14

СОГАСОВАНО:
Председатель ПК
_____Т.Н. Малая

от «14» 01 2020г.

УТВЕРЖДЕНО:
Приказом заведующего
МБДОУ детского сада № 26
от «14» 01 2020г. № 63-од
_____Л. С. Леонтьева

ПОЛОЖЕНИЕ

О работе со средствами криптографической защиты информации в информационной системе МБДОУ детском саду № 26

1. Общие положения

Средства криптографической защиты информации (СКЗИ), в состав которых входят средства шифрования и электронной цифровой подписи (ЭЦП), предназначены для:

- заверения файлов электронных документов, циркулирующих в системе предоставления сведений о контрактах (изменениях), сведений об исполнении (прекращении действия) контрактов в электронном виде по каналам связи, электронной цифровой подписью и подтверждения ее подлинности;
- шифрования файлов для закрытия содержащейся в них информации от не санкционированного просмотра при передаче по открытым каналам связи и расшифровки их при поучении.

Средства шифрования и ЭЦП могут использоваться в системе для предоставления сведений о контрактах (изменениях) сведений об исполнении (прекращении действия) контрактов в электронном виде по

каналам связи (далее - система). Указанные средства могут использоваться для защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

2. Работа со средствами шифрования

Для работы с СКЗИ (средствами шифрования и ЭЦП) привлекаются уполномоченные лица, назначенные соответствующим приказом руководителя организации. Должностные лица, уполномоченные соответствующим приказом руководителя организации эксплуатировать СКЗИ, получать и использовать ключи шифрования и ЭЦП, несут персональную ответственность за:

- сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с СКЗИ;
- сохранение в тайне содержания закрытых ключей шифрования и ЭЦП;
- сохранность носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями.

В организации, предоставляющей сведений о контрактах (изменениях), сведений об исполнении (прекращении действия) контрактов в электронном виде по каналам связи/налоговых органах (далее - пользователь), должны быть обеспечены условия хранения ключевых носителей и карточки отзыва ключей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации и паролей отзыва ключей. Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется, после получения ключевых дискет, создать рабочие копии. Копии должны быть соответствующим образом маркированы и должны использоваться и храниться также, как оригиналы. Пользователь несет ответственность за то, чтобы на компьютере, на котором установлены средства шифрования и ЭЦП, 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 криптографической защиты информации на данном рабочем месте должна быть прекращена и должны быть организованы мероприятия по анализу и ликвидации негативных последствий данного нарушения.

Не допускается:

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;
- вставлять ключевой носитель в ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровка информации, заверение файлов ЭЦП, подтверждение ее подлинности);
- записывать на ключевом носителе постороннюю информацию;
- вносить какие-либо изменения в программное обеспечение средств шифрования и ЭЦП;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).

  Посторонние лица не должны допускаться к работе с компьютером, на котором установлены средства шифрования и ЭЦП. Пользователь несет ответственность за проведение в полном объеме организационных и технических мероприятий, обеспечивающих выполнение настоящих правил.

3. Действия в случае компрометации (утраты) ключей

Под компрометацией закрытых ключей 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 закрытые ключи могут стать доступными несанкционированным лицам и (или) процессам.

Пользователь самостоятельно должен определить факт компрометации закрытого ключа и оценить значение этого события для пользователя. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием СКЗИ, организует и осуществляет сам пользователь. При компрометации ключа пользователя, он должен немедленно прекратить обмен файлами по каналам связи с Уполномоченным органом и поставить в известность

Удостоверяющий центр о факте компрометации, с указанием особой информации (пароля), содержащейся в карточке отзыва ключа. Информация о компрометации может передаваться по телефону или непосредственно представителю Удостоверяющего центра в его офисе. Не позднее 1 часа после поступления сообщения о компрометации ключа, скомпрометированный ключ будет заблокирован. Разблокировка будет произведена только после замены скомпрометированных ключей. Для получения новых ключей уполномоченный представитель организации - пользователя, у которой были скомпрометированы ключи, должен обратиться в Удостоверяющий центр, имея при себе документы, подтверждающие его полномочия (паспорт и две доверенности, одна из которых на получение материальных ценностей (ключевой дискеты), а вторая на получение ключевых документов). За выдачу новых ключей взимается оплата в соответствии с действующими расценками оператора системы на день оплаты.