12

УТВЕРЖДАЮ

«09» 01 2017 г.

ИНСТРУКЦИЯ
по работе со средствами криптографической защиты информации, сертификатами ключей электронной подписи, открытыми и закрытыми ключами электронной подписи в МБОУ СОШ № 7 п. Николаевка

1. Общие положения

1.1. Инструкция разработана в целях повышения безопасности хранения и обработки с использованием средств криптографической защиты информации (далее – СКЗИ) конфиденциальной информации, в соответствии с Федеральным Законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», приказом ФАПСИ от 13.06.2001 №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», приказом ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

1.2. Инструкция регламентирует порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации в МБОУ СОШ № 7 п. Николаевка.

1.3. Действие настоящей инструкции распространяется на пользователей средств криптографической защиты информации в МБОУ СОШ № 7 п. Николаевка.

1.4. Помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее – Помещения) необходимо оснащать входными дверьми с замками и обеспечить постоянное закрытие дверей Помещений на замок и их открытие только для санкционированного прохода. По окончании рабочего дня необходимо опечатывать Помещения. В случае невозможности опечатывания Помещения, его необходимо оборудовать соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещения.

1.5. В инструкции используются следующие понятия и определения:

– криптографический ключ (криптоключ) – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

– ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

– исходная ключевая информация – совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

– ключевой документ – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию;

– ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации);

– автоматизированное рабочее место (АРМ) – это программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

1.6. Пользователь – физическое лицо, непосредственно допущенное к работе с СКЗИ в МБОУ СОШ № 7 п. Николаевка.

2. Обязанности пользователя

2.1 Сертификат ключа подписи, закрытый и открытый ключи электронной подписи (далее – ЭП), эксплуатационную и техническую документацию к СКЗИ, ключевые документы должны хранится в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

2.2 Хранить ключи ЭП на съемном носителе (USB-токены), а не на жестком диске компьютера.

2.3 Использовать сложные PIN-пароли для защиты ключевой информации (не менее 8 знаков).

2.4 Ни в коем случае не отвечать на письма с требованиями (просьбами, предложениями) зайти на сайт, прислать секретный ключ или пароль доступа к нему, а немедленно сообщить о подобном факте администратору информационной безопасности или администратору АИС.

2.5 Не разглашать конфиденциальную информацию, к которой допущен, рубежи ее защиты, в том числе сведения о криптоключах.

2.6 Соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ.

2.7 Сообщать администратору информационной безопасности о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним.

2.8 Сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным приказом ФАПСИ от 13.06.2001 №152 , при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ.

2.9 Немедленно уведомлять администратора информационной безопасности 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.

2.10 Не отлучаться от компьютера, пока в нем находится съемный носитель, содержащий секретный ключ ЭП.

2.11 Извлекать из компьютера съемный носитель, содержащий секретный ключ, сразу после завершения работы.

2.12 На компьютере должно быть установлено антивирусное программное обеспечение с регулярно обновляемыми базами.

2.13 Если срок действия сертификата ключа подписи закончился, он поступает в папку архивного хранения с указанием даты поступления и росписью уполномоченного представителя.

2.14 В случае компрометации закрытого ключа ЭП, искажения личного закрытого ключа, а также, в случае если уполномоченному представителю стало известно, что этот ключ используется или использовался ранее другими лицами, следует немедленно обратиться в удостоверяющий центр с заявлением на аннулирование сертификата открытого ключа в течении не более чем одного рабочего дня со дня получения информации о таком нарушении.

2.15 В случае увольнения по любой причине пользователя, на имя которого удостоверяющим центром выдан сертификат ключа подписи, следует немедленно обратиться в удостоверяющий центр с заявлением на аннулирование сертификата ключа подписи.

2.16 Используемые или хранимые СКЗИ, сертификаты ключей подписи, открытые и закрытые ключи ЭП, эксплуатационная и техническая документация к ним, подлежат поэкземплярному учету по установленным формам в соответствии с требованиями Положения ПКЗ-2005.

2.17 Руководствоваться требованиями «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», утвержденной Приказом ФАПСИ от 13.06.2001 № 152.

3. Пользователю запрещается

3.1 Снимать несанкционированные копии с ключевых носителей.

3.2 Использовать сертификат ключа подписи без согласия законного владельца.

3.3 Использовать ключ электронной подписи в случае его компрометации.

3.4 Знакомить с содержанием ключевых носителей или передавать ключевые носители лицам, к ним не допущенным.

3.5 Выводить секретные ключи на дисплей (монитор) компьютера или принтер.

3.6 Устанавливать ключевой носитель в считывающее устройство (дисковод) компьютера, не предусмотренное функционированием системы, а также в другие компьютеры.

4. Ответственность пользователя:

4.1 Сертификат ключа подписи, открытый и закрытый ключи электронной подписи относится к конфиденциальной информации – служебной тайне или служебной информации.

4.2 Пользователь должен соблюдать требования по охране средств ЭП и СКЗИ в пределах своих полномочий.

4.3 Пользователь должен извещать работодателя обо всех случаях нарушения режима охраны тайны закрытого ключа ЭП и СКЗИ.

4.4 Пользователь несёт ответственность за нарушение режима охраны тайны СКЗИ, закрытого ключа ЭП, в том числе вплоть до возмещения ущерба.

4.5 За невыполнение или ненадлежащее выполнение обязательств по настоящей инструкции пользователь несёт ответственность в соответствии с законодательством Российской Федерации.