МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ СВЕРДЛОВСКОЙ ОБЛАСТИ
государственное автономное профессиональное образовательное учреждение Свердловской области
«Уральский политехнический колледж - Межрегиональный центр компетенций»
(ГАПОУ СО «Уральский политехнический колледж - МЦК»)

ПРИНЯТО
решением Совета колледжа
протокол от 03.06.2019 № 3

УТВЕРЖДЕНО
приказом ГАПОУ СО
«Уральский политехнический
колледж – МЦК»
от 03.06.2019 г. № 01-05/200

ПОЛОЖЕНИЕ

по обеспечению безопасности информации с помощью средств криптографической защиты информации в информационных системах ГАПОУ СО «Уральский политехнический колледж — МЦК»

г. Екатеринбург

Содержание

1. Общие положения

Настоящее Положение по обеспечению безопасности информации с помощью средств криптографической защиты информации в информационных системах ГАПОУ СО «Уральский политехнический колледж — МЦК» (далее — Положение) разработано в соответствии со следующими нормативными правовыми актами:

– Федеральный закон Российской Федерации (далее — РФ) от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказ Федерального агентства правительственной связи и информации при Президенте РФ от 13 июня 2001 г. № 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»;

– Приказ Федеральной службы безопасности (далее — ФСБ) РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

– Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

– Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утверждены руководством 8 Центра ФСБ России 31.03.2015 г. № 149/7/2/9-432).

К шифровальным (криптографическим) средствам защиты информации (далее — СКЗИ), включая документацию на эти средства, относятся:

1) средства шифрования — аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче;

2) средства имитозащиты — аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации;

3) средства электронной подписи;

4) средства кодирования — средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций;

5) средства для изготовления ключевых документов — аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящих в состав этих шифровальных (криптографических) средств;

6) ключевые документы — электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах.

2. Организация и обеспечение функционирования СКЗИ

Организация и обеспечение функционирования СКЗИ представляет следующий комплекс мероприятий:

– установка и ввод в эксплуатацию СКЗИ в соответствии с эксплуатационной и технической документацией к этим средствам;

– проверка готовности СКЗИ к использованию с составлением заключений о возможности их эксплуатации;

– разработка мероприятий по обеспечению функционирования и безопасности, применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам;

– создание исходной ключевой информации, создание из исходной ключевой информации ключевых документов, их распределение, рассылку и учет;

– обучение сотрудников, использующих СКЗИ, работе с ними;

– поэкземплярный учет используемых СКЗИ, предусмотренных эксплуатационной и технической документацией к ним;

– проведение служебной проверки и составление заключений по фактам нарушения условий криптографической защиты информации.

2.1. Структура ответственных лиц

Структуру ответственных лиц по направлению организации и обеспечению криптографической защиты информации в ГАПОУ СО «Уральский политехнический колледж — МЦК» образуют:

– ответственный пользователь СКЗИ;

– пользователи СКЗИ.

Лица, осуществляющие работу с СКЗИ, должны быть ознакомлены с документами, регламентирующими организацию и обеспечение криптографической защитой информации, под подпись и несут ответственность за несоблюдение ими требований указанных документов в соответствии с законодательством РФ.

Контроль за организацией и обеспечением функционирования СКЗИ возлагается на ответственного пользователя СКЗИ в пределах его служебных полномочий.

Контроль за организацией, обеспечением функционирования и безопасности СКЗИ осуществляется в соответствии с законодательством РФ.

2.1.1. Ответственный пользователь СКЗИ

Ответственный пользователь СКЗИ назначается в соответствии с документом, утвержденным руководителем ГАПОУ СО «Уральский политехнический колледж — МЦК».

Организация и обеспечение функционирования СКЗИ возлагается на ответственного пользователя СКЗИ.

Перед допуском к работе ответственный пользователь СКЗИ обязан ознакомиться с нормативными правовыми документами, регулирующими организацию и обеспечение криптографической защиты информации, с настоящим Положением и локальными актами, определяющими порядок защиты информации с помощью СКЗИ в ГАПОУ СО «Уральский политехнический колледж — МЦК».

Ответственный пользователь СКЗИ осуществляет:

– организацию безопасности обработки информации с использованием СКЗИ;

– обеспечение функционирования и безопасности СКЗИ;

– организацию и обеспечение эксплуатации СКЗИ;

– разработку и осуществление мероприятий по организации и обеспечению безопасности хранения, обработке и передаче информации с использованием СКЗИ;

– поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, и ключевых документов;

– учет сотрудников, являющихся пользователями СКЗИ;

– обучение пользователей СКЗИ работе с СКЗИ;

– инсталляцию (деинсталляцию) СКЗИ с рабочих мест пользователей СКЗИ, прием, выдачу, уничтожение ключевой информации, эксплуатационной и технической документации к ним;

– плановую смену ключей, а также смену ключей в случае их компрометации;

– контроль за соблюдением пользователями СКЗИ условий использования СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

– участие в комиссиях по расследованию фактов нарушений условий использования СКЗИ, которые могут привести (привели) к снижению уровня характеристик безопасности информации;

– участие в комиссиях по плановой проверке правильности учета и соблюдения правил обращения с СКЗИ и их хранением;

– уведомление руководства о фактах нарушения порядка эксплуатации СКЗИ.

Ответственный пользователь СКЗИ несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности хранения, обработки с использованием СКЗИ требованиям законодательства, эксплуатационной и технической документации к СКЗИ, настоящим Положением.

2.1.2. Пользователь СКЗИ

Пользователь СКЗИ обязан:

– не разглашать информацию, к которой он допущен, в том числе сведения об СКЗИ, ключевых документах к ним и других мерах защиты;

– соблюдать требования к обеспечению безопасности СКЗИ и ключевых документов к ним;

– обеспечивать с помощью СКЗИ безопасность хранения, обработки информации, ключевых документов к СКЗИ и парольной информации к ним;

– осуществлять эксплуатацию СКЗИ в соответствии с требованиями эксплуатационной документации;

– не допускать снятие копий с ключевых документов;

– не допускать записи на ключевой носитель посторонней информации;

– не допускать установки ключевых документов на другие автоматизированные рабочие места (далее — АРМ);

– хранить инсталлирующие СКЗИ носители, 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;

– предусматривать раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей;

– сообщать о ставших известных попытках получения сведений об используемых СКЗИ или ключевых документах к ним лицами, не обладающими правом доступа к таким сведениям;

– немедленно уведомлять ответственного пользователя СКЗИ, руководство о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее — Помещения), хранилищ, личных печатей, предназначенных для опечатывания Помещений (хранилищ), и о других фактах, которые могут привести к снижению уровня характеристик безопасности информации;

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

2.2. Требования к обеспечению безопасности хранения и обработки информации с использованием СКЗИ

Безопасность хранения и обработки с использованием СКЗИ информации достигается:

– соблюдением пользователями СКЗИ конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документах к ним;

– точным выполнением пользователями СКЗИ требований к обеспечению безопасности информации;

– надежным хранением эксплуатационной и технической документации к СКЗИ, ключевых документов, носителей информации;

– своевременным выявлением сотрудниками попыток получения сведений о защищаемой информации, об используемых СКЗИ или ключевых документах к ним лицами, не обладающими правом доступа к таким сведениям;

– немедленным принятием мер по предупреждению разглашения защищаемой информации, а также возможной ее утечки при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от Помещений, хранилищ, сейфов, личных печатей и т.п.

2.2.1. Требования к помещениям

Размещение, специальное оборудование, охрана и организация режима в Помещениях, должны обеспечивать сохранность защищаемой информации, СКЗИ и ключевых документов к ним.

Помещения должны удовлетворять требованиям, предъявляемым эксплуатационной и технической документацией к СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

Размещение, специальное оборудование, охрана и организация режима в Помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

Обеспечение режима, препятствующего возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих права доступа в Помещения, который достигается путем:

– оснащением Помещений входными дверьми с замками;

– обеспечением постоянного закрытия дверей Помещений на замок и их открытия только для санкционированного прохода, а также опечатывания Помещений по окончании рабочего дня или оборудование Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений;

– утверждения правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

– утверждения перечня лиц, имеющих право доступа в Помещения.

Помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие Помещений в нерабочее время. Для предотвращения просмотра Помещений извне их окна должны быть защищены.

Ответственный пользователь СКЗИ осуществляет учет хранилищ, ключей от них в журнале учета хранилищ и ключей от них, форма которого приведена в Приложении № 1 к настоящему Положению.

Помещения подлежат опечатыванию или должны быть оснащены охранной сигнализацией, связанной со службой охраны здания. Исправность охранной сигнализации периодически необходимо проверять ответственному пользователю СКЗИ и с отметкой в журнале проверки работы средств охранной сигнализации,

размещенных в помещении, форма которого приведена в Приложении № 2 к настоящему Положению.

Ключи от дверей Помещений подлежат учету, который осуществляет ответственный пользователь СКЗИ в журнале учета хранилищ и ключей от них.

Дубликаты ключей от Помещений следует хранить ответственному пользователю СКЗИ в сейфе.

Личные печати сотрудников, предназначенные для опечатывания хранилищ и Помещений, должны находиться у пользователей СКЗИ, ответственных за эти хранилища и Помещения. Выдачу личных печатей сотрудникам осуществляет ответственный пользователь СКЗИ с отметкой в журнале учета личных печатей, предназначенных для опечатывания помещений (хранилищ), форма которого приведена в Приложении № 3 к настоящему Положению.

По окончании рабочего дня Помещения и установленные в нем хранилища должны быть закрыты, а также поставлены на охрану посредством технических средств охраны или опечатаны, о чем производится запись в журнале опечатывания (вскрытия) помещений (хранилищ), форма которого приведена в Приложении № 4 к настоящему Положению.

Ответственный пользователь СКЗИ осуществляет контроль за вскрытием, опечатыванием хранилищ с обязательной отметкой в журнале опечатывания (вскрытия) хранилищ. Хранение ключей от хранилищ ответственный пользователь СКЗИ осуществляет в личном или специально выделенном хранилище.

При утрате ключа от хранилища или от входной двери в Помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный пользователь СКЗИ.

В обычных условиях Помещения, а также находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями СКЗИ, имеющими право доступа в соответствующие помещения, или ответственным пользователем СКЗИ.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в Помещения о случившемся должно быть немедленно сообщено ответственному пользователю СКЗИ или руководству. Прибывший ответственный пользователь СКЗИ должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации и к замене скомпрометированных криптоключей.

Обеспечение сохранности носителей персональных данных достигается:

– хранением съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с

использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов);

– поэкземплярным учетом машинных носителей персональных данных в соответствующем журнале.

В Помещениях для хранения выданных им ключевых документов, эксплуатационной и технической документации к СКЗИ, инсталлирующих СКЗИ носителей необходимо наличие достаточного числа надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ. Дубликаты ключей от хранилищ должны храниться в сейфе ответственного пользователя СКЗИ.

Техническое обслуживание СКЗИ и смена криптоключей осуществляется в отсутствие лиц, не допущенных к работе с данными СКЗИ.

2.2.2. Требования к СКЗИ

Для криптографической защиты информации должны применяться только сертифицированные по требованиям Федеральной службы безопасности РФ СКЗИ.

2.2.3. Требования к АРМ, на которые инсталлируются СКЗИ

Технические характеристики и состав ПО должны соответствовать требованиям, предъявляемым эксплуатационной и технической документацией к СКЗИ.

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. При наличии технической возможности на время отсутствия пользователей СКЗИ данные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

2.2.4. Требования к криптоключам

По истечению срока действия, криптоключ подлежит смене, в порядке, предусмотренном эксплуатационной и технической документацией к СКЗИ или регламентом удостоверяющего центра, от которого получен ключевой документ.

2.3. Эксплуатация СКЗИ

2.3.1. Регистрация и учет СКЗИ, ключевых документов и эксплуатационной и технической документации к ним

Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету в журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов, форма которого приведена в Приложении № 5 к настоящему Положению.

Единицей поэкземплярного учета криптоключей является ключевой носитель. Если один и тот же ключевой носитель многократно используется для записи криптоключей, то каждый раз он подлежит отдельной регистрации.

Журналы ведутся ответственным пользователем СКЗИ. С учетом особенности эксплуатации отдельных СКЗИ допускается добавление в журналы полей или их перестановка. При ведении журналов не допускается применение корректирующих средств.

Журналы ведутся до полного использования, после чего закрываются. Все числящиеся на момент закрытия журнала СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы берутся на учет во вновь заведенном журнале поэкземплярного учета.

Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале, форма которого приведена в Приложении № 6 или в журнале поэкземплярного учета ключевых носителей, ключевых документов, форма которого приведена в Приложении № 11, ведущимся непосредственно пользователем СКЗИ.

2.3.2. Выдача СКЗИ, ключевых документов, эксплуатационной и технической документации к ним

Выдача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов осуществляется ответственным пользователем СКЗИ под подпись в журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов между пользователями СКЗИ допускается между пользователями СКЗИ и (или) ответственным пользователем СКЗИ под подпись в соответствующем журнале поэкземплярного учета. Такая передача между пользователями СКЗИ должна быть санкционирована ответственным пользователем СКЗИ.

Заказ на изготовление очередных ключевых документов, их изготовление и рассылку на места использования для своевременной замены действующих ключевых документов следует производить заблаговременно.

Изготовление (заказ) ключевой информации осуществляется на основе решения руководителя или заявки на установку СКЗИ.

Ключи записываются только на учтенные машинные носители информации.

Указание о вводе в действие очередных ключевых документов может быть дано ответственным пользователем СКЗИ только после поступления от всех заинтересованных пользователей СКЗИ подтверждения о получении ими очередных ключевых документов.

Неиспользованные или выведенные из действия ключевые документы подлежат возвращению ответственному пользователю СКЗИ или по его указанию должны быть уничтожены на месте.

2.3.3. Инсталляция СКЗИ

Перед инсталляцией СКЗИ проводится обследование Помещения на соответствие требованиям, предъявляемым к Помещениям технической и эксплуатационной документацией к СКЗИ.

Допуск пользователей СКЗИ к работе с СКЗИ осуществляется после прохождения ими обучения работе с СКЗИ. Обучение проводит ответственный пользователь СКЗИ. Обучение включает ознакомление с требованиями нормативных правовых актов и локальных актов ГАПОУ СО «Уральский политехнический колледж — МЦК», регламентирующих организацию криптографической защиты информации и предусматривающих порядок обращения с СКЗИ, эксплуатационной и технической документацией к СКЗИ, и настоящим Положением. О факте проведения обучения делается отметка в журнале учета пользователей средств криптографической защиты информации, форма которого приведена в Приложении № 7 к настоящему Положению.

По завершении инсталляции составляется Акт установки и ввода в эксплуатацию СКЗИ, форма которого приведена в Приложении № 8. Акт установки и ввода в эксплуатацию СКЗИ подлежит хранению у ответственного пользователя СКЗИ. Сведения о пользователе СКЗИ заносятся в журнале учета пользователей средств криптографической защиты информации.

2.3.4. Порядок эксплуатации СКЗИ

Эксплуатация СКЗИ осуществляется в соответствии с технической и эксплуатационной документацией к нему.

Эксплуатационная и техническая документация для СКЗИ, ключевые документы хранятся в хранилищах в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Отдельно от ключей подлежат хранению резервные ключевые документы, предназначенные для применения в случае компрометации действующих.

Перед началом работы с АРМ контролируется наличие и целостность номерной наклейки (пломбы), которой опечатан системный блок. После входа в операционную систему контролируется запуск антивирусного программного обеспечения и актуальность антивирусных баз.

Во время эксплуатации СКЗИ осуществляется контроль целостности установленного СКЗИ с помощью механизма самого СКЗИ или с помощью программного обеспечения контроля целостности.

Во время эксплуатации СКЗИ пользователям СКЗИ запрещается:

– изменять настройки СКЗИ;

– осуществлять вскрытие системного блока АРМ с установленными СКЗИ, подключать к ним дополнительные устройства без разрешения ответственного пользователя СКЗИ;

– оставлять без контроля ключевые носители, а также АРМ с установленными СКЗИ при включенном питании;

– вносить какие-либо несанкционированные изменения в СКЗИ;

– выводить на монитор защищаемую информацию (в т.ч. информацию ключевых документов), обрабатываемых с использованием СКЗИ в присутствии лиц, не имеющих к такой информации права доступа;

– применять скомпрометированные ключи и пароли;

– осуществлять несанкционированное копирование ключевой информации;

– вставлять ключевой носитель в устройства, штатный порядок работы которых не предусматривает использование ключевого носителя.

2.3.5. Контроль за соблюдением эксплуатации средств криптографической защиты информации

Ежегодно комиссией, в которую входят сотрудники ГАПОУ СО «Уральский политехнический колледж — МЦК», проводятся плановые проверки:

– наличия, правильности учета и соблюдения правил обращения и хранения СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

– выявление установочных носителей СКЗИ, ключевых документов, экземпляров технической и эксплуатационной документации подлежащей уничтожению;

– соблюдения правил обращения, предусмотренных настоящим Положением пользователями СКЗИ.

Внеплановые проверки проводятся комиссией, в которую входят сотрудники ГАПОУ СО «Уральский политехнический колледж — МЦК», в случаях нарушения установленного в ГАПОУ СО «Уральский политехнический колледж — МЦК» порядка криптографической защиты информации.

Состав комиссии определяет руководитель ГАПОУ СО «Уральский политехнический колледж — МЦК».

По завершении проверки комиссией составляется Акт проверки, в котором указывается состав комиссии, основание проверки, проверочные мероприятия, недостатки, выявленные в ходе проверки, и рекомендации по их устранению,

рекомендации по совершенствованию криптографической системы защиты информации.

2.3.6. Порядок проведения служебной проверки по фактам нарушения правил эксплуатации СКЗИ

В случае возникновения конфликтной ситуации и по фактам (подозрению) нарушения конфиденциальности информации, защищаемой с помощью СКЗИ, проводится служебная проверка.

Основаниями проведения служебной проверки являются докладная записка сотрудника, информационные письма (претензии) сторонних организаций, непосредственное обнаружение руководством факта (подозрения) нарушения конфиденциальности защищаемой информации, безопасность которых обеспечивается применением СКЗИ.

Служебная проверка назначается руководителем не позднее трех дней с момента поступления информации о факте нарушения конфиденциальности защищаемой информации.

В ходе служебной проверки устанавливается:

– действительно ли имело место нарушение конфиденциальности защищаемой информации;
– лица виновные в нарушении, их вина и ее степень;
– причины и условия, способствовавшие нарушению;
– характер и размер причиненного ущерба;
– предложения по недопущению подобных случаев впредь;
– иные сведения, имеющие отношения к нарушению.

Служебная проверка осуществляется комиссией, состав комиссии утверждается руководителем ГАПОУ СО «Уральский политехнический колледж — МЦК», состав комиссии должен представлять не менее трех человек.

Срок завершения служебной проверки указывается в документе о проведении служебной проверки. Если срок не указан, то служебная проверка завершается не позднее, чем через месяц со дня обнаружения нарушения.

На первом этапе служебной проверки комиссия устанавливает суть нарушения, его последствия, предполагает, что могло послужить причиной.

На втором этапе собирается вся необходимая интересующая информация о нарушении, объяснения с участников.

На третьем этапе на основании собранных в ходе первых двух этапов служебной проверки материалов оформляется письменное заключение (акт). В нем указываются основание и сроки проведения служебной проверки, состав комиссии, значимые обстоятельства, установленные в ходе служебной проверки. Акт подписывается всеми членами комиссии и направляется руководителю.

2.3.7. Порядок действий при компрометации ключа

Под компрометацией ключей понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

Различают явную и неявную компрометацию ключей. Явной называется компрометация, факт которой становится известным на отрезке установленного времени действия данного ключа. Неявной называется компрометация ключа, факт которой остается неизвестным для лиц, являющихся законными пользователями данного ключа.

События, квалифицируемые как явная компрометация:

– утрата ключевого носителя;

– утрата ключевого носителя с последующим обнаружением;

– нарушение правил хранения и уничтожения (после окончания срока действия) ключевой информации.

К событиям, связанным с неявной компрометацией ключей и требующим их рассмотрения в каждом конкретном случае, относятся:

– навязывание заведомо ложной информации в документах, защищенных имитовставками;

– случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями, содержащими ключевую информацию, в том числе случаи, когда дискета (*eToken* и др.) вышла из строя и доказательно не опровергнуто, что данный факт произошел в результате несанкционированного доступа злоумышленника.

Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их чтения, копирования.

При наступлении компрометации ключа или подозрения в компрометации ключа пользователь СКЗИ обязан немедленно прекратить работу с СКЗИ и сообщить ответственному пользователю СКЗИ о факте компрометации (в том числе и предполагаемом).

По факту компрометации ключей (в том числе предполагаемому) проводится служебная проверка в соответствии с п. 2.3.7 настоящего Положения.

По завершению проверки оформляется письменное заключение (акт) о проведении служебной проверки.

Скомпрометированные ключи по завершению проверки подлежат уничтожению в порядке, определенном настоящим Положением.

Взамен скомпрометированных ключей ответственный пользователь СКЗИ производит замену ключей в порядке, предусмотренном технической и эксплуатационной документацией, или в соответствии с Регламентом удостоверяющего центра.

2.3.8. Деинсталляция средств криптографической защиты информации

Деинсталляция СКЗИ с рабочих мест пользователей СКЗИ осуществляется на основании решения руководителя или по соответствующей заявке, форма которой приведена в Приложении № 9 к настоящему Положению.

Деинсталляция СКЗИ осуществляется рабочей группой в соответствии с процедурой, предусмотренной эксплуатационной и технической документацией к СКЗИ, с составлением Акта деинсталляции СКЗИ, форма которого приведена в

Приложении № 10 к настоящему Положению. Акт о деинсталляции СКЗИ подлежит хранению у ответственного пользователя СКЗИ. В рабочую группу включается ответственный пользователь СКЗИ.

Одновременно с деинсталляцией СКЗИ уничтожаются криптоключи, если не планируется их дальнейшее использование. В противном случае они возвращаются ответственному пользователю СКЗИ с отметкой в соответствующем журнале**.**

О факте деинсталляции СКЗИ делается отметка в журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

2.3.9. Уничтожение СКЗИ

Основаниями для уничтожения инсталляционных носителей СКЗИ, эксплуатационной и технической документации к ним, ключевых документов являются утвержденные акты на списание и уничтожение материальных носителей и подлежащие хранению у ответственного пользователя СКЗИ.

Основанием для уничтожения ключей является истечение срока их действия, вывод из эксплуатации СКЗИ, увольнение сотрудника, снятие с сотрудника обязанностей, связанных с использованием СКЗИ и т.д.

Неиспользуемые или выведенные из действия ключевые носители подлежат возращению ответственному пользователю СКЗИ либо криптоключи, записанные на них, подлежат уничтожению на месте.

Уничтожение криптоключей производится путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей без повреждения ключевого носителя.

Криптоключи стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков, Smart Card и т.п.). Непосредственные действия по стиранию криптоключей, а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируется эксплуатационной и технической документацией к соответствующем СКЗИ, а также указаниями организаций, производивших запись криптоключей.

Ключевые носители уничтожаются путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановление ключевой информации. Непосредственные действия по стиранию криптоключей, а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируется эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей.

Ключевые документы должны уничтожаются 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 десяти дней после вывода их из действия.

В эти же сроки с отметкой в соответствующем журнале подлежат уничтожению разовые ключевые носители и ранее введенная, и хранящаяся в СКЗИ или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключам; хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в СКЗИ или иных дополнительных устройствах уничтожаются пользователями этих СКЗИ самостоятельно под подпись в соответствующем журнале.

Ключевые документы уничтожаются либо пользователями СКЗИ, либо ответственным пользователем СКЗИ с указанием отметки о факте уничтожения в соответствующем 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. После уничтожения пользователи СКЗИ должны уведомить об этом ответственного пользователя СКЗИ.

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

Определенные к уничтожению СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к ним процедура удаления программного обеспечения СКЗИ, и они полностью отсоединены от аппаратных средств.

Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее с СКЗИ оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.) разрешается использовать после уничтожения СКЗИ без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования должна быть надежно удалена.

Факт уничтожения носителей эксплуатационной и технической документации, установочных носителей СКЗИ, криптоключей, путем уничтожения ключевых носителей фиксируется в Акте уничтожения. Уничтожение производится комиссией в составе не менее трех человек из числа пользователей СКЗИ. В акте указывается, что уничтожается и в каком количестве, а также делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых инсталлирующих носителей СКЗИ, эксплуатационной и технической документации к ним. Акт уничтожения подлежит хранению у ответственного пользователя СКЗИ.

Факт уничтожения криптоключей с ключевого носителя совместно с деинсталляцией СКЗИ с его рабочего места фиксируется в Акте деинсталляции СКЗИ. Акт деинсталляции СКЗИ подлежит хранению у ответственного пользователя СКЗИ. О факте уничтожении делаются отметки в соответствующем журнале поэкземплярного учета.

Приложение № 1

Форма журнала
учета хранилищ и ключей от них

№ п/п	Номер ключа от хранилища, вид и регистра-ционный (инвентар-ный) номер хранилища	Место нахождения хранилища	Ключ в пенале (да/нет)	ПОЛУЧЕНО (Фамилия, инициалы, подпись получившего ключ, дата)	СДАНО (Фамилия, инициалы, подпись сдавшего ключ, дата)	УТЕРЯНО (Фамилия, инициалы, подпись утерявшего ключ, дата)	Примечание
1	2	3	4	5	6	7	8

Приложение № 2

Форма журнала
проверки работы средств охранной сигнализации,
размещенных в помещении _____

Дата	Вид работы	Ф.И.О., подпись ответственного лица
1	2	3

Приложение № 3

Форма журнала
учета личных печатей, предназначенных для опечатывания помещений (хранилищ)

№ п/п.	Наименование печати	Оттиск печати	Наименование подразделения, должность, фамилия, имя, отчество получателя	Подпись в получении, дата	Результат ежегодной проверки печатей (их оттиски и дата проверки)	Оттиск печатей, возвращенных для уничтожения, дата возврата	Отметка об уничтожении, номер акта и дата	Приме-чание
1	2	3	4	5	6	7	8	9

Приложение № 4

Форма журнала
опечатывания (вскрытие) помещений (хранилищ)

№ п/п	Номер печати, которой опечатано помещение (хранилище)	Дата и время опечатывания помещения (хранилища)	Ф.И.О. и подпись лица, опечатавшего помещение (хранилище)	Дата и время вскрытия помещения (хранилища)	Номер печати, которой было опечатано помещение (хранилище)	Ф.И.О. и подпись лица, вскрывшего помещение (хранилище)
1	2	3	4	5	6	7

Приложение № 5

Форма журнала
поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

Левый разворот

№ п/п.	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Тип носи-теля	Регистрационные номера СКЗИ, эксплуата-ционной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптогра-фические номера) ключевых документов	Отметка о получении			Отметка о выдаче	
					От кого полу-чены	Дата и номер сопрово-дительного письма, товарной накладной (иного документа о получении)	Ф.И.О. ответственного пользователя СКЗИ, получившего СКЗИ, эксплуатацион-ную и техническую документацию к ним, ключевые документы, дата получения, подпись	Наименование юридического лица или Ф.И.О. сотрудника, выдавшего СКЗИ, эксплуата-ционную и техничес-кую документа-цию, ключевые документы	Ф.И.О. сотрудника, получившего СКЗИ, эксплуата-ционную и техническую документацию, ключевые документы, дата и подпись
1	2	3	4	5	6	7	8	9	10

Правый разворот

Отметка о подключении (установке) СКЗИ				Отметка об изъятии СКЗИ из аппаратных средств, выводе СКЗИ из эксплуатации, уничтожении ключевых документов			Приме-чание
Ф.И.О. ответственного пользователя СКЗИ, производившего подключение, (установку) СКЗИ	Дата подключения (установки) СКЗИ и подписи лиц, производивших подключение (установку)	Наименование и номера аппаратных средств, в которые установлены и/или к которым подключены СКЗИ/ номер ключевого носителя или зоны СКЗИ, в которую введены криптоключи	Дата и номер акта о вводе в эксплуата-цию СКЗИ	Дата изъятия СКЗИ из аппаратных средств, деинсталляции СКЗИ, уничтожения ключевых документов (с указанием наименования производимой процедуры)	Дата и номер акта об изъятии СКЗИ из аппаратных средств, о деинсталляции СКЗИ, об уничтожении ключевых документов	Ф.И.О. ответственного пользователя СКЗИ, производившего изъятие СКЗИ из аппаратных средств, деинсталляцию СКЗИ из эксплуатации, уничтожение ключевых документов	
11	12	13	14	15	16	17	18

Приложение № 6

Форма
технического (аппаратного) журнала

№ п/п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи	Дата	Подпись пользователя СКЗИ	
1	2	3	4	5	6	7	8	9	10

Приложение № 7

Форма журнала
учета пользователей средств криптографической защиты информации

№ п/п	Дата	Ф.И.О. пользователя СКЗИ	Наименование СКЗИ	Номер помещения, где размещено СКЗИ	Подпись пользователя СКЗИ, прошедшего инструктаж	Ф.И.О. и подпись ответственного пользователя СКЗИ
1	2	3	4	5	6	7

Приложение № 8

Форма акта
установки и ввода в эксплуатацию
средства криптографической защиты информации

АКТ
установки и ввода в эксплуатацию
средства криптографической защиты информации

№ _____ «___» _____ 20__ г.

Рабочая группа в составе:

_____ _____
_ — _____ _____
_ — _____ _____
_ —

(должность) *(Фамилия, Имя, Отчество)*

составила настоящий акт о том, что на основании заявки/служебной записки _____
_____
___

(№, дата документа на инсталляцию СКЗИ)

на технические средства и системы, приведенные в таблице 1, и находящиеся в пользовании
_____
__

(должность, фамилия, имя, отчество пользователя СКЗИ)

_____
___

(далее — пользователь СКЗИ) установлено средство криптографической защиты информации

(далее — СКЗИ)
_____

(наименование, версия, сборка СКЗИ)

_____
__в соответствии с эксплуатационно-технической документацией и введено в эксплуатацию.

Комплектация СКЗИ соответствует составу, приведенному в таблице 2.

Таблица 1.

Технические средства и системы, размещенные в помещении № _____,
расположенном по адресу _____

№ п/п	Вид оборудования	Тип	Учетный (заводской) номер
1	2	3	4
1	*Приводятся сведения о техническом средстве (например, системный блок, моноблок), на жесткий диск которого установлено СКЗИ*		
2	*Приводятся сведения о жестком диске, на который установлено СКЗИ*		

Таблица 2.

№ п/п	Наименование
1	2
1	*Сообщаются сведения о наименовании СКЗИ*
1.1	*Сообщаются сведения о специальном защитном знаке, размещенном на установочном компакт-диске с программным обеспечением и эксплуатационной документацией*
1.2	*Сообщаются сведения о формуляре на СКЗИ*
1.3	*Сообщаются сведения о сертификате соответствия на СКЗИ*

Проведена проверка работоспособности СКЗИ. Установленное программное обеспечение работает в штатном режиме, настройки СКЗИ соответствуют требованиям технической и эксплуатационной документации к ним и правам пользователя СКЗИ, а также параметрам, приведенным в приложении к настоящему акту *(при наличии таковых параметров)*.

Проведено обучение пользователя СКЗИ работе с СКЗИ.

Проведено обследование помещения № _____ на соответствие требованиям эксплуатационной и технической документации. Размещение и оборудование помещения отвечают требованиям технической и эксплуатационной документации к СКЗИ, позволяют установить СКЗИ и обеспечить сохранность СКЗИ, информации ограниченного доступа, и ключевых документов *(при наличии ключевых документов)*.

Корпус технического средства с установленным СКЗИ опечатан пломбами (номерными наклейками) № _____ от «___» _____ 20__ года. Замечания отсутствуют.

Криптоключ(и) № _____ установлены на ключевой носитель № _____ и переданы пользователю СКЗИ *(при наличии ключевых документов)*.

Лицо, проводившее установку: _____
(должность, подпись, расшифровка подписи)

Пользователь СКЗИ:
_____
(должность, подпись, расшифровка подписи)

Приложение № 9

Форма заявки
на деинсталляцию средств криптографической защиты информации

ЗАЯВКА
на деинсталляцию
средства криптографической защиты информации

Прошу деинсталлировать средство криптографической защиты информации _____
_____
___
(наименование средства криптографической защиты информации)
_____
___
с накопителя на жестких магнитных дисках _____
(модель, серийный номер)
_____
__ ,
встроенного в системный блок _____
(модель системного блока, серийный (инвентарный) номер системного блока)
АРМ, расположенной в помещении № _____, находящегося по адресу _____
_____
__,
в пользовании в связи с _____
(причина деинсталляции средства криптографической защиты информации)

_____
(должность) *(подпись)* *(расшифровка подписи)*

Приложение № 10

Форма акта
деинсталляции средства криптографической защиты информации

АКТ
деинсталляции
средства криптографической защиты информации

№ _____ «___» _____ 20__ г.

Рабочая группа в составе:

_____	_____
(должность)	*(Фамилия, Имя, Отчество)*
_____	_____
(должность)	*(Фамилия, Имя, Отчество)*
_____	_____
(должность)	*(Фамилия, Имя, Отчество)*

составила настоящий акт о том, что на основании заявки/служебной записки _____
_____
(№, дата документа на инсталляцию СКЗИ)

с технических средств и систем, приведенных в таблице 1, и находящихся в пользовании _____
_____
(должность, фамилия, имя, отчество пользователя СКЗИ)

произведена деинсталляция средства криптографической защиты информации (далее — СКЗИ)
_____
(наименование, версия, сборка СКЗИ)

следующим способом:[1] _____ .

[1] Способ уничтожения СКЗИ и ключевых документов регламентируется эксплуатационной и технической документацией к ним. В частности, к способам уничтожения относятся переформатирование, удаление программного обеспечения СКЗИ, физическое уничтожение носителей.

Таблица 1.

Технические средства и системы, размещенные в помещении № _____,
расположенном по адресу _____

№ п/п	Вид оборудования	Тип	Учетный (заводской) номер
1	2	3	4
1	*Приводятся сведения о техническом средстве (например, системный блок, моноблок), с жесткого диска которого деинсталлировано СКЗИ*		
2	*Приводятся сведения о жестком диске, с которого деинсталлировано СКЗИ*		

Ключевые документы № _____, находящиеся на ключевом носителе № _____ уничтожены (возвращены ответственному пользователю СКЗИ) *(при наличии ключевых документов)*.

Лицо, проводившее деинсталляцию:

_____
(должность, подпись, расшифровка подписи)

Пользователь СКЗИ:

_____
(должность, подпись, расшифровка подписи)

Приложение № 11

Форма журнала
поэкземплярного учета ключевых носителей, ключевых документов
Левый разворот

№ п/п	Наименование ключевого носителя, ключевого документа	Тип носителя	Номер ключевого носителя, номер ключевого документа	Номер экземпляра ключевого документа	Отметка о получении		
					Наименование юридического лица, от кого получены ключевой носитель, ключевой документ	Дата и номер сопроводительного письма, товарной накладной (иного документа о получении)	Ф.И.О. ответственного пользователя СКЗИ, получившего ключевой носитель, ключевой документ
1	2	3	4	5	6	7	8

Правый разворот

Отметка о выдаче				Отметка об уничтожении ключевых документов			Приме-чание
Ф.И.О. ответственного пользователя СКЗИ, производив-шего выдачу ключевого носителя, ключевого документа	Дата выдачи ключевого носителя, ключевого документа	Ф.И.О. работника, получившего ключевой носитель, ключевой документ, дата и подпись	Номер ключевого носителя или зоны СКЗИ, в которую введен ключевой документ	Дата уничтожения ключевых документов (с указанием наименования производимой процедуры)	Дата и номер акта об уничтожении ключевых документов	Ф.И.О. ответственного пользователя СКЗИ, уничтожение ключевых документов	
9	10	11	12	13	14	15	16