Правила по обеспечению информационной безопасности на рабочем месте

1. Введение

Настоящие правила предназначены для обязательного ознакомления выделенному в организации сотруднику, отвечающему за информационную безопасность при использовании средств криптографической защиты информации и работе в защищенной телекоммуникационной системе.

2. Основные понятия

Система − автоматизированная информационная система передачи и приема информации в электронном виде по телекоммуникационным каналам связи в виде юридически значимых электронных документов с использованием средств электронной подписи.

Автоматизированное рабочее место (АРМ) – ПЭВМ, с помощью которой пользователь осуществляет подключение для работы в Системе.

Средство криптографической защиты информации (СКЗИ) − средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Электронная подпись (ЭП) − информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. В Системе для подписания электронных документов электронной подписью используется технология электронно-цифровой подписи (ЭЦП) в инфраструктуре открытых ключей.

Ключ ЭП - уникальная последовательность символов, предназначенная для создания электронной подписи. Ключ ЭП хранится пользователем системы в тайне. В инфраструктуре открытых ключей соответствует закрытому ключу ЭЦП.

Ключ проверки ЭП - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи. Ключ проверки ЭП известен всем пользователям системы и позволяет определить автора подписи и достоверность электронного документа, но не позволяет вычислить ключ электронной подписи. Ключ проверки ЭП считается принадлежащим пользователю, если он был ему выдан установленным порядком. В инфраструктуре открытых ключей соответствует открытому ключу ЭЦП.

Сертификат ключа проверки ЭП - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Удостоверяющий центр - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законодательством.

Владелец сертификата ключа проверки ЭП - лицо, которому в установленном порядке выдан сертификат ключа проверки электронной подписи.

Средства ЭП − шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Сертификат соответствия − документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям.

Подтверждение подлинности электронной подписи в электронном документе − положительный результат проверки соответствующим средством ЭП принадлежности электронной подписи в электронном документе владельцу сертификата ключа проверки подписи и отсутствия искажений в подписанном данной электронной подписью электронном документе.

Компрометация ключа − утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей, относятся, включая, но не ограничиваясь, следующие:

- Потеря ключевых носителей.
- Потеря ключевых носителей с их последующим обнаружением.
- Увольнение сотрудников, имевших доступ к ключевой информации.
- Нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа.
- Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.
- Нарушение печати на сейфе с ключевыми носителями.
- Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).

3. Риски использования электронной подписи

При использовании электронной подписи существуют определенные риски, основными из которых являются следующие:

1. Риски, связанные с аутентификацией (подтверждением подлинности) пользователя. Лицо, на которого указывает подпись под документом, может заявить о том, что подпись сфальсифицирована и не принадлежит данному лицу.
2. Риски, связанные с отрекаемостью (отказом от содержимого документа). Лицо, на которое указывает подпись под документом, может заявить о том, что документ был изменен и не соответствует документу, подписанному данным лицом.
3. Риски, связанные с юридической значимостью электронной подписи. В случае судебного разбирательства одна из сторон может заявить о том, что документ с электронной подписью не может порождать юридически значимых последствий или считаться достаточным доказательством в суде.

4. Риски, связанные с несоответствием условий использования электронной подписи установленному порядку. В случае использования электронной подписи в порядке, не соответствующем требованиям законодательства или соглашений между участниками электронного взаимодействия, юридическая сила подписанных в данном случае документов может быть поставлена под сомнение.
5. Риски, связанные с несанкционированным доступом (использованием электронной подписи без ведома владельца). В случае компрометации ключа ЭП или несанкционированного доступа к средствам ЭП может быть получен документ, порождающий юридически значимые последствия и исходящий от имени пользователя, ключ которого был скомпрометирован.

Для снижения данных рисков или их избежания помимо определения порядка использования электронной подписи при электронном взаимодействии предусмотрен комплекс правовых и организационно-технических мер обеспечения информационной безопасности.

4. Общие принципы организации информационной безопасности в Системе

Криптографическая подсистема Системы опирается на отечественное законодательство в области электронной подписи, инфраструктуры открытых ключей и защиты информации, в том числе, на действующие ГОСТ и руководящие документы ФСБ и ФСТЭК, а также на международный стандарт X.509, определяющий принципы и протоколы, используемые при построении систем с открытыми ключами.

Инфраструктура открытых ключей − это система, в которой каждый пользователь имеет пару ключей − закрытый (секретный) и открытый. При этом по закрытому ключу можно построить соответствующий ему открытый ключ, а обратное преобразование неосуществимо или требует огромных временных затрат. Каждый пользователь Системы генерирует себе ключевую пару, и, сохраняя свой закрытый ключ в строгой тайне, делает открытый ключ общедоступным. С точки зрения инфраструктуры открытых ключей, шифрование представляет собой преобразование сообщения, осуществляемое с помощью открытого ключа получателя информации. Только получатель, зная свой собственный закрытый ключ, сможет провести обратное преобразование и прочитать сообщения, а больше никто сделать этого не сможет, в том числе − и сам отправитель шифрограммы. Электронная подпись в инфраструктуре открытых ключей − это преобразование сообщения с помощью закрытого ключа отправителя. Любой желающий может для проверки подписи провести обратное преобразование, применив общедоступный открытый ключ (ключ проверки ЭП) автора документа, но никто не сможет имитировать такой документ, не зная закрытого ключа (ключа ЭП) автора.

Обязательным участником любой инфраструктуры открытых ключей является Удостоверяющий центр, выполняющий функции центра доверия всей системы документооборота. При этом Удостоверяющий центр обеспечивает выполнение следующих основных функций:

- выпускает сертификаты ключей проверки электронных подписей и выдает их пользователям;
- выдает пользователям средства электронной подписи;
- создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;
- получает и обрабатывает сообщения о компрометации ключей; аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей, доверие к которым утрачено;

- ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования и обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов;
- проверяет уникальность ключей проверки электронных подписей в реестре сертификатов; осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей; определяет порядок разбора конфликтных ситуаций и доказательства авторства электронного документа.

Свою деятельность Удостоверяющий центр осуществляет в строгом соответствии с законодательством, собственным регламентом и соглашениями между участниками электронного взаимодействия. Благодаря соблюдению необходимых требований исключаются риски, связанные с юридической значимостью документов, подписанных электронной подписью, и снижаются риски несоответствия условий использования электронной подписи установленному порядку.

Сертификат ключа проверки ЭП заверяется электронной подписью Удостоверяющего центра и подтверждает факт владения того или иного участника документооборота тем или иным ключом проверки ЭП и соответствующим ему ключом ЭП. Благодаря сертификатам, пользователи Системы могут опознавать друг друга, а, кроме того, проверять принадлежность электронной подписи конкретному пользователю и целостность (неизменность) содержания подписанного электронного документа. Таким образом исключаются риски, связанные с подтверждением подлинности пользователя и отказом от содержимого документа.

Преобразования сообщений с использованием ключей достаточно сложны и производятся с помощью специальных средств электронной подписи. В Системе для этих целей используется СКЗИ, имеющее сертификат соответствия установленным требованиям как средство электронной подписи. Данное СКЗИ − это программное обеспечение, которое решает основные задачи защиты информации, а именно:

- обеспечение конфиденциальности информации − шифрование для защиты от несанкционированного доступа всех электронных документов, которые обращаются в Системе;
- подтверждение авторства документа – применение ЭП, которая ставится на все возникающие в Системе электронные документы; впоследствии она позволяет решать на законодательно закрепленной основе любые споры в отношении авторства документа;
- обеспечение неотрекаемости − применение ЭП и обязательное сохранение передаваемых документов на сервере Системы у отправителя и получателя; подписанный документ обладает юридической силой с момента подписания: ни его содержание, ни сам факт существования документа не могут быть оспорены никем, включая автора документа;
- обеспечение целостности документа − применение ЭП, которая содержит в себе хэш-значение (усложненный аналог контрольной суммы) подписываемого документа; при попытке изменить хотя бы один символ в документе или в его подписи после того, как документ был подписан, будет нарушена ЭП, что будет немедленно диагностировано;

- аутентификация участников взаимодействия в Системе − каждый раз при начале сеанса работы сервер Системы и пользователь предъявляют друг другу свои сертификаты и, таким образом, избегают опасности вступить в информационный обмен с анонимным лицом или с лицом, выдающим себя за другого.

Уровень защищенности Системы в целом равняется уровню защищенности в ее самом слабом месте. Поэтому, учитывая то, что система обеспечивает высокий уровень информационной безопасности на пути следования электронных документов между участниками документооборота, для снижения или избежания рисков необходимо так же тщательно соблюдать меры безопасности непосредственно на рабочих местах пользователей.

В следующем разделе содержатся требования и рекомендации по основным мерам информационной безопасности на рабочем месте пользователя.

5. Требования и рекомендации по обеспечению информационной безопасности на рабочем месте пользователя

Рабочее место пользователя Системы использует СКЗИ для обеспечения целостности, конфиденциальности и подтверждения авторства информации, передаваемой в рамках Системы. Порядок обеспечения информационной безопасности при работе в Системе определяется руководителем организации, подключающейся к Системе, на основе рекомендаций по организационно-техническим мерам защиты, изложенным в данном разделе, эксплуатационной документации на СКЗИ, а также действующего российского законодательства в области защиты информации.

5.1 Персонал

Должен быть определен и утвержден список лиц, имеющих доступ к ключевой информации.

К работе на АРМ с установленным СКЗИ допускаются только определенные для эксплуатации лица, прошедшие соответствующую подготовку и ознакомленные с пользовательской документациеи˘ на СКЗИ, а также другими нормативными документами по использованию электронной подписи.

К установке общесистемного и специального программного обеспечения, а также СКЗИ, допускаются доверенные лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее ПО и на СКЗИ.

Рекомендуется назначение в организации, эксплуатирующей СКЗИ, администратора безопасности, на которого возлагаются задачи организации работ по использованию СКЗИ, выработки соответствующих инструкций для пользователей, а также контролю за соблюдением требований по безопасности.

Должностные инструкции пользователей АРМ и администратора безопасности должны учитывать требования настоящих Правил.

В случае увольнения или перевода в другое подразделение (на другую должность), изменения функциональных обязанностей сотрудника, имевшего доступ к ключевым носителям (ЭП и шифрования), должна быть проведена смена ключей, к которым он имел доступ.

5.2 Размещение технических средств АРМ с установленным СКЗИ

Должно быть исключено бесконтрольное проникновение и пребывание в помещениях, в которых размещаются технические средства АРМ, 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.

Рекомендуется использовать АРМ с СКЗИ в однопользовательском режиме. В отдельных случаях, при необходимости использования АРМ несколькими лицами, эти лица должны обладать равными правами доступа к информации.

Не допускается оставлять без контроля АРМ при включенном питании и загруженном программном обеспечении СКЗИ после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение экранной заставки, защищенной паролем. В отдельных случаях при невозможности использования парольной защиты, допускается загрузка ОС без запроса пароля, при этом должны быть реализованы дополнительные организационно-режимные меры, исключающие несанкционированный доступ к АРМ.

Рекомендуется предусмотреть меры, исключающие возможность несанкционированного изменения аппаратной части АРМ, например, опечатывание системного блока АРМ администратором. Также возможно в этих целях применение специальных средств защиты информации - аппаратных модулей доверенной загрузки.

Рекомендуется принять меры по исключению вхождения лиц, не ответственных за администрирование АРМ, в режим конфигурирования BIOS (например, с использованием парольноиˇ защиты).

Рекомендуется определить в BIOS установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске: отключается возможность загрузки с гибкого диска, привода CD-ROM, исключаются прочие нестандартные виды загрузки ОС, включая сетевую загрузку.

Средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты.

5.3 Установка программного обеспечения на АРМ

На технических средствах АРМ с установленным СКЗИ необходимо использовать только лицензионное программное обеспечение фирм-изготовителей, полученное из доверенных источников.

На АРМ должна быть установлена только одна операционная система. При этом не допускается использовать нестандартные, измененные или отладочные версии операционной системы.

Не допускается установка на АРМ средств разработки и отладки программного обеспечения. Если средства отладки приложений необходимы для технологических потребностей пользователя, то их использование должно быть санкционировано администратором безопасности. В любом случае запрещается использовать эти средства для просмотра и редактирования кода и памяти приложений, использующих СКЗИ. Необходимо исключить попадание в систему средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам, а также программ, позволяющих, пользуясь ошибками ОС, получать привилегии администратора.

Рекомендуется ограничить возможности пользователя запуском только тех приложений, которые разрешены администратором безопасности.

Рекомендуется установить и использовать на АРМ антивирусное программное обеспечение.

Необходимо регулярно отслеживать и устанавливать обновления безопасности для программного обеспечения АРМ (Service Packs, Hot fix и т.п.), обновлять антивирусные базы.

5.4 Настройка операционной системы АРМ

Администратор безопасности должен сконфигурировать операционную систему, в среде которои˘ планируется использовать СКЗИ, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

- правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности.
- всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права.
- У группы Everyone должны быть удалены все привилегии.
- Рекомендуется исключить использование режима автоматического входа пользователя в операционную систему при ее загрузке.
- рекомендуется переименовать стандартную учетную запись Administrator.
- Должна быть отключена учетная запись для гостевого входа Guest.
- исключить возможность удаленного управления, администрирования и модификации ОС и ее¨ настроек, системного реестра, для всех, включая группу Administrators.
- все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.).
- Должно быть исключено или ограничено с учетом выбранной в организации политики безопасности использование пользователями сервиса Scheduler (планировщик задач). При использовании данного сервиса состав запускаемого программного обеспечения на АРМ согласовывается с администратором безопасности.
- рекомендуется организовать затирание временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это невыполнимо, то ОС должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;
- Должны быть установлены ограничения на доступ пользователей к системному реестру в соответствии с принятой в организации политикой безопасности, что реализуется при помощи ACL или установкой прав доступа при наличие NTFS.
- На все директории, содержащие системные файлы Windows и программы из комплекта СКЗИ, должны быть установлены права доступа, запрещающие запись всем пользователям, кроме Администратора (Administrator), Создателя/Владельца (Creator/Owner) и Системы (System).
- Должна быть исключена возможность создания аварийного дампа оперативной памяти, так как он может содержать криптографически опасную информацию.
- Рекомендуется обеспечить ведение журналов аудита в ОС, при этом она должна быть настроена на завершение работы при переполнении журналов.
- Рекомендуется произвести настройку параметров системного реестра в соответствии с эксплуатационной документацией на СКЗИ.

Рекомендуется 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 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;
- личный пароль пользователь не имеет права сообщать никому;
- не допускается хранить записанные пароли в легкодоступных местах;
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев.
- Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС.

5.5 Установка и настройка СКЗИ

Установка и настроик̆а СКЗИ на АРМ должна выполняться в присутствии администратора, ответственного за работоспособность АРМ.

Установка СКЗИ на АРМ должна производиться только с дистрибутива, полученного по доверенному каналу.

Установка СКЗИ и первичная инициализация ключевой информации осуществляется в соответствии с эксплуатационной документацией на СКЗИ.

При установке ПО СКЗИ на АРМ должен быть обеспечен контроль целостности и достоверность дистрибутива СКЗИ.

Рекомендуется перед установкой произвести проверку ОС на отсутствие вредоносных программ с помощью антивирусных средств.

По завершении инициализации осуществляются настройка и контроль работоспособности ПО.

Запрещается вносить какие-либо изменения, не предусмотренные эксплуатационной документацией, в программное обеспечение СКЗИ.

5.6 Подключение АРМ к сетям общего пользования

При использовании СКЗИ на АРМ, подключенных 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. В качестве такой меры рекомендуется установка и использование на АРМ средств межсетевого экранирования. Должен быть закрыт доступ ко всем неиспользуемым сетевым портам.

В случае подключения АРМ 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.

5.7 Обращение с ключевыми носителями

В организации должен быть определен и утвержден порядок учета, хранения и использования носителей ключевой информации с ключами ЭП и шифрования, который должен исключать возможность несанкционированного доступа к ним.

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

Запрещается:

- Снимать несанкционированные администратором безопасности копии с ключевых носителей.
- Знакомить с содержанием ключевых носителей или передавать ключевые носители лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей (монитор) АРМ или принтер.
- Устанавливать ключевой носитель в считывающее устройство ПЭВМ АРМ в режимах, не предусмотренных функционированием системы, а также устанавливать носитель в другие ПЭВМ.
- Записывать на ключевой носитель постороннюю информацию.

5.8 Обращение с ключевой информацией

Владелец сертификата ключа проверки ЭП обязан:

- Хранить в тайне ключ ЭП (закрытый ключ).
- Не использовать для электронной подписи и шифрования ключи, если ему известно, что эти ключи используются или использовались ранее.
- Немедленно требовать приостановления действия сертификата ключа проверки ЭП при наличии оснований полагать, что тайна ключа ЭП (закрытого ключа) нарушена (произошла компрометация ключа).
- Обновлять сертификат ключа проверки ЭП в соответствии с установленным регламентом.

5.9 Учет и контроль

Действия, связанные с эксплуатацией СКЗИ, должны фиксироваться в «Журнале пользователя сети», который ведет лицо, ответственное за обеспечение информационной безопасности на АРМ. В журнал кроме этого записываются факты компрометации ключевых документов, нештатные ситуации, происходящие в системе и связанные с использованием СКЗИ, проведение регламентных работ, данные о полученных у администратора безопасности организации ключевых носителях, нештатных ситуациях, произошедших на АРМ, с установленным ПО СКЗИ.

В журнале может отражаться следующая информация:

- дата, время;
- запись о компрометации ключа;
- запись об изготовлении личного ключевого носителя пользователя, идентификатор носителя;
- запись об изготовлении копий личного ключевого носителя пользователя, идентификатор носителя;
- запись об изготовлении резервного ключевого носителя пользователя, идентификатор носителя
- запись о получении сертификата ключа проверки ЭП, полный номер ключевого носителя, соответствующий сертификату;

- записи, отражающие выдачу на руки пользователям (ответственным исполнителям) и сдачу ими на хранение личных ключевых носителей, включая резервные ключевые носители;
- события, происходившие на АРМ пользователя с установленным ПО СКЗИ, с указанием причин и предпринятых действий.

Пользователь (либо администратор безопасности) должен периодически (не реже одного раза в два месяца) проводить контроль целостности и легальности установленных копий ПО на всех АРМ со встроенной СКЗИ с помощью программ контроля целостности, просматривать сообщения о событиях в журнале EventViewer операционной системы, а также проводить периодическое тестирование технических и программных средств защиты.

В случае обнаружения "посторонних" (не зарегистрированных) программ, 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, где произошло нарушение, и организованы работы по анализу и ликвидации негативных последствии˘данного нарушения.

Рекомендуется организовать на АРМ систему аудита в соответствии с политикои˘безопасности, принятой в организации, с регулярным анализом результатов аудита.

6. Заключение

Настоящие правила составлены на основе:

- Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- приказа ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции 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»;
- приказа ФСБ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
- эксплуатационной документации на СКЗИ, которое используется в Системе