

бюджетное учреждение профессионального образования Ханты-Мансийского автономного
округа - Югры «Няганский технологический колледж»
(БУ «Няганский технологический колледж»)

П Р И К А З

«12» 09 2017 г.

№ 297

Нягань

***Об обращении с шифровальными (криптографическими)
средствами защиты информации***

В соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и «Инструкцией 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», утвержденной приказом ФАПСИ от 13.06.2001 г. №152,

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемую Инструкцию по обращению с шифровальными (криптографическими) средствами защиты информации в БУ «Няганский технологический колледж» (далее – Инструкция).
2. Утвердить прилагаемый Перечень работников, допущенных к работе с шифровальными (криптографическими) средствами защиты информации в БУ «Няганский технологический колледж» (далее – Перечень).
3. Ответственному за обеспечение безопасности персональных данных в информационных системах ознакомить работников, осуществляющих обработку персональных данных с прилагаемой Инструкцией.
4. Контроль за исполнением настоящего приказа оставляю.

Директор



В. В. Минаев

ИНСТРУКЦИЯ

по обращению с шифровальными (криптографическими) средствами защиты информации в БУ «Няганский технологический колледж»

1. Основные термины и определения

Закрытый ключ – криптоключ, который хранится пользователем системы в тайне.

Ключевой документ - физический носитель определенной структуры, содержащий криптоключи.

Компрометация криптоключа - утрата доверия к тому, что используемые криптоключи обеспечивают безопасность информации.

Контролируемая зона - территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа.

Криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

Модель нарушителя - предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Пользователь криптосредства - лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

Режимные помещения - помещения, где установлены криптосредства или хранятся ключевые документы к ним.

2. Общие положения

2.1 Настоящая Инструкция по обращению с шифровальными (криптографическими) средствами защиты информации (далее – Инструкция) в БУ «Няганский технологический колледж», определяет порядок обращения, размещения, хранения, учета и уничтожения, сертифицированных ФСБ России шифровальных (криптографических) средств защиты информации (далее - СКЗИ), а также ответственных за эксплуатацию СКЗИ.

2.2 Настоящая Инструкция разработана в соответствии с документами:

– Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное Приказом ФСБ России №66 от 9 февраля 2005 года;

– Приказ ФАПСИ при Президенте РФ №152 от 13 июня 2001 года «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».

2.3 Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности персональных данных, и не исключает обязательного выполнения их требований.

2.4 Аппаратные средства, с которыми осуществляется штатное функционирование криптосредств, а также аппаратные и аппаратно-программные криптосредства должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы).

2.5 Место опечатывания (опломбирования) криптосредств, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

2.6 Передача закрытых криптоключей по техническим средствам связи не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

3. Ответственные лица

3.1 В БУ «Няганский технологический колледж» ответственность за эксплуатацию сертифицированных СКЗИ, несут:

а) Ответственный за обеспечение безопасности персональных данных в информационных системах, на которого возлагаются задачи организации работ по:

- обеспечению корректного и безопасного функционирования СКЗИ;
- обеспечению корректной и безопасной эксплуатации СКЗИ;
- выработке соответствующих инструкций и ознакомление с ними пользователей СКЗИ;
- контролю работоспособности и соблюдения правил эксплуатации СКЗИ;
- обеспечению режима сохранности СКЗИ, эксплуатационной и технической документации.

б) Пользователи СКЗИ, на которых возлагаются задачи по:

- соблюдению правил корректной и безопасной эксплуатации СКЗИ;
- обеспечению режима сохранности СКЗИ и ключевых документов, переданных им.

4. Обязанности ответственного за защиту информации

4.1 Ответственный за защиту информации в ИС осуществляет:

- разработку 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;
- ознакомление лиц, использующих СКЗИ, правилам работы с ними с получением росписи о прохождении ознакомления;
- поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним;
- учет лиц, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности персональных данных (пользователей СКЗИ);
- контроль за соблюдением условий использования СКЗИ, предусмотренных эксплуатационной и технической документацией к ним;
- расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

5. Обращение с СКЗИ

5.1 Пользователи СКЗИ допускаются к работе с СКЗИ согласно «Перечню работников, допущенных к работе с шифровальными (криптографическими) средствами защиты информации в БУ «Няганский технологический колледж», только после ознакомления под роспись с настоящей Инструкцией и обучения правилам работы с СКЗИ.

5.2 Для организации и обеспечения безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации следует использовать СКЗИ.

5.3 При эксплуатации СКЗИ не допускается:

- снимать копии с ключевых документов, за исключением создания резервных копий ключевых документов;
- передавать содержимое документов ключевой информации или передавать сами документы лицам, не имеющим к ним допуска;
- выводить ключи проверки электронной подписи на дисплей, принтер или другие внешние устройства отображения информации;
- записывать на ключевой носитель постороннюю информацию;
- подключать к персональной электронно-вычислительной машине дополнительные устройства и соединители без соответствующего предписания на возможность их совместного использования;

- работать на персональной электронно-вычислительной машине, если во время его начальной загрузки не проходит встроенный тест, предусмотренный в персональной электронно-вычислительной машине;
- оставлять без контроля вычислительные средства, входящие в состав СКЗИ, при включенном питании и загруженном программном обеспечении СКЗИ;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- несанкционированно устанавливать, создавать и использовать на персональной электронно-вычислительной машине посторонние программы;
- осуществлять несанкционированное вскрытие системных блоков персональной электронно-вычислительной машине.

5.4 Ключевые документы, СКЗИ с введёнными криптографическими ключами относятся к материальным носителям, содержащие конфиденциальную информацию, при этом должны выполняться требования настоящей Инструкции и иных документов, регламентирующих порядок обращения с конфиденциальной информацией ограниченного распространения.

5.5 Криптоключи в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ.

5.6 О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать ответственному обеспечению безопасности персональных данных в информационных системах.

5.7 Ответственный за обеспечение безопасности персональных данных в информационных системах, обязан провести мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, передававшейся (хранящейся) с использованием СКЗИ.

6. Размещение технических средств с СКЗИ

6.1 Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним (далее - режимные помещения), должны обеспечивать сохранность криптосредств и ключевых документов к ним, исключать возможность неконтролируемого проникновения или пребывания в режимных помещениях посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

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

6.3 Требования к режимным помещениям:

- режимные помещения выделяются с учетом размеров контролируемой зоны организации;
- помещения должны быть оборудованы входными дверьми с замками, гарантирующими обеспечение постоянного закрытия дверей помещения на замок и их открытия только для санкционированного прохода;
- помещения должны опечатываться по окончании рабочего дня или должны быть оборудованы соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещения;
- окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, должны быть оборудованы металлическими решетками, или ставнями, или должны быть оборудованы соответствующими техническими устройствами, сигнализирующими о несанкционированном проникновении в помещение;
- окна помещений, должны быть защищены от просмотра режимных помещений извне.

6.4 Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать ответственному за обеспечение безопасности персональных данных в информационных системах и пользователям СКЗИ сохранность доверенных им СКЗИ, конфиденциальных документов и сведений, включая ключевую информацию, и свести к минимуму возможность неконтролируемого доступа к ним посторонних лиц.

7. Хранение СКЗИ

7.1 СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы, находящиеся у ответственного за обеспечение безопасности персональных данных в информационных системах и пользователей СКЗИ, должны храниться в месте, исключающем возможность несанкционированного доступа к ним (сейф, шкаф с замком и т.п.).

8. Учет СКЗИ

8.1 Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету ответственным за обеспечение безопасности персональных данных в информационных системах в «Журнале поэкземплярного учета шифровальных (криптографических) средств защиты информации, используемых в БУ «Няганский технологический колледж», эксплуатационной и технической документации к ним, ключевых документов» (Приложение 1).

9. Уничтожение СКЗИ

9.1 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).

9.2 Ключевые документы 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).

9.3 Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ

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

9.5 СКЗИ уничтожают (утилизируют) в соответствии с требованиями Положения ПКЗ-2005.

9.6 Намеченные к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали.

10. Компрометация действующих ключей к СКЗИ

10.1 К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

- явная компрометация ключей:
 - потеря ключевых носителей;
 - потеря ключевых носителей с их последующим обнаружением;
 - увольнение работников, имевших доступ к ключевой информации;
 - нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа;
- неявная компрометация ключей:
 - возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;

- нарушение печати на сейфе с ключевыми носителями;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).

10.20 нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшихся (хранящихся) с их использованием ПДн, пользователи СКЗИ обязаны сообщать ответственным за защиту информации в информационной системе.

11. Инструкция по восстановлению связи в случае компрометации действующих ключей к СКЗИ

11.1Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ.

11.2В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается по решению ответственного за защиту информации в информационной системе, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

11.30 нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать ответственным за защиту информации в информационной системе.

11.4Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

11.5В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

11.6Мероприятия по розыску и локализации последствий компрометации ключевых документов организует и осуществляет ответственный за защиту информации в информационной системе.

11.7Порядок оповещения пользователей СКЗИ о предполагаемой компрометации криптоключей и их замене устанавливается ответственным за защиту информации в информационной системе.

12. Обязанности пользователей СКЗИ

12.1Пользователи СКЗИ обязаны:

- обеспечить конфиденциальность информации о СКЗИ, других мерах защиты;
- точно соблюдать требования настоящей инструкции;
- надежно хранить эксплуатационную и техническую документацию к СКЗИ, ключевые документы, носители дистрибутивов криптосредств;
- сдать СКЗИ эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;
- своевременно выявлять и сообщать ответственному за обеспечение безопасности персональных данных в информационных системах о ставших известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- немедленно уведомлять ответственного за обеспечение безопасности персональных данных в информационных системах при утрате или недостачи криптосредств, ключевых

документов к ним, ключей от помещений, хранилищ, личных печатей, удостоверений, пропусков, при других фактах, которые могут привести к компрометации закрытых ключей.

13. Контроль соблюдения условий эксплуатации и работоспособности СКЗИ

13.1 Государственный контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации осуществляют федеральные органы безопасности.

13.2 В ходе государственного контроля изучаются и оцениваются:

- организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации;
- достигнутый уровень криптографической защиты конфиденциальной информации;
- условия использования СКЗИ.

13.3 Ответственный за обеспечение безопасности персональных данных в информационных системах, обязан контролировать выполнение указаний по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, а также условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатом ФСБ и настоящей Инструкцией.

ПЕРЕЧЕНЬ
работников, допущенных к работе
с шифровальными (криптографическими) средствами защиты информации
в БУ «Няганский технологический колледж»

№ п/п	Допущенные работники
1.	Казвирова Марина Геннадьевна, заместителя директора по финансам
2.	Гизатулина Галина Тимофеевна, зам по АХЧ
3.	Перминова Оксана Валерьевна, заместитель директора по учебной работе
4.	Мальцева Марина Геннадьевна ,секретарь учебной части
5.	Лягаев Андрей Юрьевич, системный администратор
6.	Шалаева Марина Александровна, бухгалтер
7.	Голубева Надежда Яковлевна, бухгалтер
8.	Карпова Лидия Владимировна, бухгалтер
9.	Бедрина Марина Сергеевна, специалист по государственному заказу (контрактный управляющий)
10.	Керимова Ирина Сергеевна Экономист
11.	Рогалева Ирина Владимировна Экономист

