Приложение № 14
к Порядку реализации функций аккредитованного удостоверяющего
центра БУ «Центр информационных технологий»
Мининформполитики Чувашии

Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи

1. Общие принципы обеспечения информационной безопасности при организации электронного взаимодействия с использованием электронной подписи.

Организация электронного взаимодействия с использованием электронной подписи должна осуществляться с учетом требований федеральных законов «Об электронной подписи», «Об информации, информационных технологиях и о защите информации», Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152 (далее также – Инструкция ФАПСИ № 152), других федеральных законов и нормативных правовых актов, осуществляющих правовое регулирование отношений в области обеспечения защиты информации и использования электронной подписи, руководящих документов ФСТЭК России и ФСБ России, эксплуатационной и технической документации на используемые средства электронной подписи, средства криптографической защиты информации (далее также – СКЗИ).

Если иное не установлено федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или решением о создании корпоративной информационной системы, порядок использования электронной подписи в корпоративной информационной системе может устанавливаться оператором этой системы или соглашением между участниками электронного взаимодействия в ней.

2. Риски, связанные с использованием электронных подписей и средств электронной подписи.

2.1. Виды рисков, связанных с использованием электронных подписей и средств электронной подписи.

В случае, если электронное взаимодействие с использованием электронной подписи осуществляется без учета требований нормативных правовых актов, регулирующих отношения в области использования электронных подписей, используется неквалифицированная электронная подпись или средства электронной подписи не сертифицированы на соответствие требованиям безопасности информации, могут возникнуть или существенно возрасти риски, связанные с использованием электронной подписи, основными из которых могут являться:

риски, связанные с нарушением целостности электронного документа и возможностью отказа от него. Данные риски могут быть связаны с внесенными в электронный документ изменениями, произведенными после его подписания. Лицо, подписавшее электронный документ неквалифицированной электронной подписью, или лицо, осуществляющее проверку такой электронной подписи, может заявить о том, что содержание электронного документа было изменено после его подписания и электронный документ не соответствует тому документу, который был подписан неквалифицированной электронной подписью;

риски, связанные с проверкой принадлежности ключа электронной подписи, с помощью которой подписан электронный документ, владельцу сертификата ключа проверки электронной подписи (далее – владелец сертификата). Лицо, владеющее сертификатом ключа проверки электронной подписи и соответствующим ключом электронной подписи, которым был подписан электронный документ, может заявить о том, что неквалифицированная электронная подпись, содержащаяся в электронном документе, не принадлежит данному владельцу сертификата;

риски, связанные с признанием юридической силы электронного документа, подписанного неквалифицированной электронной подписью. Одна из сторон может заявить о том, что подписанный неквалифицированной электронной подписью документ не может порождать юридически значимых последствий или считаться достаточным доказательством в суде;

риски, связанные с несоответствием условий использования электронной подписи установленному порядку. В случае, если порядок использования неквалифицированной электронной подписи и средств электронной подписи не соответствует требованиям нормативных правовых актов Российской Федерации, осуществляющих правовое регулирование отношений в использовании электронной подписи или не соответствует порядку использования неквалифицированной электронной подписи, определяемому соглашениями сторон, юридическая значимость подписанных такой электронной подписью документов может быть не признана одной из сторон участника электронного взаимодействия;

риски, связанные с нарушением конфиденциальности ключей электронной подписи (использование ключей электронной подписи без согласия владельца). В случае нарушения конфиденциальности ключей электронной подписи, в том числе компрометации ключей, несанкционированного доступа к ключевым носителям или средствам электронной подписи, участником электронного взаимодействия может быть принят в исполнение подписанный неквалифицированной электронной подписью документ, порождающий юридически значимые последствия;

риски, связанные с несовместимостью средств электронной подписи, используемых сторонами для организации электронного взаимодействия. Несовместимость средств электронной подписи, протоколов и форматов данных, используемых сторонами для организации электронного взаимодействия, может привести к невозможности проверки неквалифицированной электронной подписи документа или к её некорректной проверке;

риски, связанные с определением полномочий лица, подписавшего электронной подписью документ. В случае, если участниками электронного взаимодействия не определены лица, участвующие в электронном взаимодействии, полномочия данных лиц по подписанию электронных документов от имени участника электронного взаимодействия, а также в случае, если полномочия лица по подписанию электронных документов прекращены, одна из сторон может заявить, что полученный электронный документ содержит неквалифицированную электронную подпись лица, не уполномоченного на подписание данного документа и не может быть принят в исполнение;

риски, связанные с использованием сертификатов ключей проверки электронной подписи и ключей электронной подписи, прекративших своё действие. В случае использования для подписания электронных документов ключа электронной подписи, прекратившего своё действие на момент подписания, либо, если момент подписания электронного документа не определен, а также в случае использования сертификата ключа проверки электронной подписи, который стал недействующим на день проверки электронной подписи, сторона, получившая подписанный неквалифицированной

электронной подписью документ, может заявить о непризнании такого электронного документа.

2.2. Меры по снижения вероятности возникновения рисков, связанных с использованием электронных подписей.

В целях снижения вероятности возникновения и реализации указанных рисков участникам электронного взаимодействия необходимо предусмотреть обеспечение комплекса правовых и организационно-технических мероприятий по обеспечению информационной безопасности при осуществлении электронного взаимодействия с использованием усиленной квалифицированной электронной подписи (далее также – электронная подпись) и сертифицированных по требованиям безопасности информации средств электронной подписи, получивших подтверждение соответствия требованиям к средствам электронной подписи, установленным в соответствии с Федеральными законом «Об электронной подписи» (далее также – сертифицированные средства электронной подписи).

Электронное взаимодействие с использованием усиленной квалифицированной электронной подписи и сертифицированных средств электронной подписи, осуществляемое с учетом требований Федерального закона «Об электронной подписи», других федеральных законов, принимаемых в соответствии с ними нормативных правовых актов, регулирующих отношения в области использования электронных подписей, позволяет обеспечить:

неотказуемость от электронного документа, содержащего электронную подпись. Квалифицированная электронная подпись позволяет определить лицо, подписавшее электронный документ;

целостность электронного документа. Квалифицированная электронная подпись позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания.

В случае необходимости обеспечения конфиденциальности передаваемой информации ключи электронной подписи и СКЗИ могут использоваться для обеспечения защиты информации, в том числе при её передаче по информационно-телекоммуникационным сетям, а также для организации защищенных каналов связи с использованием шифровальных (криптографических) средств.

Использование квалифицированной электронной подписи и сертифицированных средств электронной подписи позволяет:

установить факт изменения подписанного электронного документа после момента его подписания;

обеспечить практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки;

создать электронную подпись в формате, обеспечивающем возможность ее проверки всеми средствами электронной подписи.

При создании электронной подписи сертифицированные средства электронной подписи должны:

показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписываемой с использованием указанных средств, лицу, осуществляющему создание электронной подписи, содержание информации, подписание которой производится;

создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи

однозначно показывают, что квалифицированная электронная подпись создана.

При проверке электронной подписи сертифицированные средства электронной подписи должны:

показывать содержание электронного документа, подписанного электронной подписью;

показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;

указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

Одной из составных частей инфраструктуры открытых ключей и системы криптографической защиты информации является аккредитованный удостоверяющий центр, выполняющий функции по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей (далее также – квалифицированный сертификат).

Удостоверяющий центр осуществляет свою деятельность в строгом соответствии с нормативными правовыми актами Российской Федерации, руководящими документами, эксплуатационной документацией на используемые средства, Порядком реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей (далее также – Порядок) и другими документами, регулирующими вопросы использования электронной подписи.

Квалифицированные сертификаты, изготавливаемые Удостоверяющим центром, заверяются электронной подписью уполномоченного лица удостоверяющего центра, что подтверждает факт принадлежности ключа электронной подписи конкретному лицу участника электронного взаимодействия. Использование квалифицированных сертификатов позволяет участника электронного взаимодействия идентифицировать лицо, подписавшее электронной подписью документ, а также позволяет подтвердить целостность (неизменность) содержания подписанного электронного документа при проверке электронной подписи. Таким образом, при соблюдении требований информационной безопасности и соблюдения порядка использования квалифицированной электронных подписей, практически исключаются риски, связанные использованием электронных подписей, в том числе риски, связанные с подтверждением юридической значимости электронных документов, подписанных усиленной квалифицированной электронной подписью

3. Меры, необходимые для обеспечения безопасности при использовании электронных подписей.

3.1. Требования и рекомендации по обеспечению информационной безопасности при использовании средств электронной подписи.

В организации, эксплуатирующей средства электронной подписи (СКЗИ), должны быть предусмотрены организационные и организационно-технические мероприятия, направленные на обеспечение информационной безопасности при использовании средств электронной подписи и определяющие требования к ответственным лицам, автоматизированным рабочим местам пользователей СКЗИ (далее также - АРМ), системному и прикладному программному обеспечению, условиям хранения и использования средств электронной подписи, ключей электронной подписи и ключевых носителей.

3.1.1. Требования и рекомендации по назначению ответственных лиц.

В организации должны быть определены лица, ответственные за осуществление электронного взаимодействии с использованием электронной подписи и имеющие доступ к ключевым носителям, а также лица, ответственные за организацию работ по

защите информации и соблюдению условий хранения и использования ключей электронной подписи и средств электронной подписи.

К работе со средствами электронной подписи должны допускаться лица, прошедшие соответствующее обучение и ознакомленные с Инструкцией ФАПСИ №152, другими нормативными правовыми актами и руководящими документами, в том числе внутренними организационными документами и инструкциями по защите информации при использовании электронной подписи, а также эксплуатационной документацией на используемые средства электронной подписи.

В организации, эксплуатирующей СКЗИ, должно быть назначено лицо, выполняющее функции администратора информационной безопасности, на которого возлагаются задачи организации работ по защите информации, подготовки соответствующих инструкций, обучения и инструктажа пользователей СКЗИ, ведению журналов учета СКЗИ, настройке системного, прикладного программного обеспечения, СКЗИ и средств защиты от несанкционированного доступа, устанавливаемого на АРМ пользователей СКЗИ, контролю за соблюдением требований по безопасности, а также взаимодействия с удостоверяющим центром по вопросам использования электронной подписи.

3.1.2. Требования и рекомендации к помещениям и размещению технических средств АРМ.

Помещения, в которых расположены АРМ, предназначенные для работы со средствами электронной подписи (далее – спецпомещения), должны соответствовать требованиям Инструкции ФАПСИ №152. Должен быть исключен бесконтрольный допуск лиц, не допущенных к работе в указанных спецпомещениях. В случае необходимости присутствия посторонних лиц в спецпомещениях должен быть обеспечен контроль за их действиями.

Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Окна спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

Размещение АРМ должно производиться с учетом схемы контролируемой зоны и исключать возможность просмотра посторонними лицами работ, осуществляемых на АРМ.

Спецпомещения рекомендуется оснащать охранной сигнализацией, связанной со службой охраны здания или дежурным по организации.

3.1.3. Требования и рекомендации к АРМ пользователей СКЗИ.

Не допускается оставлять без контроля АРМ при включенном питании и подключенными ключевыми носителями. Перед уходом пользователь СЗКИ должен выключить АРМ либо заблокировать рабочую станцию с использованием средств защиты информации от несанкционированного доступа или с использованием средств операционной системы. Рекомендуется настроить автоматическое включение экранной заставки, защищенной паролем.

На АРМ пользователей рекомендуется установить сертифицированные средства защиты информации от несанкционированного доступа, а также средства антивирусной защиты.

В целях исключения возможности несанкционированного изменения аппаратной части системного блока администратору рекомендуется предусмотреть опечатывание системного блока АРМ.

Необходимо предусмотреть организацию парольной защиты при включении АРМ и загрузке операционной системы с использованием средств защиты информации (средств доверенной загрузки), либо средств BIOS и средств операционной системы, также рекомендуется определить установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске, отключить возможность загрузки с внешних съемных дисков, исключить возможность нестандартных видов загрузки операционной системы.

3.1.4. Требования и рекомендации по настройке системного и прикладного программного обеспечения.

На технических средствах АРМ с установленными средствами электронной подписи необходимо использовать только лицензионное программное обеспечение, полученное из доверенных источников. Не допускается использовать нестандартные, измененные или отладочные версии операционной системы.

Не допускается установка на АРМ средств разработки и отладки программного обеспечения. Необходимо исключить возможность установки средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам, а также вредоносного программного обеспечения, позволяющего получать привилегии администратора.

Рекомендуется ограничить права пользователя АРМ по самостоятельной установке программного обеспечения и настроить возможность выполнения пользователем АРМ только тех приложений, которые разрешены администратором информационной безопасности.

Необходимо регулярно отслеживать и устанавливать обновления безопасности для операционной системы, программного обеспечения АРМ, регулярно осуществлять обновление антивирусных баз.

3.1.5. Требования к настройкам операционной системы, установленной на АРМ пользователя.

До начала использования средств электронной подписи администратор информационной безопасности должен произвести настройку операционной системы, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль настроек в соответствии со следующими рекомендациями:

правом установки и настройки операционной системы и средств электронной подписи должен обладать только администратор безопасности;

в целях возможности разграничения прав доступа рекомендуется использовать средства, входящие в состав средств защиты информации;

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

все привилегии группы Everyone должны быть удалены;

необходимо исключить использование режима автоматического входа пользователя в операционную систему при ее загрузке без ввода пароля;

рекомендуется переименовать стандартную учетную запись администратора;

рекомендуется отключить учетная запись для гостевого входа;

исключить возможность удаленного управления, администрирования и модификации операционной системы и её настроек, системного реестра, для всех, включая группу администраторов;

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

должно быть исключено или ограничено использование пользователями сервиса планировщика задач. При использовании данного сервиса состав запускаемого

программного обеспечения на АРМ согласовывается с администратором информационной безопасности;

рекомендуется организовать удаление временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы средств электронной подписи. Если это невыполнимо, то операционная система должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;

должны быть отключены средства удаленного администрирования, в случае если такое подключение осуществляется без использования защищенных каналов связи;

должны быть установлены ограничения на доступ пользователей к системному реестру путем настройки прав доступа к системному реестру;

на все директории (папки), содержащие системные файлы и программы из комплекта СКЗИ, должны быть установлены права доступа, запрещающие запись всем пользователям, кроме пользователя, имеющего права администратора, создателя (владельца) и права системы;

необходимо обеспечить ведение журналов аудита в операционной системе;

настройка параметров системного реестра производится в соответствии с эксплуатационной документацией на средства электронной подписи.

3.1.6. Требования и рекомендации при организации парольной защиты.

Рекомендуется разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, доступа к ключам электронной подписи), использовать правила формирования и хранения паролей в соответствии со следующими правилами:

длина пароля должна быть не менее 8 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 и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);

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

пользователь АРМ должен обеспечивать конфиденциальность паролей, не допускается хранить записанные пароли в легкодоступных местах;

периодичность смены пароля определяется принятой политикой безопасности (инструкцией по организации парольной защиты), но не должна превышать двух месяцев.

указанная политика должна применяться для всех учетных записей пользователей, зарегистрированных в операционной системе.

3.1.7. Требования к установке, настройке и использованию средств электронной подписи.

Установка и настройка средств электронной подписи (СКЗИ) должна выполняться администратором информационной безопасности либо лицом, ответственным за работоспособность АРМ и прошедшим соответствующее обучение.

Установка средств электронной подписи должна производиться только с дистрибутива, полученного по доверенному каналу, в соответствии с эксплуатационной документацией на средства электронной подписи.

При установке средств электронной подписи должен быть обеспечен контроль целостности устанавливаемого программного обеспечения.

Перед установкой средств электронной подписи необходимо произвести проверку операционной системы на отсутствие вредоносных программ с помощью антивирусных средств.

После завершения установки осуществляются настройка и контроль работоспособности средств электронной подписи.

Использование средств электронной подписи должно осуществляться в соответствии с эксплуатационной документацией и инструкциями на средства электронной подписи.

3.1.8. Требования обеспечения информационной безопасности при подключении АРМ к сетям связи общего пользования, в том числе к информационно-телекоммуникационной сети «Интернет».

Не рекомендуется подключать к сетям связи общего пользования АРМ пользователя при работе со средствами электронной подписи и носителями ключей электронной подписи. В случае необходимости подключения АРМ к сетям связи общего пользования такое подключение рекомендуется производить с использованием сертифицированного межсетевого экрана, настроенного в соответствии с требованиями эксплуатационной документации на средства межсетевого экранирования.

В случае подключения АРМ с установленными средствами электронной подписи к сетям связи общего пользования необходимо ограничить возможность запуска и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX и т.д.), полученных из сетей общего пользования. Не допускается открывать такие файлы без проведения соответствующих проверок антивирусными средствами на предмет содержания в них программных закладок и вредоносных программ.

3.2. Порядок обращения с носителями ключевой информации.

При использовании и хранении ключей электронной подписи должен быть определен и утвержден порядок учета, хранения и использования носителей ключевой информации (ключевых носителей), содержащих ключи электронной подписи, который должен исключать возможность несанкционированного доступа к ним.

Для хранения ключевых носителей в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами.

В качестве ключевых носителей рекомендуется использовать учтенные в установленном порядке сертифицированные ключевые носители USB-ключи и смарт-карты.

При хранении и использовании ключей электронной подписи пользователю СКЗИ запрещается:

выполнять копирование ключа электронной подписи на иные ключевые носители без разрешения администратора информационной безопасности;

знакомить с содержанием ключевых носителей или передавать ключевые носители иным лицам;

устанавливать ключевой носитель в другие АРМ, не предназначенные для работы с ключевой информацией;

записывать на ключевой носитель постороннюю информацию;

использовать ранее использовавшиеся ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации с использованием сертифицированных средств электронной подписи либо средств, гарантирующих практическую невозможность восстановления информации с ключевых носителей.

Владелец ключа электронной подписи (владелец сертификата) обязан:

хранить в тайне ключ электронной подписи;

немедленно обратиться в удостоверяющий центр для приостановления действия сертификата ключа проверки электронной подписи или его отзыва в случае

компрометации ключа электронной подписи или при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

не использовать ключ проверки электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который отозван или действие которого приостановлено.

3.3. Учет и контроль выполнения требований информационной безопасности и порядка использования средств электронной подписи.

Действия, связанные с хранением и эксплуатацией средств электронной подписи и ключей электронной подписи, должны фиксироваться в журналах поэкземплярного учета, ведение которого осуществляется администратором информационной безопасности в соответствии с Инструкцией ФАПСИ № 152.

Администратор информационной безопасности должен периодически, не реже одного раза в два месяца, проводить проверку установленного программного обеспечения, журналов аудита операционной системы и средств защиты информации на всех АРМ пользователей СКЗИ, осуществлять контроль за условиями использования и хранения ключевых носителей, а также проводить периодическое тестирование технических и программных средств защиты информации.

В случае обнаружения постороннего программного обеспечения, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на АРМ должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией, назначенной руководителем организации, а также организованы работы по анализу и устранению выявленных нарушений.