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 цифровой подписи.

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

Электронная цифровая подпись (ЭЦП) − реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Средства ЭЦП − аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций − создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

Сертификат средства ЭЦП − документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средства ЭЦП установленным требованиям.

Закрытый ключ ЭЦП − уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств ЭЦП.

Открытый ключ ЭЦП − уникальная последовательность символов, соответствующая закрытому ключу ЭЦП, доступная любому пользователю информационной системы и предназначенная для подтверждения использованием средств ЭЦП подлинности электронной цифровой подписи в электронном документе.

Сертификат ключа подписи (сертификат) − документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, включающий в себя открытый ключ шифрования и/или ЭЦП, которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи, идентификации владельца сертификата ключа подписи и/или обеспечения конфиденциальности информации.

Владелец сертификата (пользователь) − физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств ЭЦП создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Подтверждение подлинности электронной цифровой подписи в электронном документе − положительный результат проверки соответствующим сертифицированным средством ЭЦП с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанного данной электронной цифровой 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) секретного 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. Общие принципы организации защиты информации в Системе

Криптографическая подсистема Системы опирается на отечественное законодательство в области 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 − секретный (закрытый) и открытый. При этом по секретному ключу можно построить соответствующий ему открытый ключ, а обратное преобразование неосуществимо или требует огромных временных затрат. Каждый пользователь системы генерирует себе секретный ключ, вычисляет по нему открытый ключ, и, сохраняя свой секретный 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 секретный ключ, сможет провести обратное преобразование и прочитать сообщения, а больше никто сделать этого не сможет, в том числе − и сам отправить шифрограммы. Электронная подпись в инфраструктуре открытых ключей − это преобразование сообщение с помощью секретного ключа отправителя. Любой желающий может провести обратное преобразование, применив общедоступный открытый ключ автора документа, но никто не сможет имитировать такой документ, не зная закрытого ключа автора.

Обязательным участником любой инфраструктуры открытых ключей является Удостоверяющий центр − программно-аппаратный комплекс и система мероприятий, выполняющие функции центра доверия всей системы документооборота. Главная задача Удостоверяющего центра заключается в выпуске сертификатов открытых ключей пользователей системы документооборота. Сертификат открытого ключа − это электронный документ, заверенный электронной подписью Удостоверяющего центра и заверяющий факт владения того или иного участника документооборота тем или иным открытым ключом. Благодаря сертификатам, пользователи системы могут опознавать друг друга, а, кроме того, проверять принадлежность электронной подписи конкретному абоненту и целостность (неизменность) содержания подписанного электронного документа.

Преобразования сообщений с использованием ключей достаточно сложны и производятся автоматически с помощью специальных программ. В Системе для этих целей используется СКЗИ «КриптоПро CSP»[1]. СКЗИ «КриптоПро CSP» − это программа, которая решает основные задачи защиты информации, а именно:

- защита от несанкционированного доступа − автоматическое шифрование всех электронных документов, которые обращаются в системе;

- подтверждение авторства документа – применение ЭЦП, которая автоматически ставится на все возникающие в системе электронные документы; которая позволяет в последствии решать на законодательно закрепленной основе любые споры в отношении авторства документа;

- обеспечение неотрекаемости документа − применение ЭЦП и обязательное автоматическое резервное копирование всех документов на сервере системы, у отправителя и получателя; подписанный документ обладает юридической силой с самого момента подписания и ни его содержание, ни сам факт существования документа не могут быть оспорены никем, включая автора документа;

[1] В некоторых системах используется СКЗИ «Крипто-Про JSP», аналогичные по функциям СКЗИ «КриптоПро CSP».

- обеспечения целостности документа − применение ЭЦП, 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 ЭЦП, что будет немедленно диагностировано;

- аутентификация пользователя в системе − каждый раз при начале сеанса работы сервер системы и пользователь автоматически 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 информации в Системе в целом равняется уровню защищенности информации в самом слабом месте системы, которым является рабочее место пользователя. За сохранность информации до того момента, как она начинает обрабатываться в системе, несет ответственность только ее владелец, и в его силах обезопасить себя от возможных негативных последствий, связанных с утечкой, разглашением или искажением данных.

4. Порядок действий пользователя

Автоматизированное рабочее место пользователя Системы использует СКЗИ для обеспечения целостности, авторства и конфиденциальности информации, передаваемой в рамках информационной системы.

Порядок обеспечения информационной безопасности при работе в Системе определяется организацией, подключающейся к Системе, на основании действующего российского законодательства в области защиты информации.

Владелец сертификата ключа обязан:

- Не использовать для электронной цифровой подписи и шифрования открытые и закрытые ключи, если ему известно, что эти ключи используются или использовались ранее.

- Хранить в тайне закрытый ключ.

- Немедленно требовать приостановления действия сертификата ключа при наличии оснований полагать, что тайна закрытого ключа нарушена (компрометация ключа).

- Обновлять сертификат ключа подписи в соответствии с установленным регламентом.

Рекомендуется:
Установка и настройка СКЗИ на Автоматизированное рабочее место (АРМ) должна выполняться в присутствии администратора. Перед установкой необходимо проверить целостность программного обеспечения СКЗИ. Запрещается устанавливать СКЗИ, целостность которого нарушена.

5. Рекомендуемые организационно-технические меры по обеспечению информационной безопасности в организации

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

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

Для хранения носителей закрытых ключей ЭЦП и шифрования в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами с двумя экземплярами ключей (один у исполнителя, другой в службе безопасности).

Использовать АРМ со встроенными средствами криптографической защиты в однопользовательском режиме. В отдельных случаях, при необходимости использования АРМ несколькими лицами, эти лица должны обладать равными правами доступа к информации.

При загрузке операционной системы и при возвращении после временного отсутствия пользователя на рабочем месте должен запрашиваться пароль, состоящий не менее чем из 6 символов. 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 этим АРМ.

Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых установлены технические средства АРМ со встроенными СКЗИ.

Должны быть предусмотрены меры, исключающие возможность несанкционированного изменения аппаратной части рабочей станции с установленными СКЗИ.

Установленное на АРМ программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.

Администрирование должно осуществляться доверенными лицами.

Средствами BIOS исключить возможность сетевой загрузки ОС рабочей станции.

Средствами BIOS исключать возможность работы на ПЭВМ, если во время ее начальной загрузки не проходят встроенные тесты.

Вхождение пользователей в режим конфигурирования BIOS штатными средствами BIOS должно осуществляться только с использованием парольной защиты при длине пароля не менее 6 символов.

При использовании ОС Windows 98/ME/NT/2000/XP/Vista все пользователи рабочей станции должны иметь право доступа ко всей конфиденциальной информации, обрабатываемой на этой станции.

При использовании ОС Windows NT/2000/XP/Vista принять меры, исключающие доступ пользователя к системному реестру.

Ограничить либо исключить использование программного продукта Scheduler (планировщик заданий), входящего в состав ОС Windows. При использовании Scheduler состав запускаемого программного обеспечения на АРМ согласовывается с администратором безопасности.

При использовании ОС Windows NT/2000/XP/Vista исключить возможность удаленного редактирования системного реестра пользователями (исключая администратора).

При использовании ОС Windows NT/2000/XP/Vista переименовать пользователя Administrator, отключить учетную запись для гостевого входа (Guest).

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

Не допускается:

- Снимать несанкционированные копии с ключевых носителей.
- Знакомить с содержанием ключевых носителей или передавать ключевые носители лицам, к ним не допущенным.
- Выводить секретные ключи на дисплей (монитор) ПЭВМ или принтер.
- Устанавливать ключевой носитель в считывающее устройство (дисковод) ПЭВМ АРМ, не предусмотренных функционированием системы, а также в другие ПЭВМ.
- Записывать на ключевой носитель постороннюю информацию.
- Хранить пароли в виде записей на бумажном носителе.

6. Учет действий по защите информационной безопасности

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

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 открытого ключа ЭЦП, 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.

Кроме того, в организации должен быть установлен порядок учета выдачи, обновления и хранения паролей.