Сведения об аккредитованном Удостоверяющем центре:
ООО «Такском»
Фактический адрес: г. Москва, Нагатинская, дом 1
Тел.: (495) 739-42-31
E-mail: security@taxcom.ru
Сайт: http://www.taxcom.ru

# 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 электронной подписи, 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. Пользователи СКЗИ** 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 со сведениями о ключах, выдаваемых с ключевыми носителями.

**4. Владельцем сертификата (юридическим лицом или ИП) должны быть обеспечены** условия хранения ключевых носителей ключей ЭП, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

**5. Владелец сертификата несёт 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, нужно прекратить использование средств защиты информации и организовать 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 г. № 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. Ключи квалифицированных электронных подписей по истечении сроков действия подлежат незамедлительному уничтожению. Для уничтожения ключей электронных подписей должны применяться прошедшие в установленном порядке процедуру оценки соответствия средства электронной подписи, в которых реализована функция уничтожения информации.

**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 ключевой носитель 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 сертификата (уполномоченное лицо) самостоятельно должен определить факт компрометации ключа ЭП и оценить значение этого события для Владельца сертификата. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием СКЗИ, организует и осуществляет сам Владелец сертификата;

**в.** При компрометации ключа ЭП Владелец сертификата должен немедленно поставить в известность представителей Удостоверяющего центра о факте компрометации. Заявление на аннулирование сертификата может подаваться в УЦ 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 лица, имеющего право действовать от имени организации без 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 невозможна. Для получения новых ключей уполномоченный представитель Заявителя, у которого были скомпрометированы ключи, должен обратиться в УЦ, 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 сертификата на носителе.**

PIN-код для Рутокен, Рутокен ЭЦП 2.0, Рутокен ЭЦП 3.0 по умолчанию – 12345678.

PIN-код для JaCarta LT по умолчанию – 1234567890.

PIN-код для Jacarta PKI/ГОСТ и Jacarta-2 PKI/ГОСТ – 0987654321.

Владелец сертификата 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 на сайте https://www.cryptopro.ru/.**

**11. В случае отсутствия у пользователя СКЗИ установочного модуля СКЗИ «КриптоПро CSP» последний может быть получен одним из ниже перечисленных способов:**

1. Дистрибутив на носителе (за дополнительную плату).

2. Посредством загрузки через Интернет.

На странице загрузки вместе с дистрибутивом и документацией размещается отделённая электронная подпись, для проверки которой необходимо использовать утилиту «cpverify», полученную доверенным образом и содержащую ключ проверки данной электронной подписи. Средство контроля целостности (cpverify.exe) первоначально должно быть получено пользователем на физическом носителе в офисе компании ООО «КРИПТО-ПРО» либо у официального дилера. Далее полученной доверенным образом признается очередная версия утилиты, полученная любым образом, например, скачанная с сайта www.cryptopro.ru, при условии, что она была проверена другим экземпляром утилиты, полученным ранее доверенным образом, и проверка была успешной.

**12. Пользователи допускаются к работе с СКЗИ после соответствующего обучения.**

Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники органа криптографической защиты – Лицензиата ФСБ (в соответствии с тарифами) – или обладателя конфиденциальной информации.