или приостановление действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления до момента времени официального уведомления об аннулировании (отзыве) или приостановлении действия сертификата, либо об отказе в аннулировании (отзыве) или приостановлении действия сертификата соответственно.
- При использовании средств криптографической защиты информации (СКЗИ) на рабочем месте, подключенном к сетям общего пользования, должны быть предприняты дополнительные меры, исключающие возможность несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей. Должен быть закрыт доступ ко всем неиспользуемым сетевым портам.
- В случае подключения рабочего места с установленным СКЗИ к общедоступным сетям передачи данных необходимо ограничить возможность открытия и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX и т.д.), полученных из сетей общего пользования, без проведения соответствующих проверок на предмет содержания в них программных закладок и вредоносных программ.
- При обнаружении на рабочем месте, оборудованном СКЗИ и средствами электронной подписи, посторонних программ или вирусов, нарушающих работу указанных средств, работа с электронной подписью на данном рабочем месте должна быть прекращена и должны быть организованы мероприятия по анализу и ликвидации негативных последствий данного нарушения.
- Использовать для проверки электронных подписей и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

Пользователям, работающим с носителями ключевой информации, запрещается:

- передавать свой ключевой носитель (эталонную или его рабочую копию) другим лицам (кроме как для хранения ответственному за информационную безопасность в опечатанном пенале с росписью в соответствующих учетных формах);
- делать неучтенные копии ключевого носителя, распечатывать или переписывать с него файлы на иной носитель информации (например, жесткий диск ПЭВМ), вносить изменения в файлы, находящиеся на ключевом носителе, записывать на ключевой носитель постороннюю информацию, а также выводить ключевую информацию на дисплей (монитор) или принтер;
- использовать ключевой носитель на заведомо неисправном считывателе и/или ПЭВМ;
- не вставлять и не оставлять ключевой носитель в ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей, а также на рабочих станциях, не задействованных в системе электронного документооборота;
- подписывать своей электронной подписью любые электронные сообщения и документы, кроме тех видов документов, которые регламентированы технологическим процессом и областями использования, указанными в сертификате ключа проверки электронной подписи;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ.