ГОСУДАРСТВЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ТУЛЬСКОЙ ОБЛАСТИ «ТУЛЬСКАЯ ШКОЛА» (ГОУ ТО «ТУЛЬСКАЯ ШКОЛА»)

Приложение к приказу
от 30.08.2024 № 74-осн

УТВЕРЖДЕНА приказом
ГОУ ТО «Тульская школа»
от 30.08.2024 № 74-осн

ИНСТРУКЦИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ СРЕДСТВ КРИПТОГРАФИЧЕСКОМ ЗАЩИТЫ ИНФОРМАЦИИ (СКЗИ) ГОУ ТО «ТУЛЬСКАЯ ШКОЛА»

г. Тула

1. Термины и определения

1.1. В настоящей Инструкции по эксплуатации средств криптографической защиты информации (далее – СКЗИ) государственного общеобразовательного учреждения Тульской области «Тульская школа» (далее – Учреждение) применяются следующие термины и определения:

1.1.1. безопасность эксплуатации СКЗИ – совокупность мер управления и контроля, защищающая СКЗИ и криптографические ключи от несанкционированного (умышленного или случайного) их раскрытия, модификации, разрушения или использования;

1.1.2. администратор безопасности (ответственный за эксплуатацию) СКЗИ – сотрудник, осуществляющий организацию и обеспечение работ по техническому обслуживанию СКЗИ и управление криптографическими ключами (далее – Администратор СКЗИ).

1.1.3. пользователь СКЗИ – сотрудник Учреждения, использующий СКЗИ для выполнения своих трудовых обязанностей;

1.1.4. средства криптографической защиты информации (СКЗИ) – совокупность программно-технических средств, обеспечивающих применение шифрования при осуществлении электронного документооборота, в том числе программное обеспечение с реализацией криптографических функций.

2. Общие положения

2.1. Настоящая Инструкция определяет:

2.1.1. порядок учета, хранения и использования СКЗИ и криптографических ключей, а также порядок их изготовления, смены, уничтожения в целях обеспечения безопасности эксплуатации СКЗИ;

2.1.2. обязанности, права и ответственность Администратора безопасности СКЗИ.

2.2. Все действия с СКЗИ осуществляются в соответствии с эксплуатационной и технической документацией на СКЗИ.

2.3. Администратор безопасности СКЗИ назначается и смещается с должности приказом директора Учреждения.

3. Основные обязанности Администратора безопасности СКЗИ

3.1. Администратор безопасности СКЗИ обязан:

3.1.1. вести поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним;

3.1.2. вести учет Пользователей СКЗИ;

3.1.3. осуществлять контроль за соблюдением условий использования СКЗИ в соответствии с эксплуатационной и технической документацией на СКЗИ и настоящей Инструкцией;

3.1.4. вести расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации;

3.1.5. осуществлять разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

3.1.6. не разглашать конфиденциальную информацию, к которой допущен, рубежи ее защиты, в том числе сведения о криптографических ключах;

3.1.7. соблюдать требования к обеспечению безопасности конфиденциальной информации при использовании СКЗИ.

4. Допуск к эксплуатации СКЗИ

4.1. Обучение Пользователей СКЗИ правилам работы с СКЗИ осуществляет Администратор безопасности СКЗИ.

4.2. Администратор безопасности СКЗИ должен иметь соответствующий документ о квалификации в области защиты информации.

4.3. Администратор безопасности СКЗИ должен быть ознакомлен с настоящей Инструкцией под роспись.

5. Учет и хранение СКЗИ и криптографических ключей

5.1. СКЗИ, эксплуатационная и техническая документация к ним, криптографические ключи подлежат поэкземплярному учету.

5.2. Поэкземплярный учет СКЗИ ведет Администратор безопасности СКЗИ в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним (далее – Журнал).

5.3. Все полученные экземпляры СКЗИ, криптографических ключей должны быть выданы под роспись в Журнале Пользователям СКЗИ, несущим персональную ответственность за их сохранность. При необходимости Пользователю СКЗИ выдается документация по эксплуатации СКЗИ с последующим возвратом Администратору безопасности СКЗИ.

5.4. Дистрибутивы СКЗИ на носителях, эксплуатационная и техническая документация к СКЗИ, инструкции хранятся у Администратора безопасности СКЗИ. Криптографические ключи хранятся у Пользователей СКЗИ. Хранение осуществляется в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

5.5. Резервные криптографические ключи находится на хранении у Администратора безопасности СКЗИ.

5.6. Ключевые носители подлежат обязательной маркировке (если это возможно) с изготовлением наклейки, содержащей реквизиты регистрации из Журнала и/или сертификата.

5.7. Неработоспособные ключевые носители подлежат уничтожению. Уничтожение оформляется актом, утвержденным приказом директора Учреждения «О назначении комиссии по уничтожению материальных носителей конфиденциальной и ключевой информации».

5.8. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные 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.

5.9. Ключевые носители совместно с Журналом должны храниться в запираемом шкафу, сейфе (металлическом шкафу). Места хранения ключевых носителей средств криптографической информации утверждены приказом «Об утверждении мест хранения конфиденциальной информации, ключевых документов и средств криптографической защиты».

5.10. На время отсутствия Администратора безопасности СКЗИ приказом директора Учреждения должен быть назначен сотрудник, замещающий его на время отсутствия.

6. Изготовление и плановая смена криптографических ключей

6.1. Изготовление криптографических ключей производиться Администратором СКЗИ в присутствии Пользователя СКЗИ.

6.2. Криптографические ключи изготавливаются на отчуждаемый ключевой носитель (дискету, ruToken, EToken и др.) в соответствии с эксплуатационно-технической документацией на СКЗИ и требованиями безопасности, установленными настоящей Инструкцией.

6.3. В целях обеспечения непрерывности проведения работы плановую смену криптографических ключей следует производить заблаговременно.

6.4. Переход на новые криптографические ключи Пользователь СКЗИ выполняет самостоятельно в соответствии с эксплуатационной документацией на СКЗИ. Переход на новые криптографические ключи осуществляется в сроки, указанные в сертификате ключа подписи.

6.5. При замене криптографических ключей используют программное обеспечение в соответствии с документами по эксплуатации. Пользователь СКЗИ обязан самостоятельно обновить сертификат ключ подписи. Обновление справочников сертификатов ключей производится путем добавления новых сертификатов ключей подписи из файлов, содержащих сертификаты ключей подписи, предоставляемых Администратором безопасности СКЗИ. Обновление справочников сертификатов ключей подписи осуществляется в соответствии с эксплуатационной документацией на СКЗИ.

7. Действия при компрометации криптографических ключей

7.1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию Владельца и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

7.1.1. утрата (хищение) НКИ, в том числе – с последующим их обнаружением;

7.1.2. увольнение (переназначение) работников, имевших доступ к ключевой информации;

7.1.3. передача секретных ключей по линии связи в открытом виде;

7.1.4. нарушение правил хранения криптоключей;

7.1.5. вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);

7.1.6. отрицательный результат при проверке, наложенной ЭП;

7.1.7. несанкционированное или безучётное копирование ключевой информации;

7.1.8. все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

7.2. События 7.1.1 – 7.1.5 должны трактоваться как безусловная компрометация действующих ключей. Остальные события требуют специального расследования в каждом конкретном случае.

7.3. При наступлении любого из перечисленных в п. 7.1 событий Владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации директору или Администратору безопасности СКЗИ.

7.4. При подтверждении факта компрометации действующих ключей Пользователь СКЗИ обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей.

7.5. Для восстановления конфиденциальной связи, после компрометации действующих ключей, на Пользователя СКЗИ оформляются новые ключи ЭП.

8. Уничтожение криптографических ключей

8.1. Неиспользованные или выведенные из действия криптографические ключи подлежат уничтожению.

8.2. Уничтожение криптографических ключей на ключевых носителях производится уполномоченной на то комиссий с участием Администратора СКЗИ с оформлением акта, утвержденного приказом директора Учреждения.

8.3. Криптографические ключи, находящиеся на ключевых носителях, уничтожаются путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на СКЗИ. При уничтожении криптографических ключей, находящихся на ключевых носителях, необходимо:

8.3.1. установить наличие оригинала и количество копий криптографических ключей;

8.3.2. проверить внешним осмотром целостность каждого ключевого носителя;

8.3.3. установить наличие на оригинале и всех копиях ключевых носителей реквизитов путем сверки с записями в Журнале поэкземплярного учета;

8.3.4. убедиться, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат уничтожению;

8.3.5. произвести уничтожение ключевой информации на оригинале и на всех копиях носителей.

8.4. В Журнале поэкземплярного учета Администратором СКЗИ производится отметка об уничтожении криптографических ключей.

9. Права Администратора безопасности СКЗИ

9.1. Администратор СКЗИ имеет право:

9.1.1. вносить предложения по совершенствованию СКЗИ;

9.1.2. повышать уровень квалификации по использованию СКЗИ.

10. Ответственность Администратора безопасности СКЗИ

10.1. Администратор безопасности СКЗИ несет персональную ответственность за обеспечение конфиденциальности ключевых носителей.

10.2. В случае неисполнения или ненадлежащего выполнения требований настоящей Инструкции Администратора СКЗИ может быть привлечен к дисциплинарной и/или административной ответственности в соответствии с действующим законодательством Российской Федерации.