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

Настоящее Руководство составлено в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и является средством официального информирования лиц, владеющих квалифицированным сертификатом ключа проверки электронной подписи (далее – сертификат), об условиях, рисках и порядке использования квалифицированной электронной подписи и средств электронной подписи, а так же о мерах, необходимых для обеспечения безопасности при их использовании.

Владелец сертификата обязан:

- соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием средств квалифицированной электронной подписи, предусмотренные действующим законодательством Российской Федерации и настоящим Руководством;
- сдать средства квалифицированной электронной подписи и ключи электронной подписи, эксплуатационную и техническую документацию к ним в соответствии с порядком, установленным лицам, при увольнении или отстранении от исполнения обязанностей, связанных с использованием средств квалифицированной электронной подписи;
- немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи средств квалифицированной электронной подписи, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений;
- обеспечивать конфиденциальность ключей электронной подписи, в частности не допускать использование принадлежащих ему ключей электронной подписи без его согласия;
- своевременно предоставлять документы и сведения в Удостоверяющий центр АО «ЕЭТП» (далее – УЦ) для перевыпуска сертификата при изменении информации, содержащейся в сертификате;
- уведомлять УЦ, выдавший сертификат, 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;
- использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированной электронной подписи и ключей их проверки средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с действующим Федеральным законодательством;
- не использовать ключ электронной подписи и немедленно обратиться в УЦ для прекращения действия сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена;
- использовать квалифицированную электронную подпись в соответствии с ограничениями, содержащимися в сертификате (если такие ограничения установлены);
- соблюдать требования Регламента УЦ;
- принять меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным средством квалифицированной электронной подписи, посторонних лиц, по роду своей деятельности, не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на средства квалифицированной электронной подписи, технические средства, на которых эксплуатируется средства квалифицированной электронной подписи и защищаемую информацию.

Владельцу сертификата запрещается:

- оставлять без контроля вычислительные средства, на которых эксплуатируется средства квалифицированной электронной подписи, после ввода ключевой информации либо иной конфиденциальной информации;
- вносить какие-либо изменения в программное обеспечение средств квалифицированной электронной подписи;
- осуществлять несанкционированное администратором безопасности копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием средств квалифицированной электронной подписи;
- записывать на ключевые носители постороннюю информацию;
- использовать нестандартные, изменённые или отладочные версии операционных систем (далее - ОС);
- использовать ОС, отличную от предусмотренной для штатной работы;
- использовать возможность удалённого управления, администрирования и модификации ОС и её настроек;
- использовать ключевые носители в режимах, не предусмотренных функционированием средств криптографической защиты информации (далее – СКЗИ);
- подключать к компьютеру с установленным средством квалифицированной электронной подписи дополнительные устройства и соединители, не предусмотренные штатной комплектацией.
- изменять настройки, установленные программой установки средства квалифицированной электронной подписи или администратором;
- обрабатывать на персональной электронно-вычислительной машине (далее – ПЭВМ), оснащённой средством квалифицированной электронной подписи, информацию, содержащую государственную тайну;
- осуществлять несанкционированное вскрытие системных блоков ПЭВМ;
- использовать на ПЭВМ нелицензионное программное обеспечение.

Владелец сертификата несёт ответственность за:

- полноту и своевременность предоставления документов и сведений в УЦ в соответствии с Регламентом УЦ;
- обеспечение конфиденциальности ключей электронной подписи, в частности за допущение использования принадлежащих ему ключей электронной подписи без его согласия;
- не уведомление УЦ, выдавшего сертификат, 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;
- использование ключа электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.