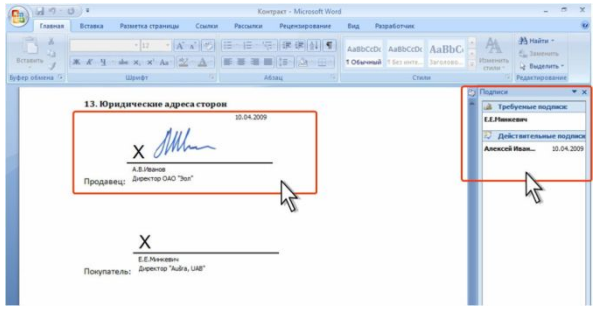
Техника безопасности при обслуживании информационных систем.

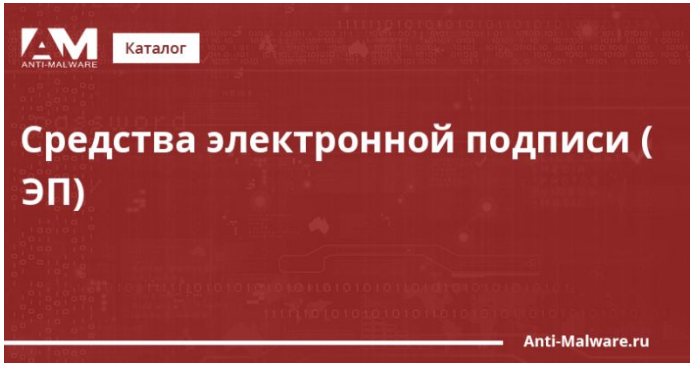
СКЗИ (средство криптографической защиты информации) — это программа или устройство, которое шифрует документы и генерирует электронную подпись (ЭП). Все операции производятся с помощью ключа электронной подписи, который невозможно подобрать вручную, так как он представляет собой сложный набор символов. Тем самым обеспечивается надежная защита информации.

Электронная подпись — это информация в электронном виде, которая формируется при помощи уникальной комбинации символов и придает электронному документу юридическую силу. Электронная подпись обеспечивает конфиденциальность подписанной информации, определяет автора документа и позволяет контролировать изменения, внесенные в документ.

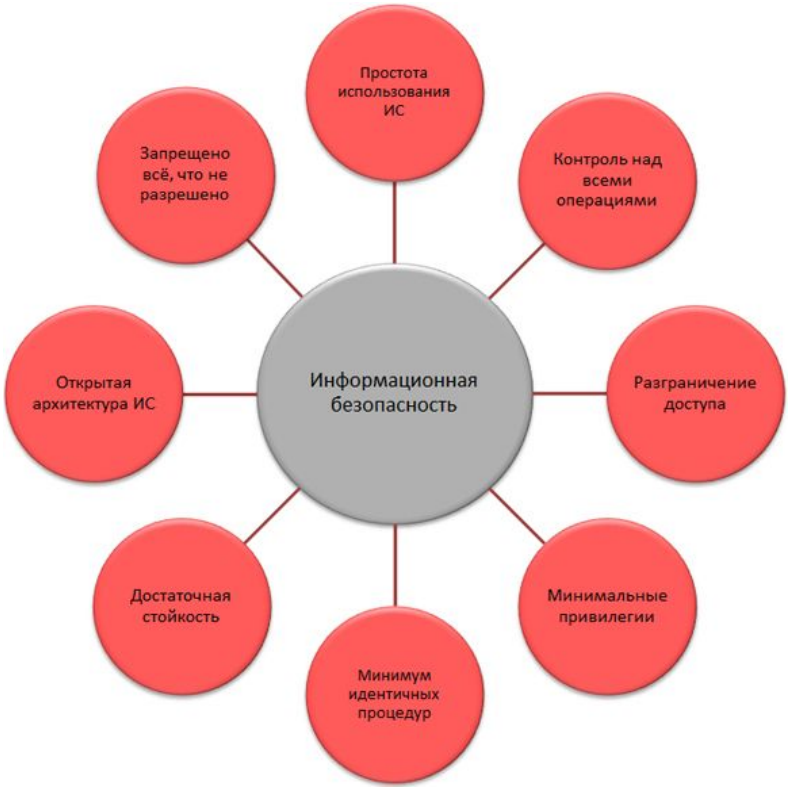


Закрытый ключ электронной подписи — это уникальная последовательность символов, применяемая для создания ЭП. *Открытый ключ* — это тоже уникальная последовательность символов для проверки оригинальности электронной подписи (распространяется свободно). Первый ключ хранится в тайне и имеется только у его владельца.

Средства электронной подписи (ЭП) — это специальные средства для криптографического преобразования данных, которые бывают программными, либо программно-аппаратными устройствами, необходимые для генерации электронной подписи (ЭП), ее проверки, создания ключей ЭП и ключей проверки подлинности электронной подписи.



Принципы информационной безопасности



1. Простота использования информационной системы. Данный принцип информационной безопасности заключается в том, что для минимизации ошибок следует обеспечить простоту использования информационной системы.

2. Контроль над всеми операциями. Этот принцип подразумевает непрерывный контроль состояния информационной безопасности и всех событий, влияющих на ИБ.

3. Запрещено всё, что не разрешено. Этот принцип ИБ заключается в том, что доступ к какому-либо объекту ИС должен предоставляться только при наличии соответствующего правила, отраженного, например, в регламенте бизнес-процесса или настройках защитного программного обеспечения.

4. Открытая архитектура ИС. Этот принцип информационной безопасности состоит в том, что безопасность не должна обеспечиваться через неясность.

5. Разграничение доступа. Данный принцип ИБ заключается в том, что каждому пользователю предоставляется доступ к информации и её носителям в соответствии с его полномочиями.

6. Минимальные привилегии. Принцип минимальных привилегий состоит в выделении пользователю наименьших прав и доступа к минимуму необходимых функциональных возможностей программ. Такие ограничения, тем не менее, не должны мешать выполнению работы.

7. Достаточная стойкость. Этот принцип информационной безопасности выражается в том, что потенциальные злоумышленники должны встречать препятствия в виде достаточно сложных вычислительных задач.

8. Минимум идентичных процедур. Этот принцип информационной безопасности состоит в том, что в системе ИБ не должно быть общих для нескольких пользователей процедур, таких как ввод одного и того же пароля. В этом случае масштаб возможной хакерской атаки будет меньше.

Требования и рекомендации по обеспечению информационной безопасности на рабочем месте пользователя

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 документацией на СКЗИ, а также другими нормативными документами по использованию электронной подписи.

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.

- Рекомендуется использовать АРМ с СКЗИ в однопользовательском режиме.

- Не допускается оставлять без контроля АРМ при включенном питании и загруженном программном обеспечении СКЗИ после ввода ключевой информации.

- Рекомендуется предусмотреть меры, исключающие возможность несанкционированного изменения аппаратной части АРМ

- Рекомендуется принять меры по исключению вхождения лиц, не ответственных за администрирование АРМ, в режим конфигурирования BIOS

- 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.

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.
- Не допускается установка на АРМ средств разработки и отладки программного обеспечения.
- 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.

Настройка операционной системы АРМ

- 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.

Установка и настройка СКЗИ

- Установка и настройка 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.

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.

Учет и контроль

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.