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

Приложение № 1 к приказу
от 30.08.2024 № 75-осн

УТВЕРЖДЕНА приказом
ГОУ ТО «Тульская школа»
от 30.08.2024 № 75-осн

ИНСТРУКЦИЯ ПО ОБРАЩЕНИЮ С ШИФРОВАЛЬНЫМИ (КРИПТОГРАФИЧЕСКИМИ) СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ В ГОУ ТО «ТУЛЬСКАЯ ШКОЛА»

г. Тула

1. Общие положения

1.1. Настоящая инструкция регламентирует порядок обращения с шифровальными (криптографическими) средствами, предназначенными для защиты информации, не содержащей сведений, составляющих государственную тайну, в процессе их получения, транспортировки, учета, хранения, уничтожения, а также порядок допуска к работам с шифровальными средствами.

1.2. К шифровальным (криптографическим) средствам (средствам криптографической защиты информации – СКЗИ) относятся:

- средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации от несанкционированного доступа при ее передаче по каналам связи и (или) при ее обработке и хранении;
- средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;
- средства электронной подписи (ЭП) – аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием закрытого ключа электронной, подтверждение с использованием открытого ключа электронной подписи подлинности электронной подписи, создание закрытых и открытых ключей электронной подписи;
- средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

1.3. Сотрудники государственного общеобразовательного учреждения Тульской области «Тульская школа» (далее – сотрудники, Учреждение) допускаются к работе с СКЗИ на основании приказа директора Учреждения.

1.4. В Учреждении должно быть назначено приказом директора лицо, ответственное за обеспечение безопасности эксплуатации средств криптографической защиты информации (администратор безопасности СКЗИ).

1.5. Все сотрудники, допущенные к работе с СКЗИ, должны ознакомиться с настоящей инструкцией под роспись и строго выполнять требования следующих документов:

- настоящая инструкция;
- эксплуатационная документация на СКЗИ;
- организационно-распорядительные документы Учреждения, связанными с СКЗИ.

1.6. Разработка и проведение мероприятий по обеспечению

безопасности при проведении работ с СКЗИ осуществляется лицом, уполномоченным руководить работами с СКЗИ – администратором безопасности СКЗИ.

2. Порядок обращения со средствами криптографической защиты информации

2.1. СКЗИ, получает уполномоченный сотрудник Учреждения непосредственно у производителя СКЗИ или организации, предоставляющей СКЗИ. Безопасность в процессе доставки обеспечивается организационными мерами.

2.2. При транспортировке СКЗИ, инсталлирующих СКЗИ носителей, должны быть обеспечены условия, исключающие возможность физических повреждений и внешнего воздействия на записанную информацию, а также ее копирование.

2.3. Все поступающие СКЗИ, инсталлирующие СКЗИ носители, эксплуатационная и техническая документация к ним должны браться на поэкземплярный учет в специальных журналах установленной формы. Ведет журналы уполномоченный на это сотрудник.

2.4. Инсталлирующие СКЗИ носители должны храниться в сейфе (металлическом шкафу, хранилище).

2.5. При вскрытии сейфа с инсталлирующими СКЗИ носителями должна быть проверена целостность печатей и замков и/или оттисков печатей. В случае нарушения целостности печатей и/или замков и/или оттисков печатей сотрудник обязан немедленно сообщить об этом администратору безопасности СКЗИ.

2.6. Хранение инсталлирующих СКЗИ носителей допускается в одном хранилище с другими документами при условиях, исключающих непреднамеренное их уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение.

2.7. В случае отсутствия у сотрудника индивидуального хранилища инсталлирующие СКЗИ носители по окончании рабочего дня должны сдаваться администратору безопасности СКЗИ.

2.8. 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 дисковод ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровка информации, заверка файлов ЭП, подтверждение ее подлинности), а также в дисководы других ПЭВМ записывать на ключевом носителе постороннюю информацию;

- вносить какие-либо изменения в программное обеспечение средств шифрования и ЭП;

- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое

уничтожение носителей).

2.9. Посторонние лица не должны допускаться к работе с компьютером, на котором установлены СКЗИ.

2.10. Пользователь СКЗИ несет ответственность за проведение в полном объеме организационных и технических мероприятий, обеспечивающих выполнение настоящей Инструкции

3. Эксплуатация средств криптографической защиты информации

3.1. К эксплуатации СКЗИ допускаются лица, утвержденные приказом директора «О допуске сотрудников к работам со средствами криптографической защиты (СКЗИ)».

3.2. Пересылка (передача) носителей криптоключей может осуществляться через фельдъегерскую или специальную связь, а также со специально выделенным нарочным (в опечатанном Ответственным конверте).

3.3. Ключевая информация на носителях уничтожается оператором СКЗИ путем переформатирования с использованием средств ЭП. Допускается данные носители после переформатирования использовать в дальнейшем операторами СКЗИ при условии записи на них новой ключевой информации.

3.4. Об уничтожении ключей операторами СКЗИ делается соответствующая запись в соответствующем журнале. Периодически Ответственный проверяет данные записи.

3.5. Перед уничтожением секретных ключей следует расшифровать архивную информацию (если такая имеется), хранящуюся в зашифрованном виде, и зашифровать ее используя новые ключи.

3.6. Выведенные из действия открытые ключи ЭП сохраняются в архивах в течение 5 (пяти) лет для обеспечения возможности в последующем выполнения процедуры разбора конфликтных ситуаций.

4. Восстановление конфиденциальной связи после компрометации действующих криптоключей

4.1. Компрометация ключевой информации» - это 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.

4.2. К событиям, связанным с компрометацией криптоключей, относятся следующие:

- потеря ключевых носителей;
- потеря ключевых носителей с их последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения и уничтожения секретного ключа;

- возникновение подозрений на утечку информации или ее искажение;

- нарушение печати на сейфе с ключевыми носителями (если такая используется);

- случаи, когда нельзя достоверно установить, что произошло с магнитными носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

4.3. Первые четыре события должны трактоваться как явная компрометация криптоключей. Три следующих события требуют специального рассмотрения в каждом конкретном случае.

4.4. При обнаружении признаков, указывающих на возможную компрометацию закрытых ключей, носителей и/или конфиденциальной информации, Оператор СКЗИ должен самостоятельно определить факт компрометации и оценить значение этого события, после чего обязан немедленно оповестить администратора безопасности СКЗИ.

4.5. Администратор безопасности СКЗИ обязан сообщить об компрометации директору Учреждения.

4.6. Администратор безопасности СКЗИ обязан оперативно оповестить всех пользователей СКЗИ о факте (или предполагаемой) компрометации.

4.7. Расследование факта (или предполагаемой) компрометации должно проводиться на месте происшествия уполномоченными лицами.

4.8. Результатом рассмотрения является квалификация или не квалификация данного события как компрометация действующих криптоключей.

4.9. При установлении факта компрометации действующих криптоключей, скомпрометированные секретные ключи шифрования уничтожаются.

5. Права и ответственность за нарушение требований Инструкции

5.1. Пользователь СКЗИ имеет право:

- запрашивать и получать от сотрудников сведения, справочные и другие материалы, необходимые для осуществления его деятельности.

принимать участие в совещаниях по вопросам, входящим в его компетенцию;

- участвовать в семинарах (конференциях и т.п.) на темы «информационных технологий» и «защиты информации» в качестве слушателя;

- ставить перед директором вопросы о создании надлежащих условий для исполнения своих должностных обязанностей.

5.2. Пользователь СКЗИ несет ответственность (дисциплинарную, административную, материальную, уголовную) за:

- разглашение конфиденциальной информации, к которой он допущены, рубежи ее защиты, в том числе сведения о криптоключах;

- не соблюдение требований к обеспечению безопасности

конфиденциальной информации с использованием СКЗИ;

- не обеспечение сохранности принятых на ответственное хранение программных и технических СКЗИ;

- не соблюдение регламента эксплуатации СКЗИ;

- не сообщение администратору безопасности СКЗИ о ставших ему известных попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним, а также 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 защищаемой конфиденциальной информации;

- ненадлежащее и несвоевременное выполнение своих функциональных обязанностей;

- не обеспечение сохранности принимаемой информации и достоверности, передаваемой;

- несвоевременного, а также некачественного исполнения документов и поручений директора;

- нерациональное использование выделенных финансовых, материальных и информационно-вычислительных ресурсов.