УЦ Тензор: Правила использования средств криптографической защиты информации и электронной подписи

1. Средства электронной подписи — шифровальные (криптографические) средства (СКЗИ), используемые для реализации хотя бы одной из следующих функций — создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки, имеющие подтверждение соответствия требованиям, установленным Федеральным законом от 06.04.2011 № 63–ФЗ «Об электронной подписи» СКЗИ и средства ЭП могут использоваться для защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.
2. Ключ электронной подписи (ключ ЭП) — уникальная последовательность символов, предназначенная для создания электронной подписи.

3. Для работы с СКЗИ и ключами ЭП привлекаются уполномоченные лица, назначенные соответствующим приказом руководителя организации. Данные должностные лица, уполномоченные соответствующим приказом руководителя организации, несут персональную ответственность за:

    - а. Сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с СКЗИ;
    - б. Сохранение в тайне содержания ключей ЭП и СКЗИ;
    - в. Сохранность носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями.
4. В организации должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.
5. Уполномоченные лица несут ответственность за то, чтобы на компьютере, на котором установлены СКЗИ, не были установлены и не эксплуатировались программы (в том числе, — вирусы), которые могут нарушить функционирование программных СКЗИ. При обнаружении на рабочем месте, оборудованном СКЗИ, посторонних программ или вирусов, нарушающих работу указанных средств, работа со средствами защиты информации на данном рабочем месте должна быть прекращена и должны быть организованы мероприятия по анализу и ликвидации негативных последствий данного нарушения.
6. Организация — обладатель конфиденциальной информации обязана вести журнал поэкземплярного учёта СКЗИ, эксплуатационной и технической документации к ним, ключевых документов в соответствии с п. 26 Приказа ФАПСИ от 13 июня 2001 года № 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». Неиспользованные или выведенные из действия ключевые документы подлежат уничтожению обладателем конфиденциальной информацией на месте, путём переформатирования ключевых носителей средствами ПО СКЗИ.

7. Не допускается:

    - а. разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;
    - б. вставлять ключевой носитель в ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной подписи и т.д.), а также в другие ПЭВМ;
    - в. записывать на ключевом носителе постороннюю информацию;
    - г. вносить какие–либо изменения в СКЗИ и ключ ЭП;
    - д. использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путём переформатирования (рекомендуется физическое уничтожение носителей);
    - е. оставлять без контроля аппаратные средства, на которых эксплуатируются средства электронной подписи;
    - ж. оставлять без контроля носители ключевой информации;
    - з. сообщать PIN–код к ключевому носителю кому бы то ни было;

8. Действия в случае компрометации ключей:

    - а. Под компрометацией ключей ЭП понимается их утрата (в том числе с их последующим обнаружением), хищение, разглашение, несанкционированное копирование, передача их по линии связи в открытом виде, увольнение по любой причине сотрудника, имеющего доступ к ключевым носителям или к ключевой информации на данных носителях, любые другие виды разглашения ключевой информации, в результате которых ключи ЭП могут стать доступными несанкционированным лицам и (или) процессам.
    - б. Владелец (уполномоченное лицо) самостоятельно должен определить факт компрометации ключа ЭП и оценить значение этого события для Владельца. Мероприятия по розыску и локализации последствий компрометации

конфиденциальной информации, переданной с использованием СКЗИ, организует и осуществляет сам владелец.
- в. При компрометации ключа ЭП, владелец ключа должен немедленно поставить в известность представителей Удостоверяющего центра о факте компрометации (контактная информация размещена на сайте https://tensor.ru/branches). Заявление на аннулирование сертификата может подаваться в Удостоверяющий центр в бумажной форме при личном прибытии Заявителя в офис удостоверяющего центра, либо почтовой или курьерской доставкой, а также в электронной форме через личный кабинет, с подписью руководителя или лица, имеющего право действовать от имени организации по доверенности. Не позднее 1 часа после поступления заявления на аннулирование ключа ЭП, сертификат проверки ключа ЭП будет аннулирован. Последующая разблокировка аннулированного сертификата ключа проверки ЭП не возможна.

Для получения новых ключей уполномоченный представитель организации, у которой были скомпрометированы ключи, должен обратиться в Удостоверяющий центр, имея при себе документы, необходимые для выпуска нового ключа ЭП. За выдачу новых ключей взимается оплата в соответствии с действующими тарифами на день оплаты.

9. PIN–код Владельца на носителе.

   - PIN–код для Рутокен, Рутокен ЭЦП 2.0 по умолчанию — 12345678.
   - PIN–код для eToken и JaCarta LT по умолчанию — 1234567890.
   - PIN–код для Jacarta PKI/ГОСТ и Jacarta–2 PKI/ГОСТ — 0987654321.

   Владелец обязан изменить PIN–код при первом использовании ключевого носителя.

   Надёжный PIN–код должен состоять из смешанного набора цифровых и буквенных символов.

10. Порядок установки и эксплуатации СКЗИ допускается в чётком соответствии с документацией на используемое СКЗИ: КриптоПро CSP, https://www.cryptopro.ru/.

Ссылки

Удостоверяющий центр - Тензор

https://sysadminmosaic.ru/ca_tensor/rules_mcpi-es

2019-06-28 13:21