РУКОВОДСТВО ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ И СРЕДСТВ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ (СКЗИ)

1. Требования по организационному обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (СКЗИ)

Требования по организационному обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (СКЗИ):

Участник СЭД приказом уполномоченного органа назначает (определяет) должностных лиц, ответственных за обеспечение безопасности использования электронной подписи и средств электронной подписи (СКЗИ);

Участник СЭД разрабатывает и утверждает приказом уполномоченного органа организационно-распорядительные документы, регламентирующие вопросы безопасности использования электронной подписи и средств электронной подписи (СКЗИ);

Участник СЭД допускает к использовании электронной подписи и средств электронной подписи (СКЗИ) работников, имеющих навыки работы на персональном компьютере, прошедших обучение и (или) ознакомленных с правилами использования электронной подписи и средств электронной подписи (СКЗИ).

2. Требования по размещению средств квалифицированной электронной подписи (СКЗИ) и режиму охраны

Требования по размещению средств квалифицированной электронной подписи (СКЗИ) и режиму охраны:

помещения, в которых размещаются технические средства с установленным программным обеспечением СЭД со встроенными СКЗИ, 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 средств электронной подписи (СКЗИ) и конфиденциальных документов;

размещение средств электронной подписи (СКЗИ), 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 они отображаются, через окна;

в режимные помещения допускаются руководители Участника СЭД, работники подразделения безопасности и исполнители, имеющие прямое отношение к использованию средств электронной подписи (СКЗИ), обработке, передаче и приему конфиденциальных документов;

системные блоки компьютеров со средствами электронной подписи (СКЗИ) оборудуются средствами контроля вскрытия;

ремонт и (или) последующее использование системных блоков осуществляется после удаления средств электронной подписи (СКЗИ).

3. Требования по обеспечению безопасности ключевой информации

Требования по обеспечению безопасности ключевой информации:

ключевые носители с ключами электронных подписей и инсталляционные носители информации с программным обеспечением средств электронной подписи (СКЗИ) должны браться на поэкземплярный учет в выделенных для этих целей журналах;

учет и хранение ключей электронных подписей должны осуществляться назначенным приказом уполномоченного органа Участника СЭД работником;

для хранения ключевых носителей с ключами электронных подписей выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации;

хранение ключей электронных подписей и инсталляционных носителей информации с программным обеспечением средств электронных подписей (СКЗИ) допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования средств электронных подписей (СКЗИ), применение;

рабочие и резервные ключи электронных подписей должны храниться раздельно с обеспечением условия невозможности их одновременной компрометации;

при транспортировке ключевых носителей с ключами электронных подписей должны создаваться условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию;

выведенные установленным порядком из действия ключи электронных подписей должны уничтожаться определенным эксплуатационной документацией на средства электронных подписей (СКЗИ) порядком.

4. Требования по установке средств квалифицированной электронной подписи (СКЗИ), общесистемного и специального программного обеспечения

Требования по установке средств квалифицированной электронной подписи (СКЗИ), общесистемного и специального программного обеспечения:

к установке средств электронной подписи (СКЗИ), общесистемного и специального программного обеспечения, допускаются лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующие средства;

при установке средств электронной подписи (СКЗИ) следует:

использовать только лицензионное программное обеспечение;

инсталлировать средства электронной подписи (СКЗИ) только с дистрибутива, полученного от Организатора СЭД;

на технических средствах с установленными средствами электронных подписей (СКЗИ) не должны устанавливаться средства разработки программного обеспечения и отладчики;

предусмотреть меры, исключающие возможность несанкционированного изменения технических средств, на которых установлены средства электронных подписей (СКЗИ), например, путем опечатывания системного блока и разъемов;

не использовать нестандартные, измененные или отладочные версии операционных систем;

исключить возможность загрузки и использования операционной системы, отличной от предусмотренной для штатной работы;

исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;

на технических средствах с установленными средствами электронных подписей (СКЗИ) должна быть установлена только одна операционная система;

все неиспользуемые ресурсы необходимо отключить (протоколы, сервисы и т.п.);

всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;

предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):

системный реестр;

файлы и каталоги;

временные файлы;

журналы системы;

файлы подкачки;

кэшируемая информация (пароли и т.п.);

отладочная информация;

необходимо обеспечить стирание (по окончании сеанса работы средств электронных подписей (СКЗИ)) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы средств электронных подписей (СКЗИ). Если это не выполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;

регулярно устанавливать пакеты обновления безопасности операционной системы (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а так же исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий;

исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

5. Требования по использованию средств квалифицированной электронной подписи (СКЗИ)

При использовании средств электронной подписи (СКЗИ) запрещается:

оставлять технические средства с установленными средствами электронных подписей (СКЗИ) без контроля после ввода ключевой информации либо иной конфиденциальной информации;

вносить какие-либо изменения в средства электронных подписей (СКЗИ);

осуществлять несанкционированное копирование ключевых носителей;

разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на монитор, принтер и иные средства отображения информации;

использовать ключевые носители в режимах, не предусмотренных эксплуатационной документацией на средства электронных подписей (СКЗИ);

записывать на ключевые носители постороннюю информацию;

подключать к техническим средствам с установленными средствами электронной подписи (СКЗИ) дополнительные устройства и соединители, не предусмотренные штатной комплектацией;

изменять настройки, установленные программой установки средств электронной подписи (СКЗИ) или Администратором безопасности;

осуществлять несанкционированное вскрытие корпуса технического средства с установленными средствами электронной подписи (СКЗИ).

6. Требования по обеспечению информационной безопасности при работе в системе электронного документооборота

При работе в системе электронного документооборота:

запрещается пересылать файлы с ключевой информацией по электронной почте сети Интернет или по внутренней электронной почте Участника СЭД (кроме запросов на сертификат и сертификатов);

ключевая информация должна размещаться на отчуждаемых носителях информации (floppy-диск, ruToken, eToken и др.). Не рекомендуется помещать ключевую информацию на локальной диск, а также в реестр операционной системы Windows;

носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средством электронной подписи криптографических операций;

запрещается записывать на ключевой носитель иную информацию (в том числе рабочие или личные файлы);

средства СЭД с установленными средствами электронной подписи (СКЗИ) должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования;

на средствах СЭД:

должно быть установлено только лицензионное программное обеспечение и лицензионное антивирусное программное с регулярно обновляемыми антивирусными базами данных;

должны быть отключены все неиспользуемые службы и процессы операционной системы Windows (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски C$ и т.д.);

должны регулярно устанавливаться обновления операционной системы;

должен быть исключен доступ (физический и/или удаленный) к средствам СЭД с установленными средствами электронной подписи (СКЗИ) третьих лиц, не имеющих полномочий для работы в СЭД;

должна использоваться регистрации событий информационной безопасности;

должна быть включена автоматическая блокировка экрана монитора после ухода при оставлении пользователем СЭД рабочего места.

в случае передачи (списания, отправки в ремонт) сторонним лицам средств СЭД, на которых установлены средства электронной подписи (СКЗИ), необходимо гарантированно удалить с них всю конфиденциальную информацию, в том числе базы данных СЭД, средства электронной подписи (СКЗИ), журналы документов и протоколы работы средств СЭД.