ГАПОУ СО "УРГЗК"

Подписано цифровой подписью: ГАПОУ СО "УРГЗК"
Дата: 2021.06.29 11:17:33 +05'00'

Министерство образования и молодежной политики Свердловской области

государственное автономное профессиональное образовательное учреждение
Свердловской области
«Уральский горнозаводской колледж имени Демидовых»

Рассмотрена
на заседании Совета
автономного учреждения
№ протокола 3
«03» 07 2020 г.

Введена в действие приказом
№144-д от «03» 07 2020г.

ИНСТРУКЦИЯ

О ВЫПОЛНЕНИИ ТРЕБОВАНИЙ ПО РАЗМЕЩЕНИЮ, ХРАНЕНИЮ, ОХРАНЕ И ОРГАНИЗАЦИИ РЕЖИМА В ПОМЕЩЕНИЯХ, ГДЕ УСТАНОВЛЕНЫ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ИЛИ ХРАНЯТСЯ КЛЮЧЕВЫЕ ДОКУМЕНТЫ К НИМ В ГАПОУ СО «УрГЗК»

Невьянск 2020

1. Общие положения

1.1. Настоящая инструкция о выполнении требований по размещению, хранению, охране и организации режима в помещениях, где установлены средства криптографической защиты информации или хранятся ключевые документы к ним в государственном автономном профессиональном образовательном учреждении Свердловской области «Уральский горнозаводской колледж имени Демидовых» (далее – Инструкция) устанавливает единые требования по обеспечению безопасности функционирования средств криптографической защиты информации и определяет порядок учета, выдачи, хранения, уничтожения средств криптографической защиты информации (далее – СКЗИ), а также действия при компрометации ключей и восстановлении связи.

Порядок применения процедуры электронно-цифровой подписи может дополнительно уточняться заключаемыми со сторонними организациями договорами (соглашениями), при условии соблюдения требований настоящей инструкции.

1.2. Инструкция разработана в соответствии с Федеральным законом от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», приказом ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащих сведений составляющих государственную тайну», приказом ФСБ РФ от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005), приказом ФСБ России от 10.07.2014 № 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», постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.3. В настоящей инструкции использована следующая терминология:

Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Безопасность информации - состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системой, от внутренних или внешних угроз

Доступ к информации (доступ) - ознакомление с информацией, ее обработка; в частности, копирование, модификация или уничтожение информации.

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Криптографическая (шифровальная) защита – защита информации от ее несанкционированного доступа и модификации посторонних лиц при помощи алгоритмов криптографического преобразования.

Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.

Конфиденциальность – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Компрометация ключа – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Несанкционированный доступ (НСД) - доступ, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Обработка информации - совокупность операций сбора, накопления, ввода-вывода, приема-передачи, записи, хранения, регистрации, уничтожения, преобразования и отображения, осуществляемых над информацией.

Ответственный пользователь – должностное лицо, назначенное ответственным за обеспечение функционирования и безопасности криптосредств в главном управлении.

Пользователь криптосредств – субъект, наделенный правом применения средства криптографической защиты для выполнения возложенных обязанностей.

Ключевой документ (криптоключ) **–** сохраняемая в тайне**,** закрытая информация, используемая криптографичеким алгоритмом при шифровании/расшифровании сообщений, постановке и проверке цифровой подписи, вычислении кодов аутентичности.

Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (далее СКЗИ) - шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Шифровальные (криптографические) средства:

а) средства шифрования – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

б) средства имитозащиты – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) средства электронной цифровой подписи – аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;

г) средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

д) средства изготовления ключевых документов (независимо от вида носителя ключевой информации);

е) ключевые документы (независимо от вида носителя ключевой информации).

2. Организационные требования

2.1. Сотрудники ГАПОУ СО «УрГЗК», использующие при работе средства криптографической защиты информации, должны быть ознакомлены с требованиями настоящей инструкции и другими документами,

регламентирующими обеспечение безопасности функционирования криптосредств. Они несут персональную ответственность за несоблюдение требований указанных документов в соответствии с законодательством Российской Федерации.

2.2. Обеспечение функционирования и безопасности СКЗИ возлагается на ответственного пользователя криптосредств (далее – ответственный пользователь), имеющего необходимый уровень квалификации и назначаемого приказом руководителя.

На ответственного пользователя возлагается выполнение следующих обязанностей:

– учет криптосредств, эксплуатационной и технической документации с использованием условных наименований и регистрационных номеров;

– выдача средств криптографической защиты информации пользователям, согласно решения руководителя;

– при необходимости изготовление (генерация) ключевых документов из исходной ключевой информации;

– установка и ввод в эксплуатацию средств криптографической защиты информации в соответствии с эксплуатационной и технической документацией к этим средствам;

– контроль за соблюдением пользователями криптосредств, 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 криптосредств и ключевых документах к ним;

– организация работ по безопасному применению средств криптографической защиты информации в главном управлении;

– надежное хранение резервных ключевых документов, эксплуатационной и технической документации к криптосредствам,;

– принятие мер к минимизации возможных последствий при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

– обучение лиц, использующих криптосредства, работе с ними;

– учет лиц, допущенных к работе со средствами криптографической защиты информации (пользователи криптосредств);

– контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;

– разбирательства по фактам нарушения условий хранения и использования криптосредств, которые могут привести к нарушению или к снижению уровня защищенности информации;

2.3. К работе с СКЗИ пользователи допускаются приказом директора для исполнения обязанностей, связанных с использованием криптосредств.

Пользователи криптосредств обязаны:

- соблюдать требования по обеспечению безопасности функционирования СКЗИ;

- не разглашать информацию, к которой они допущены, в том числе сведения о криптосредствах, ключевых документах к ним и мерах защиты;

- не допускать снятие копий с ключевых документов;

- не допускать вывод ключевых документов на принтер;

- хранить ключевую информацию в сейфах и помещениях, гарантирующих их сохранность и конфиденциальность;

- не допускать записи на ключевой носитель посторонней информации;

- во время работы не оставлять ключевые документы без присмотра;

- сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;

- немедленно уведомлять руководителя о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к нарушению безопасности.

- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы Ответственному пользователю при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;

2.4. Ключевые документы для ГАПОУ СО «УрГЗК» или исходная ключевая информация для выработки ключевых документов изготавливаются ФСБ России на договорной основе или лицами, имеющими лицензию ФСБ России на деятельность по изготовлению шифровальных средств.

2.5. Изготовлять (генерировать) ключевые документы из исходной ключевой информации разрешено Ответственному пользователю криптосредств, если такая возможность предусмотрена эксплуатационной и технической документацией к СКЗИ.

3. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним

3.1. В помещениях, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее - режимные помещения) обеспечивается режим, препятствующий возможности неконтролируемого проникновения или пребывания в них лиц, не имеющих права доступа в режимные помещения, которое достигается путем:

а) оснащения режимных помещений входными дверьми с замками, обеспечения постоянного закрытия дверей режимных помещений на замок и их открытия только для санкционированного прохода, а также опечатывания режимных помещений по окончании рабочего дня или оборудование режимных помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии режимных помещений;

б) утверждения правил доступа в режимные помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

в) утверждения перечня лиц, имеющих право доступа в режимные помещения,

г) оборудования средствами пожарной сигнализации.

3.2. При оборудовании режимных помещений должны выполняться требования к размещению, монтажу криптосредств, а также другого оборудования, функционирующего с криптосредствами.

3.3. По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от помещений должны быть сданы под расписку в соответствующем журнале на пост охраны.

3.4. Системные блоки ПЭВМ со СКЗИ должны быть опечатаны для осуществления контроля их вскрытия.

3.5. Пользователи криптосредств хранят выданные им для использования ключевые документы в сейфах индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение. В случае отсутствия индивидуального сейфа по окончании рабочего дня Пользователь обязан сдать СКЗИ ответственному пользователю.

Хранение эксплуатационной и технической документации к СКЗИ, а также копии сертификатов открытых ключей ЭЦП в бумажном виде, осуществляется ответственным пользователем.

Хранение криптоключей и инсталляционного ПО СКЗИ допускается в одном сейфе с другими документами при условиях исключающих их непреднамеренное уничтожение или иное, непредусмотренное правилами применение.

4. Порядок учета и выдачи средств криптографической защиты информации

4.1. Должностные лица, допущенные к работе с криптосредствами, заносятся в журнал регистрации пользователей (Приложение №1). Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, а также ключевые документы подлежат учету в журнале поэкземплярного учета (Приложение №2). При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или

аппаратно-программные криптосредства подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие криптосредства учитываются также совместно с соответствующими аппаратными средствами.

Единицей поэкземплярного учета ключевых документов считается носитель с ключевой информацией. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

4.2. Все необходимые для работы экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета Пользователям криптосредств, несущим персональную ответственность за их сохранность.

4.3. Если в эксплуатационной и технической документации к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в криптосредствах, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале (Приложение № 3), непосредственно пользователем СКЗИ. В техническом (аппаратном) журнале отражают также данные об эксплуатации криптосредств и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на криптосредства не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к криптосредствам).

4.4. Передача криптосредств, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями криптосредств и ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета. Передача учтенных СКЗИ без санкции ответственного пользователя запрещается.

5. Порядок уничтожения средств криптографической защиты информации

5.1. СКЗИ, непригодные для дальнейшего использования, или надобность в использовании которых миновала, уничтожаются (утилизируются) по решению директора колледжа.

5.2. Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

5.3. Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), Data Key, Smart Card, Touch Memory и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

5.4. Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации.

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

5.5. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам.

5.6. Ключевые документы уничтожаются пользователями совместно с Ответственным пользователем криптосредств под расписку журнале поэкземплярного учета, при этом пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. Уничтожение большого объема ключевых документов может быть оформлено актом. Уничтожение по акту производит комиссия в составе не менее трех человек из числа лиц, допущенных к пользованию криптосредств. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих криптосредства носителей, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки журнале поэкземплярного учета.

6. Действия при компрометации или повреждении ключевой информации. Порядок проведения расследования

6.1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает необходимую защиту информации. Криптоключи, в отношении которых возникло подозрение в компрометации, необходимо немедленно вывести из действия, если иной

порядок не оговорен в эксплуатационной и технической документации к криптосредствам.

6.2. К событиям, связанным с компрометацией криптографических ключей, относятся:

– утеря (хищение) носителей ключевой информации, в том числе с последующим их обнаружением;

– увольнение сотрудника, имевшего доступ к ключевой информации;

– передача закрытых ключей по линиям связи;

– нарушение правил хранения или уничтожения криптоключа;

– несанкционированное или безучетное копирование ключевой информации;

– нарушение целостности печати на сейфе с ключевыми носителями;

– вскрытие фактов утечки (искажения или изменения) передаваемой информации;

– все случаи, когда нельзя достоверно установить, что произошло с носителем ключевой информации.

6.3. При наступлении любого из перечисленных случаев, или иных нарушениях, которые могут привести к компрометации криптоключей, пользователь должен прекратить использование СКЗИ и немедленно сообщить о произошедшем Ответственному пользователю.

6.4. Осмотр ключевых носителей посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

6.5. В каждом случае, по факту (или предполагаемой) компрометации ключевых документов, специально назначенной комиссией, проводится служебное расследование. Результатом расследования является квалификация или не квалификация данного события как компрометация.

В случаях недостачи, не предъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску. Мероприятия по розыску и локализации последствий компрометации ключевых документов организует и осуществляет руководитель.

6.6. О факте компрометации ключевой информации Пользователями совместно с Ответственным пользователем производится информирование всех заинтересованных участников информационного обмена.

6.7. Выведенные из действия скомпрометированные ключевые документы после проведения расследования уничтожаются, о чем делается соответствующая запись в журнале поэкземплярного учета.

6.8. Для своевременно восстановления связи создается резервный запас криптоключей в необходимом количестве. Использование резервных ключей осуществляется в случаях крайней необходимости, по решению Ответственного пользователя, согласованному с руководителем.

6.9. Так как любой ключевой носитель может быть поврежден или выйти из строя, для восстановления работы с СКЗИ Ответственным пользователем подготавливаются копии ключевых носителей с необходимыми ключами и сертификатами, которые подлежат основному учету и хранятся в его сейфе, в конвертах опечатанных печатями пользователей. Данные копии применяются с разрешения руководителя, в случае если по результатам расследования не было установлено факта компрометации.

6.10. Хранение резервных носителей ключевой информации, осуществляется отдельно от рабочих (актуальных) ключей, с целью обеспечения невозможности их одновременной компрометации.

Приложение № 1
к Инструкции
о выполнении требований
по размещению, хранению, охране
и организации режима в помещениях,
где установлены средства
криптографической защиты информации
или хранятся ключевые документы к ним
в ГАПОУ СО «УрГЗК»

Журнал регистрации пользователей СКЗИ

№ п.п.	Должность пользователя	Ф.И.О. пользователя	Дата регистрации	Дата выбытия	Примечание
1	2	3	4	5	6

В журнале фиксируется зарегистрированные пользователи.

Приложение № 2
к Инструкции
о выполнении требований
по размещению, хранению, охране
и организации режима в помещениях,
где установлены средства
криптографической защиты информации
или хранятся ключевые документы к ним
в ГАПОУ СО «УрГЗК»»

ЖУРНАЛ
поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов

№ п.п.	Наименование криптосредства, эксплуатационной и технической документации к ним, Вид носителя ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя криптосредств	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены криптосредства	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение № 3
к Инструкции
о выполнении требований
по размещению, хранению, охране
и организации режима в помещениях,
где установлены средства
криптографической защиты информации
или хранятся ключевые документы к ним
в ГАПОУ СО «УрГЗК»»

Технический (аппаратный) журнал

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