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»)

ПРИКАЗ

06.06.2019 № 01-05/221

г. Екатеринбург

Об утверждении Инструкции по организации и обеспечению криптографической защиты информации в ГАПОУ СО «Уральский политехнический колледж – МЦК»

С целью организации и обеспечения с помощью средств криптографической защиты информации безопасности информации в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» при их обработке в ГАПОУ СО «Уральский политехнический колледж - МЦК»

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Инструкцию по организации и обеспечению криптографической защиты информации в ГАПОУ СО «Уральский политехнический колледж – МЦК» (приложение).
2. Настоящий приказ довести до сведения пользователей СКЗИ, назначенных приказами от 03.06.2019 № 01-05/208 «Об утверждении перечня средств криптографической защиты информации, их мест размещения и их пользователей», от 03.06.2019 № 01-05/208 «Об утверждении перечня средств криптографической защиты информации, их мест размещения и их пользователей» под подпись.

Директор В.В. Камский

УТВЕРЖДЕНА

приказом ГАПОУ СО «Уральский политехнический колледж – МЦК»
от 06.06.2019 № 01-05/221

ИНСТРУКЦИЯ

по организации и обеспечению криптографической защиты информации в ГАПОУ СО «Уральский политехнический колледж – МЦК»

Оглавление

1. Общие положения

Настоящая Инструкция по организации и обеспечению криптографической защиты информации в ГАПОУ СО «Уральский политехнический колледж – МЦК» (далее – Инструкция) разработана в соответствии со следующими нормативными правовыми актами:

– Приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации 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»;

– Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное приказом ФСБ России № 66 от 09.02.2005 г.

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

а) 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;

б) 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;

в) средства электронной подписи;

г) 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;

д) 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;

е) 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 средств криптографической защиты информации

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 работников, использующих СКЗИ, работе с ними;

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

– проведение служебных проверок и составление заключений по фактам нарушения условий криптографической защиты информации.

2.1. Структура ответственных лиц

Структуру ответственных лиц по направлению 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 Российской Федерации.

Текущий 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 действующим законодательством Российской Федерации.

2.1.1 Ответственный пользователь средств криптографической защиты информации

Ответственный пользователь СКЗИ назначается приказом директора.

Организация и обеспечение функционирования СКЗИ возлагается на ответственного пользователя СКЗИ.

В должностную инструкцию ответственного пользователя СКЗИ включаются функциональные обязанности, соответствующие задачам, предусмотренным настоящей инструкцией.

Перед допуском к работе ответственный пользователь СКЗИ обязан ознакомиться с нормативными правовыми документами, регулирующими организацию и обеспечение криптографической защиты информации, с настоящей Инструкцией 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 работников, 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 действующего законодательства, эксплуатационной и технической документации к СКЗИ, настоящей Инструкции.

2.1.2. Пользователь средств криптографической защиты информации

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 безопасное хранение действующих резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей;

– сообщать о ставших им известными 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, хранилищ, личных печатей 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 с использованием СКЗИ информации ограниченного доступа.

Безопасность хранения и обработки с использованием СКЗИ информации ограниченного доступа 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 ограниченного доступа;

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

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

– немедленным принятием мер по предупреждению разглашения информации ограниченного доступа, 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, в которых осуществляется работа со средствами криптографической защиты информации

Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ и хранятся ключевые документы к ним, должны обеспечивать сохранность информации ограниченного доступа, СКЗИ и ключевых документов к ним.

Помещения, где установлены СКЗИ и хранятся ключевые документы к ним, должны удовлетворять требованиям, предъявляемым эксплуатационной и технической документацией к СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

Помещения, где установлены СКЗИ и хранятся ключевые документы к ним, 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 извне помещений, где установлены СКЗИ и хранятся ключевые документы к ним, их окна должны быть защищены. Окна помещений, расположенных на первых или последних этажах здания, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения.

Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ и хранятся ключевые документы к ним, должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

Помещения, где установлены СКЗИ и хранятся ключевые документы к ним, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания. Исправность сигнализации периодически необходимо проверять ответственному пользователю СКЗИ и с отметкой в журнале «Проверка средств охранной сигнализации, размещенных в помещении, форма которого приведена в Приложении 1.

Двери помещений, где установлены СКЗИ и хранятся ключевые документы к ним, должны подлежать опечатыванию, а также должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода работников.

Ключи от дверей, где установлены СКЗИ и хранятся ключевые документы к ним, подлежат учету, который осуществляет ответственный пользователь СКЗИ в журнале «Учет хранилищ и ключей от них», форма которого приведена в Приложении 2.

Печати, предназначенные для опечатывания хранилищ и помещений, где установлены СКЗИ и хранятся ключевые документы к ним, должны находиться у пользователей СКЗИ, ответственных за эти хранилища и помещения. Выдачу личных печатей работникам осуществляет ответственный пользователь СКЗИ с отметкой в журнале «Учет личных печатей, предназначенных для опечатывания», форма которого приведена в Приложении 3 к настоящей Инструкции.

Ответственный пользователь СКЗИ осуществляет учет хранилищ и ключей от них в журнале «Учет хранилищ и ключей от них», форма которого приведена в Приложении 1 к настоящей Инструкции.

Дубликаты ключей от помещений, где установлены СКЗИ и хранятся ключевые документы к ним, следует хранить ответственному пользователю СКЗИ в сейфе.

Учет дубликатов ключей от помещений, где установлены СКЗИ и хранятся ключевые документы к ним, осуществляется ответственным пользователем СКЗИ в журнале «Учет хранилищ и ключей от них», форма которого приведена в Приложении 2 к настоящей Инструкции.

По окончании рабочего дня помещение, где установлены СКЗИ и хранятся ключевые документы к ним, и установленные в нем хранилища должны быть закрыты и опечатаны, о чем производится запись в журналах «Опечатывание (вскрытие) помещений», форма которого приведена в Приложении 4 к настоящей инструкции, и «Опечатывание (вскрытие) хранилищ», форма которого приведена в Приложении 5 к настоящей Инструкции.

Ответственный пользователь СКЗИ осуществляет контроль за вскрытием, опечатыванием хранилищ с обязательной отметкой в журнале «Опечатывание (вскрытие) хранилищ». Хранение и выдачу ключей от хранилищ ответственный пользователь СКЗИ осуществляет в личном или специально выделенном хранилище.

При утрате ключа от хранилища или от входной двери в помещение, где установлены СКЗИ и хранятся ключевые документы к ним, 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, где установлены СКЗИ и хранятся ключевые документы к ним, 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, где установлены СКЗИ и хранятся ключевые документы к ним, или хранилища посторонних лиц, 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 информации ограниченного доступа и к замене скомпрометированных криптоключей.

В помещениях, где установлены СКЗИ и хранятся ключевые документы к ним, 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.

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

2.2.2. Требования к средствам криптографической защиты информации

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

2.2.3. Требования к АРМ, на которые инсталлируются средства криптографической защиты информации

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.

2.3.4. 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.

2.4. Эксплуатация средств криптографической защиты информации

2.4.1. Регистрация и учет средств криптографической защиты информации, ключевых документов и эксплуатационной и технической документации к ним

Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые носители, ключевые документы подлежат поэкземплярному учету в журнале «Поэкземплярный учет средств криптографической защиты информации, эксплуатационной и технической документации к ним», форма которого приведена в Приложении 6 к настоящей Инструкции, и в журнале «Поэкземплярный учет ключевых носителей, ключевых документов», форма которого приведена в Приложении 7 к настоящей Инструкции.

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 8, ведущимся непосредственно пользователем СКЗИ.

2.4.2. Выдача средств криптографической защиты информации, 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 «Поэкземплярный учет средств криптографической защиты информации, эксплуатационной и технической документации к ним», форма которого приведена в Приложении 6 к настоящей Инструкции, и в журнале «Поэкземплярный учет ключевых носителей, ключевых документов», форма которого приведена в Приложении 7 к настоящей Инструкции.

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов между пользователями СКЗИ допускается только по согласованию с ответственным пользователем СКЗИ с составлением акта приема-передачи СКЗИ (технической и эксплуатационной документации, ключевых носителей) без обязательной отметки в соответствующем журнале поэкземплярного учета. Акты приема-передачи СКЗИ подлежат хранению у ответственного пользователя СКЗИ.

2.4.3. Изготовление ключей для средств криптографической защиты информации

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.

Ключевые документы для СКЗИ или исходная ключевая информация для выработки ключевых документов изготавливаются Федеральной службой безопасности России на договорной основе лицами, имеющими лицензию ФСБ России на деятельность по изготовлению ключевых документов для СКЗИ. Изготовлять ключевые документы из исходной ключевой информации может ответственный пользователь СКЗИ, применяя штатные СКЗИ, если такая возможность предусмотрена эксплуатационной и технической документацией к СКЗИ.

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

2.4.4. Инсталляция средств криптографической защиты информации

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 настоящей Инструкцией. О факте проведения обучения делается отметка в журнале «Учет пользователей средств криптографической защиты информации», форма которого приведена в Приложении 9 к настоящей Инструкции.

По завершении инсталляции составляется Акт установки и ввода в эксплуатацию СКЗИ, форма которого приведена в Приложении 10. Акт установки и ввода в эксплуатацию СКЗИ подлежит хранению у ответственного пользователя СКЗИ. Сведения о пользователе СКЗИ заносятся в журнал «Учет пользователей средств криптографической защиты информации», форма которого приведена в Приложении 9 к настоящей Инструкции.

2.4.5. Порядок эксплуатации средств криптографической защиты информации

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, которой опечатан системный блок. После входа в операционную систему контролируется запуск антивирусного ПО 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 информацию ограниченного доступа, обрабатываемую 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.

2.4.6. Контроль за соблюдением эксплуатации средств криптографической защиты информации

Ежегодно комиссией, в которую входят работники 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 работники ГАПОУ СО «Уральский политехнический колледж – МЦК», в случаях нарушения установленного порядка криптографической защиты информации.

Состав комиссии определяет директор 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.

2.4.7. Порядок проведения служебной проверки по фактам нарушения правил эксплуатации средств криптографической защиты информации

В случае возникновения конфликтной ситуации и по фактам (подозрению) нарушения конфиденциальности информации, защищаемой с помощью СКЗИ, проводятся служебные проверки.

Основаниями проведения служебной проверки являются докладная записка работника, информационные письма (претензии) сторонних организаций, непосредственное обнаружение руководством факта (подозрения) нарушения конфиденциальности информации ограниченного доступа, защищаемой с помощью СКЗИ.

Служебная проверка назначается директором не позднее трех дней с момента поступления информации о факте нарушения конфиденциальности информации ограниченного доступа, защищаемой с помощью СКЗИ.

В ходе служебной проверки устанавливается:

действительно ли имело место нарушение конфиденциальности информации ограниченного доступа, защищаемой с помощью СКЗИ;

- 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, назначаемой приказом директора в составе не менее трех человек.

Срок завершения служебной проверки указывается в Приказе о проведении служебной проверки. Если срок не указан, то служебная проверка должна завершиться 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 проверки материалов оформляется письменное заключение (акт). В нем указываются основание и сроки проведения служебной проверки, состав комиссии, значимые обстоятельства, установленные в ходе расследования. Акт подписывается всеми членами комиссии и направляется руководителю.

2.4.8. 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. 2.4.7 настоящей Инструкции.

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

Скомпрометированные ключи по завершению расследования подлежат уничтожению в порядке, определенном настоящей Инструкцией.

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

2.4.9. Деинсталляция средств криптографической защиты информации

Деинсталляция СКЗИ с рабочих мест пользователей СКЗИ осуществляется на основании решения директора или по соответствующей заявке, форма которой приведена в Приложении 11 к настоящей Инструкции.

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 12 к настоящей Инструкции. 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 производится отметка в журнале «Поэкземплярный учет средств криптографической защиты информации, эксплуатационной и технической документации к ним», форма которого приведена в Приложении 6 к настоящей Инструкции.

2.4.10. Уничтожение средств криптографической защиты информации

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.

Основанием для уничтожения ключей является истечение срока их действия, вывод из эксплуатации СКЗИ, увольнение работника, снятие с работника 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 под подпись 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.

Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

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
«Проверка работы средств охранной сигнализации, размещенных в помещении _____

№ п/п	Дата	Вид работы	Ф.И.О. и подпись ответственного лица
1	2	3	4

Приложение 2

Форма журнала
«Учет хранилищ и ключей от них»

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

Приложение 3

Форма журнала
«Учет личных печатей, предназначенных для опечатывания»

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

Приложение 4

Форма журнала
«Опечатывание (вскрытие) помещений»

№ п/п	Номер печати, которой опечатано помещение	Дата и время опечатывания помещения	ФИО и подпись лица, опечатавшего помещение	Дата и время вскрытия помещения	Номер печати, которой было опечатано помещение	ФИО и подпись лица, вскрывшего помещение
1	2	3	4	5	6	7

Приложение 5

Форма журнала
«Опечатывание (вскрытие) хранилищ в помещении»

№ п/п	Номер печати, которой опечатано хранилище	Дата и время опечатывания хранилища	ФИО и подпись лица, опечатавшего хранилище	Дата и время вскрытия хранилища	Номер печати, которой было опечатано хранилище	ФИО и подпись лица, вскрывшего хранилище
1	2	3	4	5	6	7

Приложение 6

Форма журнала
«Поэкземплярный учет средств криптографической защиты информации, эксплуатационной и технической документации к ним»
(начало)

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним	Тип носителя	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним	Номера экземпляров	Отметка о получении		Отметка о выдаче	
					От кого получены	Дата и номер сопроводительного письма, товарной накладной (иного документа о получении)	Наименование юридического лица или ФИО работника, выдавшего СКЗИ, эксплуатационную и техническую документацию	ФИО работника, получившего СКЗИ, эксплуатационную и техническую документацию, дата и подпись
1	2	3	4	5	6	7	8	9

Форма журнала
«Поэкземплярный учет средств криптографической защиты информации, эксплуатационной и технической документации к ним» (продолжение)

Отметка о подключении, установке СКЗИ				Отметка об изъятии СКЗИ из аппаратных средств, выводе СКЗИ из эксплуатации			Примечание
ФИО 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 установки и ввода в эксплуатацию СКЗИ	Дата изъятия СКЗИ из аппаратных средств, деинсталляции СКЗИ (с указанием наименования производимой процедуры)	Дата и номер акта об изъятии СКЗИ из аппаратных средств, о деинсталляции СКЗИ	ФИО ответственного пользователя СКЗИ, производившего изъятие СКЗИ из аппаратных средств, деинсталляцию СКЗИ	
10	11	12	13	14	15	16	17

Приложение 7

Форма журнала
«Поэкземплярный учет ключевых носителей, ключевых документов»
(начало)

№ 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 сопроводи-тельного письма, товарной накладной (иного документа о получении)	ФИО ответственного пользователя СКЗИ, получившего ключевой носитель, ключевой документ
1	2	3	4	5	6	7	8

Форма журнала
«Поэкземплярный учет ключевых носителей, ключевых документов»
(продолжение)

Отметка о выдаче				Отметка об уничтожении ключевых документов			Примечание
ФИО ответственного пользователя СКЗИ, производившего выдачу ключевого носителя, ключевого документа	Дата выдачи ключевого носителя, ключевого документа	ФИО 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	ФИО ответственного пользователя СКЗИ, уничтожение ключевых документов	
9	10	11	12	13	14	15	16

Приложение 8

Форма журнала
«Технический (аппаратный) журнал»

№ 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 9

Форма журнала
«Учет пользователей средств криптографической защиты информации»

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

Приложение 10

Форма
Акт установки и ввода в эксплуатацию СКЗИ

УТВЕРЖДАЮ

Директор
ГАПОУ СО «Уральский
политехнический колледж – МЦК»

_____ В.В. Камский

«___» _____ 201_ г.

М.П.

АКТ
установки и ввода в эксплуатацию
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 приказа (заявки, служебной записки)

_____
(*№, дата документа на инсталляцию СКЗИ*)

в помещении № _____ на АРМ _____,
(*модель АРМ, № системного блока*)

находящейся в пользовании _____
_____,
(*должность, Фамилия Имя Отчество*)

установлено средство криптографической защиты информации (далее - СКЗИ) _____.

(*наименование, версия, сборка*)

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.

Проведено обучение пользователя СКЗИ работе с СКЗИ. Пользователь СКЗИ ознакомлен с эксплуатационной и технической документацией к СКЗИ, с нормативными правовыми актами и локальными актами, регламентирующими порядок эксплуатации СКЗИ. Пользователю СКЗИ разъяснены правила пользования СКЗИ, ключевыми документами и парольной информацией к СКЗИ.

Криптоключи № _____ переданы пользователю СКЗИ (установлены на ключевой носитель № _____.

Пользователю СКЗИ передана парольная карточка № _____.

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

АРМ с установленным СКЗИ опечатана номерной наклейкой № _____ от «___» _____ 20__ года. Замечания отсутствуют.

Лицо, проводившее инсталляцию:

_____

(*должность, подпись, расшифровка*)

Пользователь СКЗИ:

_____

(*должность , подпись, расшифровка*)

Приложение 11

Форма заявки
на деинсталляцию средств криптографической защиты информации

УТВЕРЖДАЮ

Директор
ГАПОУ СО «Уральский
политехнический колледж – МЦК»

_____ В.В. Камский

«___» _____ 201_ г.

М.П.

ЗАЯВКА
на деинсталляцию
средства криптографической защиты информации

Прошу деинсталлировать средство криптографической защиты информации

_____

(*наименование средства криптографической защиты информации)*

с АРМ _____, расположенной в помещении № _____
и находящейся в пользовании _____
(*должность, Фамилия Имя Отчество)*

в связи с _____
(причина деинсталляции средства криптографической защиты информации)

_____

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

Приложение 12

Форма акта
деинсталляции средства криптографической защиты информации

УТВЕРЖДАЮ

Директор
ГАПОУ СО «Уральский
политехнический колледж – МЦК»

_____ В.В. Камский

«___» _____ 201_ г.

М.П.

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 приказа (заявки, служебной записки) _____

(*№, дата документа на инсталляцию СКЗИ*)

в помещении № _____ на АРМ _____,

(*модель АРМ, № системного блока*)

находящейся в пользовании _____

(*должность, Фамилия Имя Отчество*)

_____ .

1. Произведена деинсталляция средства криптографической защиты информации (далее - СКЗИ) _____

(наименование СКЗИ)

путем[1] _____ .

2. Ключи № _____ , находящиеся на ключевом носителе № _____ уничтожены (возвращены ответственному пользователю СКЗИ).

Лицо, проводившее деинсталляцию:

_____

(должность, подпись, расшифровка)

Пользователь СКЗИ:

_____

(должность, подпись, расшифровка)

[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.

ЛИСТ ОЗНАКОМЛЕНИЯ

№ п/п	ФИО	Дата ознакомления	Подпись
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			
36			