РУКОВОДСТВО

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

Настоящее руководство предназначено для обязательного ознакомления сотрудникам, отвечающим за информационную безопасность при использовании средств криптографической защиты информации и непосредственно использующим средства криптографической защиты информации.

Настоящее руководство создано с учетом:

- 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.

I. Термины и определения

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.

Ключ ЭП - уникальная последовательность символов, предназначенная для создания электронной подписи. Ключ ЭП хранится пользователем системы в тайне.

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 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 Удостоверяющим центром порядком.

Сертификат ключа проверки ЭП - электронный документ или документ на бумажном носителе, выданные Удостоверяющим центром Общество с ограниченной ответственностью «НОВАГ-СЕРВИС», либо доверенным лицом Удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Удостоверяющий центр (УЦ) - юридическое лицо Общество с ограниченной ответственностью «НОВАГ-СЕРВИС», осуществляющее 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 (нарушение конфиденциальности ключа) − утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей, относятся, включая, но не ограничиваясь, следующие:

- утеря ключевых носителей. В том числе с их последующим обнаружением;
- нарушение правил хранения и уничтожения (после окончания срока действия) ключа ЭП;
- возникновение подозрений на утечку информации или ее искажение в любой;
- нарушение печати на сейфе с ключевыми носителями;
- любые 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 действий злоумышленника).

II. Условия и о порядок использования электронных подписей

Обязанности владельца квалифицированного сертификата ключа проверки ЭП:

1. Обеспечить конфиденциальность ключей ЭП;
2. Применять для формирования ЭП только действующий ключ ЭП;
3. Не применять ключ ЭП при наличии оснований полагать, что он был скомпрометирован;
4. Применять ключ ЭП с учетом ограничений, содержащихся в сертификате ключа проверки ЭП (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки ЭП), если такие ограничения были установлены;

5. Немедленно обратиться в УЦ ООО «НОВАГ-СЕРВИС» любым способом с заявлением о прекращение действия сертификата ключа проверки ЭП в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.
6. Не использовать ключ ЭП, связанный с сертификатом ключа проверки ЭП, заявление на прекращение действия которого подано в УЦ ООО «НОВАГ-СЕРВИС», в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в УЦ по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия;
7. Не использовать ключ ЭП, связанный с сертификатом ключа проверки ЭП, который аннулирован или действие которого прекращено;
8. Использовать для создания и проверки квалифицированных ЭП, создания ключей ЭП и ключей проверки ЭП сертифицированные в соответствии с правилами сертификации Российской Федерации средства ЭП.

III. Условия и о порядок использования средств квалифицированной электронной подписи

Средства квалифицированной ЭП должны применяться владельцем квалифицированного сертификата ключа проверки ЭП в соответствии с положениями эксплуатационной документации на применяемое средство квалифицированной ЭП.

IV. Риски использования электронной подписи

При использовании ЭП существуют риски, основными из которых являются следующие:

- риски, связанные с аутентификацией (подтверждением подлинности) пользователя. Лицо, на которого указывает подпись в документе, может заявить, что подпись сфальсифицирована и ему не принадлежит;
- риски, связанные с отрекаемостью (отказом от содержимого документа). Лицо, на которое указывает подпись в документе, может заявить, что документ был изменен и не соответствует тому документу, который был им подписан;
- риски, связанные с юридической значимостью ЭП. В случае судебного разбирательства любая из сторон может заявить, что документ с ЭП не может порождать юридически значимых последствий или считаться достаточным доказательством в суде;
- риски, связанные с несоответствием условий использования ЭП установленному порядку. В случае использования ЭП в порядке, не соответствующем требованиям законодательства и/или соглашений между участниками электронного взаимодействия, юридическая сила подписанных в данном случае документов может быть поставлена под сомнение;
- риски, связанные с несанкционированным доступом (использованием ЭП без ведома владельца). В случае компрометации ключа ЭП и/или несанкционированного доступа к средствам ЭП может быть получен документ, порождающий юридически значимые последствия и исходящий от имени пользователя, ключ которого был скомпрометирован.

Во избежание данных рисков помимо определения порядка использования электронной подписи при электронном взаимодействии предусмотрены правовые и организационно-технические мероприятия по обеспечения информационной безопасности.

V. Организационно-технические мероприятия, необходимые для обеспечения безопасности ЭП и их проверки

1. Требования и рекомендации по обеспечению информационной безопасности на рабочем месте владельца квалифицированного сертификата:

Рабочее место владельца квалифицированного сертификата использует СКЗИ для обеспечения целостности, конфиденциальности и подтверждения авторства информации. Порядок обеспечения информационной безопасности определяется руководителем организации, сотрудник которой получает квалифицированный сертификат, на основе рекомендаций по организационно-техническим мерам защиты, изложенным в данном Руководстве, эксплуатационной документации на СКЗИ, а также действующем российском законодательстве в области защиты информации.

Должен быть определен и утвержден список лиц, имеющих доступ к ключевым носителям.

К работе с установленным СКЗИ допускаются только определенные для эксплуатации лица, прошедшие соответствующую подготовку и ознакомленные с пользовательской документацией 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 и администратора безопасности должны учитывать требования настоящего Руководства.

2. Размещение технических средств с установленным СКЗИ:

Должно быть исключено бесконтрольное проникновение и пребывание в помещениях, в которых размещаются технические средства, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе с СКЗИ. В случае необходимости присутствия таких лиц должен быть обеспечен контроль за их действиями.

Рекомендуется использовать СКЗИ в однопользовательском режиме.

Не допускается оставлять без контроля при включенном питании и загруженном программном обеспечении СКЗИ после ввода ключевой информации. При уходе владельца квалифицированного сертификата со своего рабочего места должно использоваться автоматическое включение экранной заставки, защищенной паролем. В отдельных случаях (при невозможности использования парольной защиты) допускается загрузка операционной системы без запроса пароля, однако при этом должны быть реализованы дополнительные организационно-технические меры, исключающие несанкционированный доступ.

Рекомендуется предусмотреть возможность исключить несанкционированное изменения аппаратной части компьютера. Например, опечатыванием системного блока администратором. Также возможно применение специальных сертифицированных средств защиты информации - аппаратных модулей доверенной загрузки (например, электронные замки «Соболь» или «Аккорд»).

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

Рекомендуется выставить в BIOS установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске (отключить возможность загрузки с гибкого диска, CD-ROM, USB и прочие нестандартные виды загрузки операционных систем).

Средствами BIOS исключить возможность работы на компьютере, если во время его начальной загрузки не проходят встроенные тесты.

3. Установка программного обеспечения на АРМ

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

На компьютере должна быть установлена только одна операционная система.

Не допускается установка средств разработки и отладки программного обеспечения. Если средства отладки приложений необходимы для технологических потребностей пользователя, то их использование должно быть разрешено администратором безопасности. При этом 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 своевременно обновляемое антивирусное программное обеспечение.

Регулярно отслеживать и устанавливать обновления безопасности для программного обеспечения (Service Packs, Hot fix и т.п.).

4. Настройка операционной системы АРМ

Администратор безопасности должен настроить операционную систему, в которой планируется использовать СКЗИ, и осуществлять контроль сделанных настроек в соответствии со следующими требованиями:

- правом установки и настройки операционной системы и СКЗИ должен обладать только администратор безопасности;
- всем пользователям и группам 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 операционной системы 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 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, 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 и 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;
- 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. Установка и настройка СКЗИ

Установка и настройка СКЗИ должна выполняться в присутствии администратора, ответственного за работоспособность компьютера и только с дистрибутива, полученного по доверенному каналу.

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

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

Перед установкой требуется произвести проверку ОС на отсутствие вредоносных программ с помощью актуальных антивирусных средств.

По завершении инициализации осуществляются настройка и контроль работоспособности ПО.

6. Запрещается вносить какие-либо изменения, не предусмотренные эксплуатационной документацией, в программное обеспечение СКЗИ. Подключение АРМ к сетям общего пользования

При использовании СКЗИ на компьютерах, 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 средств межсетевого экранирования. Должен быть закрыт доступ ко всем неиспользуемым сетевым портам.

В случае подключения компьютера 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.

7. Обращение с ключевыми носителями

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 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;
- устанавливать ключевой носитель в считывающее устройство в режимах, не предусмотренных функционированием системы, а также устанавливать носитель в других компьютерах;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ.
-

8. Обращение с ключевой информацией

Владелец сертификата ключа проверки ЭП обязан:

- хранить в тайне ключ ЭП;
- не использовать для ЭП и шифрования ключи, если ему известно, что эти ключи используются или использовались ранее;
- немедленно требовать отзыва 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.
-

9. Учет и контроль

Действия, связанные с эксплуатацией СКЗИ, должны фиксироваться в журнале, который ведет лицо, ответственное за обеспечение информационной безопасности. 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.

В журнале рекомендуется отражать следующую информацию:

- 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 с установленным ПО СКЗИ, с указанием причин и предпринятых действий.

Пользователь и/или администратор безопасности должны периодически, не реже одного раза в два месяца, проводить контроль целостности и легальности установленных копий ПО на всех компьютерах с установленными СКЗИ с помощью программ контроля целостности, просматривать сообщения о событиях в журнале операционной системы, а также проводить периодическое тестирование технических и программных средств защиты.

В случае обнаружения "посторонних" и/или 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 последствий данного нарушения.

Ознакомлен(а) _____ / _____

«____»_____.201__г.