|  |
| --- |
| Приложение 2к приказу финансового управленияадминистрации Александровскогомуниципального района Пермского краяот 14.05.2019 N 24 |

**ПОЛОЖЕНИЕ**

**О ПОРЯДКЕ РАБОТЫ СО СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ**

1. Термины и определения

Аккредитованный удостоверяющий центр (УЦ) - это организация (или подразделение организации), прошедшая аккредитацию в соответствии с действующим законодательством, выпускающая сертификаты;

Аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона от 06.04.2011 г. N 63-ФЗ «Об электронной подписи».

Журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (журнал поэкземплярного учета СКЗИ) - документ, содержащий данные о выданных уполномоченным сотрудникам ключевых документах.

Квалифицированный сертификат ключа проверки электронной подписи (Сертификат) - электронный документ или документ на бумажном носителе, выданный УЦ либо федеральным органом исполнительной власти (уполномоченными в сфере использования ЭП) и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа.

Компрометация криптоключа - утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

Ключ электронной подписи (криптоключ, закрытый ключ, ключ ЭП) - уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи (открытый ключ) - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

Ключевой документ - ключевой носитель, содержащий ключ электронной подписи, а при необходимости - контрольную, служебную и технологическую информацию.

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключа электронной подписи.

Пользователь СКЗИ (пользователь) - физическое лицо Участника, непосредственно допущенное к работе со средствами криптографической защиты информации.

Система - Система автоматизации финансово-казначейских органов - Автоматизированный Центр Контроля исполнения бюджета ("АЦК-Финансы"), установленная в Министерстве финансов Пермского края.

Средства криптографической защиты информации (СКЗИ) - аппаратно-программный комплекс, выполняющий функцию создания ЭП, а также обеспечивающий защиту информации по утвержденным стандартам и сертифицированный в соответствии с действующим законодательством.

Квалифицированный сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданный УЦ либо федеральным органом исполнительной власти (уполномоченными в сфере использования ЭП) и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа.

Участник - юридическое лицо, принимающее участие в юридически значимом электронном документообороте.

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.

ЭП имеет следующие характеристики:

1. получена в результате криптографического преобразования информации с использованием ключа;

2. позволяет определить лицо, подписавшее электронный документ;

3. позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4. создается с использованием средств ЭП;

5. информация для проверки ЭП указана в квалифицированном сертификате ключа проверки ЭП;

6. для создания и проверки ЭП используются средства ЭП, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 06.04.2011 г. N 63-ФЗ "Об электронной подписи".

Электронный документ - документ, в котором информация представлена в электронной форме.

Юридически значимый электронный документооборот (ЮЗЭД) - документооборот на базе Системы, в котором участники ЮЗЭД совершают действия по принятию к исполнению документов в электронной форме, удостоверенных ЭП, и при этом несут ответственность за совершение либо несовершение этих действий.

2. Общие положения

Настоящее Положение регламентирует порядок работы со средствами криптографической защиты информации (СКЗИ) в соответствии с Приказом ФАПСИ от 13.06.2001 N 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», Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным Приказом ФСБ РФ от 09.02.2005 N 66.

3. Организация и обеспечение безопасности хранения

и применения СКЗИ

Ключевые документы или исходная информация для выработки ключевых документов изготавливаются УЦ или ответственным за эксплуатацию СКЗИ сотрудником Участника.

Пользователи СКЗИ обязаны:

не разглашать сведения о криптоключах;

соблюдать требования и рекомендации указанные производителем СКЗИ в сопроводительной документации;

сообщать ответственному за эксплуатацию СКЗИ сотруднику Участника, а также Организатору о ставших им известными попытках посторонних лиц получить сведения об используемых криптоключах или ключевых документах;

сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

при получении в пользование ключевого носителя изменить PIN-код пользователя. Изменение PIN-кода администратора производит ответственный за эксплуатацию СКЗИ сотрудник Участника;

немедленно уведомлять ответственного за эксплуатацию СКЗИ сотрудника Участника, а также организатора о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

4. Порядок обращения с СКЗИ и криптоключами к ним.

Мероприятия при компрометации криптоключей

Для организации и обеспечения безопасности хранения и применения ЭП следует использовать СКЗИ, предусматривающие запись ключей ЭП на электронные ключевые носители многократного (долговременного) использования.

Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету по установленной форме в соответствии с требованиями Положения ПКЗ-2005. При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование.

Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

[Журнал](#Par101) поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов ведет ответственный за эксплуатацию СКЗИ сотрудник Участника по форме согласно Приложению к настоящему Положению.

Все полученные ответственным за эксплуатацию СКЗИ сотрудником Участника экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета СКЗИ, несущим персональную ответственность за их сохранность.

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ и(или) ответственными за эксплуатацию СКЗИ сотрудниками Участника под расписку в соответствующих журналах поэкземплярного учета СКЗИ.

Пользователи СКЗИ хранят носители СКЗИ, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей СКЗИ указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

СКЗИ и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными нарочными из числа ответственных за эксплуатацию СКЗИ сотрудников Участника или пользователей СКЗИ, для которых они предназначены, при соблюдении мер, исключающих бесконтрольный доступ к ним во время доставки.

Эксплуатационную и техническую документацию к СКЗИ можно пересылать заказными или ценными почтовыми отправлениями.

Для пересылки СКЗИ ключевые документы должны быть помещены в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. СКЗИ пересылают отдельно от ключевых документов к ним. На упаковках указывают ответственного за эксплуатацию СКЗИ сотрудника Участника или пользователя СКЗИ, для которого эти упаковки предназначены. На упаковках делают пометку "Лично". Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.

Оформленную таким образом упаковку, при предъявлении фельдсвязью дополнительных требований, помещают во внешнюю упаковку, оформленную согласно предъявляемым требованиям. До первоначальной высылки (или возвращения) адресату сообщают отдельным письмом описание высылаемых ему упаковок и печатей, которыми они могут быть опечатаны.

Для пересылки СКЗИ, эксплуатационной и технической документации к ним, ключевых документов следует подготовить сопроводительное письмо, в котором необходимо указать, что посылается и в каком количестве, учетные номера изделий или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывают в одну из упаковок.

Полученные упаковки вскрывают только ответственный за эксплуатацию СКЗИ сотрудник Участника или пользователи СКЗИ, для которых они предназначены. Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получатель составляет акт, который высылает отправителю. Полученные с такими отправлениями СКЗИ и ключевые документы до получения указаний от отправителя применять не разрешается.

Получение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должно быть подтверждено отправителю в соответствии с порядком, указанным в сопроводительном письме. Отправитель обязан контролировать доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель должен направить ему запрос и принять меры к уточнению местонахождения отправлений.

Неиспользованные или выведенные из действия ключевые документы подлежат уничтожению на месте эксплуатации.

Уничтожение криптоключей (исходной ключевой информации) производится путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования. Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к СКЗИ уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в журнале поэкземплярного учета.

Ключевые документы уничтожаются либо пользователями СКЗИ, либо ответственным за эксплуатацию СКЗИ сотрудником Участника под расписку в журнале поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом. При этом, пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи.

Уничтожение по акту производит комиссия в составе не менее двух человек из числа сотрудников Участника, в том числе ответственного за эксплуатацию СКЗИ сотрудника. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих СКЗИ носителей, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делается отметка в журнале поэкземплярного учета СКЗИ.

Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ. О выводе криптоключей из действия сообщают в УЦ и финансовое управление администрации Александровского муниципального района Пермского края. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей, пользователи СКЗИ обязаны сообщать в УЦ и финансовое управление администрации Александровского муниципального района Пермского края. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

Порядок оповещения пользователей СКЗИ о предполагаемой компрометации криптоключей и их замене устанавливается соответствующим Регламентом оказания услуг УЦ.

5. Контроль за организацией и обеспечением безопасности

хранения и применения СКЗИ

Контроль за организацией и обеспечением безопасности хранения, эксплуатации, обработки и передачи по каналам связи информации с использованием СКЗИ - государственный контроль осуществляют уполномоченные федеральные органы. В ходе государственного контроля изучаются и оцениваются:

организация безопасности хранения, эксплуатации СКЗИ;

достигнутый уровень криптографической защиты информации;

условия использования СКЗИ.

|  |
| --- |
| Приложение к Положению о порядке работы со средствами криптографической защиты информации |

Журнал

поэкземплярного учета СКЗИ, эксплуатационной и технической

документации к ним, ключевых документов

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  N п/п |  Наименование  СКЗИ, эксплуатационной и технической  документации к  ним, ключевых  документов  | Серийные номера СКЗИ, эксплуатационнойи технической  документации к ним, номера  серий ключевых документов  | Отметка о получении | Отметка о выдаче |
| От кого получены | Дата и номер сопроводи-тельного письма  | Ф.И.О. ПользователяСКЗИ  | Дата и распискав получении  |
|  1  |  2  |  3  |  4  |  5  |  6  |  7  |

|  |  |  |
| --- | --- | --- |
|  Отметка о подключении  (установке) СКЗИ  | Отметка об изъятии СКЗИ изаппаратных средств, уничтожении(утрате) ключевых документов | Примечание |
| Ф.И.О. сотрудников пользователя СКЗИ, произведших подключение (установку)  | Дата подключения (установки) и подписи лиц, произведших подключение (установку)  | Номера аппаратных средств, в которыеустановлены или к которымподключены СКЗИ  | Дата изъятия (уничтожения, утери)  | Ф.И.О. сотрудников пользователя СКЗИ, производившихизъятие(уничтожение)/ Ф.И.О. пользователя СКЗИ, утратившего  | Номер акта илираспискаоб уничтожении (утере)  |
|  8  |  9  |  10  |  11  |  12  |  13  |  14  |