|  |  |
| --- | --- |
|  |  |

ФЕДЕРАЛЬНОЕ КАЗНАЧЕЙСТВО

(Казначейство России)

|  |  |
| --- | --- |
|  |  |

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

*Настоящее руководство является информационным документом, описывающим условия и порядок использования электронных подписей и средств электронной подписи, риски, связанные с использованием электронных подписей, меры, необходимые для обеспечения безопасности электронных подписей*

**Москва, 2013**

Содержание

[1. Общие положения 3](#_Toc354384211)

[2. Требования по размещению 3](#_Toc354384212)

[3. Требования по установке средств электронной подписи и средств криптографической защиты, общесистемного и специального программного обеспечения 3](#_Toc354384213)

[4. Меры по обеспечению защиты от несанкционированного доступа 3](#_Toc354384214)

[5. Требования по обеспечению информационной безопасности при работе в системах обмена электронными документами 3](#_Toc354384215)

[5.1 Меры защиты ключей электронной подписи 3](#_Toc354384216)

[5.2 Обращение с ключевой информацией и ключевыми носителями 3](#_Toc354384217)

[5.3 Обеспечение безопасности АРМ, с установленными СКЗИ 3](#_Toc354384218)

[6. Дополнительные требования 3](#_Toc354384219)

# Общие положения

Настоящее руководство составлено в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» является средством официального информирования лиц, заинтересованных в получении или владеющих сертификатом ключа проверки электронной подписи, об условиях, рисках и порядке использования электронных подписей и средств электронной подписи, а так же о мерах, необходимых для обеспечения безопасности при использовании электронных подписей.

Применение электронных подписей в системах юридически значимого электронного документооборота и иных системах, сопровождаются рисками финансовых убытков и иного рода потерь, связанных с признанием недействительности сделок, совершенных с использованием электронной подписи при несанкционированном получении злоумышленником ключа электронной подписи или несанкционированного использования рабочего места пользователя, на котором осуществляется выработка электронной подписи. В связи с этим необходимо выполнение приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации.

# Требования по размещению

При размещении средств электронной подписи и средств криптографической защиты:

- должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства электронной подписи и средства криптографической защиты, посторонним лицам, не имеющим допуск к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной подписи, средства криптографической защиты и передаваемую информацию;

- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

# Требования по установке средств электронной подписи и средств криптографической защиты, общесистемного и специального программного обеспечения

К установке общесистемного и специального программного обеспечения, а также программного обеспечения средств электронной подписи и средств криптографической защиты, допускаются лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее программное обеспечение.

При установке программного обеспечения средств электронной подписи и средств криптографической защиты следует:

- на технических средствах, на которые устанавливаются средства электронной подписи и средства криптографической защиты, использовать только лицензионное программное обеспечение фирм-изготовителей;

- инсталляция программного обеспечения средств электронной подписи и средств криптографической защиты должна производиться только с дистрибутива, полученного в Удостоверяющем центре Федерального казначейства и должны быть обеспечены организационно-технические меры по исключению подмены дистрибутива, внесения изменений в средства электронной подписи и средства криптографической защиты после установки;

- на технических средствах с установленными средствами электронной подписи и средствами криптографической защиты не должны устанавливаться средства разработки программного обеспечения и отладчики. Если средства отладки приложений нужны для технологических потребностей пользователя, то их использование должно быть санкционировано Администратором безопасности. При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования кода и памяти программного обеспечения средств электронной подписи и средств криптографической защиты в процессе обработки защищаемой информации и/или при загруженной ключевой информации;

- предусмотреть меры исключающие возможность несанкционированного изменения аппаратной части технических средств, на которых установлены средства электронной подписи и средства криптографической защиты (например, путем опечатывания системного блока и разъемов);

Программное обеспечение используемое на технических средствах с установленными средствами электронной подписи и средствами криптографической защиты, не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;

- модифицировать собственный код и код других подпрограмм;

- модифицировать память, выделенную для других подпрограмм;

- передавать управление в области собственных данных и данных других подпрограмм;

- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;

- повышать предоставленные привилегии;

- модифицировать настройки операционной системы;

- использовать недокументированные фирмой-разработчиком функции операционной системы.

# Меры по обеспечению защиты от несанкционированного доступа

При использовании средств электронной подписи и средств криптографической защиты должны выполняться следующие меры по защите информации от несанкционированного доступа:

Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:

- длина пароля должна быть не менее 6 символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, \*, % и т.п.);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

- личный пароль пользователь не имеет права никому сообщать;

- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 дней.

Запрещается:

- оставлять технические средства с установленными средствами электронной подписи и средствами криптографической защиты без контроля, после ввода ключевой информации;

- вносить какие-либо изменения в программное обеспечение средств электронной подписи и средств криптографической защиты;

- 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 иные средства отображения информации;

- использовать ключевые носители в режимах, не предусмотренных функционированием средств электронной подписи и средств криптографической защиты;

- записывать на ключевые носители постороннюю информацию.

Администратор безопасности должен сконфигурировать операционную систему и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

- не использовать нестандартные, измененные или отладочные версии операционных систем;

- исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;

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

- на технических средствах с установленными средствами электронной подписи и средствами криптографической защиты должна быть установлена только одна операционная система;

- правом установки и настройки операционной системы, а также средств электронной подписи и средств криптографической защиты должен обладать только Администратор безопасности;

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

- режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;

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

- необходимо предусмотреть меры, максимально ограничивающие доступ к:

- ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):

- системному реестру;

- файлам и каталогам;

- временным файлам;

- журналам системы;

- файлам подкачки;

- кэшируемой информации (пароли и т.п.);

- отладочной информации.

Кроме того необходимо организовать стирание (по окончанию сеанса работы средств электронной подписи и средств криптографической защиты) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это не выполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

Должно быть исключено попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий.

Необходимо регулярно устанавливать пакеты обновлений 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.

В случае подключения технических средствах с установленными средствами электронной подписи и средствами криптографической защиты к общедоступным сетям передачи данных необходимо 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. С целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем к программному обеспечению, в окружении которого функционируют средства электронной подписи и средства криптографической защиты и к компонентам средств электронной подписи и средств криптографической защиты со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN-сетей и т.п.). Все средства защиты, должны иметь сертификат уполномоченного органа по сертификации средств защиты.

Организовать и использовать систему аудита, организовать регулярный анализ результатов аудита.

Организовать и использовать комплекс мероприятий по антивирусной защите.

**ЗАПРЕЩАЕТСЯ:**

- осуществлять несанкционированное копирование ключевых носителей;

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер (за исключением случаев, предусмотренных данными требованиями);

- вставлять ключевой носитель в устройство считывания в режимах, не

предусмотренных штатным режимом использования ключевого носителя;

- подключать к техническим средствам с установленными средствами электронной подписи и средствами криптографической защиты дополнительные устройства и соединители, не предусмотренные штатной комплектацией;

- работать на технических средствах с установленными средствами электронной подписи и средствами криптографической защиты, если во время его начальной загрузки не проходит встроенный тест ОЗУ;

- вносить какие-либо изменения в программное обеспечение средств электронной подписи и средств криптографической защиты;

- изменять настройки, выставленные программой установки средств электронной подписи и средств криптографической защиты или Администратором безопасности;

- обрабатывать на технических средствах с установленными средствами электронной подписи и средствами криптографической защиты информацию, содержащую государственную тайну;

- осуществлять несанкционированное вскрытие корпуса технического средства с установленными средствами электронной подписи и средствами криптографической защиты;

- работать со средствами электронной подписи и средствами криптографической защиты при включенных в техническое средство штатных средствах выхода в радиоканал;

- приносить и использовать в помещении, где размещены средства электронной подписи и средства криптографической защиты, радиотелефоны и другую радиопередающую аппаратуру (требование носит рекомендательный характер).

# Требования по обеспечению информационной безопасности при работе в системах обмена электронными документами

## 5.1 Меры защиты ключей электронной подписи

Ключи электронной подписи при их создании должны записываться на типы ключевых носителей, которые поддерживаются используемым средством электронной подписи согласно технической и эксплуатационной документации к ним.

Ключи электронной подписи на ключевом носителе защищаются паролем (ПИН-кодом). Пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство электронной подписи.

Если процедуру генерации ключей выполняет сотрудник Удостоверяющего центра Федерального казначейства, то он должен сообщить сформированный пароль (ПИН-код) владельцу ключа электронной подписи.

Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа электронной подписи.

Сотрудники Удостоверяющего центра Федерального казначейства, являющиеся владельцами ключей электронной подписи, также выполняют указанные в настоящем разделе меры защиты ключей электронной подписи.

## 5.2 Обращение с ключевой информацией и ключевыми носителями

Недопустимо пересылать файлы с ключевой информацией для работы в системах обмена электронными документами по электронной почте сети Интернет или по внутренней электронной почте (кроме запросов на сертификат и открытых ключей).

Ключевая информация должна размещаться на сменном носителе информации (floppy-диск, USB-flash накопитель, e-Token, ru-Token и др.). Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами электронной подписи и средствами криптографической защиты, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

Носители ключевой информации должны использоваться только их владельцем либо уполномоченным лицом на использование данного носителя, и храниться в месте не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).

Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами электронной подписи и средствами криптографической защиты операций формирования и проверки электронной подписи, зашифрования и расшифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

## 

## 5.3 Обеспечение безопасности АРМ, с установленными СКЗИ

С целью контроля исходящего и входящего подозрительного трафика, технические средства с установленными средствами электронной подписи и средствами криптографической защиты должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. Эти средства должны пресекать отправку в Интернет информации, инициированную программами, не имеющими соответствующих полномочий.

На технических средствах, используемых для работы в системах обмена электронными документами:

- на учетные записи пользователей операционной системы должны быть

установлены пароли, удовлетворяющие требованиям, приведенным в разделе 4;

- должно быть установлено только лицензионное программное обеспечение;

- должно быть установлено лицензионное антивирусное программное обеспечение 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 С$ и т.д.);

- должны регулярно устанавливаться обновления операционной системы;

- должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами электронной подписи и средствами криптографической защиты третьих лиц, не имеющих полномочий для работы в системе обмена электронными документами;

- должна быть активирована подсистема регистрации событий информационной безопасности;

- должна быть включена автоматическая блокировка экрана после ухода ответственного сотрудника с рабочего места.

В качестве автоматизированного рабочего места для работы в системах обмена электронными документами крайне не рекомендуется выбирать переносной компьютер (ноутбук). Если выбран ноутбук, недопустимо его подключение к сетям общего доступа в местах свободного доступа в Интернет (Интернет-кафе, гостиницы, офисные центры и т.д.), при этом для хранения ключевой информации должен использоваться сменный носитель информации.

В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств на которых были установлены средства электронной подписи и средства криптографической защиты, необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред организации, в том числе средства электронной подписи и средства криптографической защиты, журналы работы систем обмена электронными документами и т.д.).

# Дополнительные требования

Дополнительные требования по обеспечению информационной безопасности при работе в системах обмена электронными документами могут дополнительно устанавливаться правилами систем ЭДО, требованиями по эксплуатации и безопасности средств электронной подписи и средств криптографической защиты.

**Лист ознакомления**

с требованиями Руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Ф.И.О.** | **Дата** | **Подпись** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |