Министерство общего и профессионального образования Ростовской области

государственное бюджетное профессиональное образовательное учреждение Ростовской области «Ростовское профессиональное училище № 5»

(ГБПОУ РО ПУ № 5)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

344091, Ростовская область, г. Ростов-на-Дону, ул. Малиновского, 5 в/169

П Р И К А З

20.07.2018 № 77

Ростов-на-Дону

Об утверждении инструкций

и журнала поэкземплярного учета

средств криптографической защиты информации

В целях исполнения требований «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», утвержденной приказом ФАПСИ от 13 июня 2001 г. №152,

ПРИКАЗЫВАЮ:

1. Назначить Антонову Наталью Александровну – заместителя директора по учебно – производственной работе, ответственной за организацию работ по криптографической защите информации и эксплуатацию СКЗИ (ответственным пользователем криптосредств) в ГБПОУ РО ПУ № 5.

2. Утвердить Инструкцию ответственного за организацию работ по криптографической защите информации и эксплуатацию средств криптографической защиты информации в ГБПОУ РО ПУ № 5 (Приложение № 1).

 3. Ответственному за организацию работ по криптографической защите информации и эксплуатацию средств криптографической защиты информации ознакомиться под роспись и руководствоваться в своей деятельности Инструкцией ответственного за организацию работ по криптографической защите информации и эксплуатацию средств криптографической защиты информации.

4. Утвердить Инструкцию по обращению с сертифицированными средствами криптографической защиты информации, предназначенными для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в ГБПОУ РО ПУ № 5, и криптоключам к ним (Приложение № 2).

 5. Ответственному за организацию работ по криптографической защите информации и эксплуатацию средств криптографической защиты информации ознакомить под роспись пользователей СКЗИ с Инструкцией по обращению с СКЗИ.

6. Утвердить перечень работников, допущенных к работе с сертифицированными средствами криптографической защиты информации, предназначенными для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в ГБПОУ РО ПУ № 5 (Приложение № 3).

7. Утвердить форму Журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (Приложение № 4).

8. Утвердить Инструкцию по восстановлению связи в случае компрометации действующих ключей криптосредствам в ГБПОУ РО ПУ № 5 (Приложение N 5) и ознакомить с ней всех пользователей криптосредств из перечня работников, допущенных к работе с сертифицированными СКЗИ (Приложение № 5).

9. Утвердить перечень помещений, в которых эксплуатируются СКЗИ (Приложение № 6).

10. Утвердить форму Журнала учёта ключей от помещений, в которых осуществляется эксплуатация и хранение СКЗИ (Приложение № 7).

11. Назначить Ефремову Марину Игоревну, заведующего хозяйством, ответственной за ведение Журнала учёта ключей от помещений, в которых осуществляется эксплуатация и хранение СКЗИ.

12. Утвердить типовую форму акта об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов (Приложение № 8).

Директор М.Н. Греховодова

Приложение № 1

к приказу
ГБПОУ РО ПУ № 5
от 20.07.2018 № 77

ИНСТРУКЦИЯ

ответственного за организацию работ по криптографической защите информации и эксплуатацию средств криптографической защиты информации в ГБПОУ РО ПУ № 5

1. Общие положения

1.1. Настоящий документ определяет основные права и обязанности ответственного за организацию работ по криптографической защите информации и эксплуатацию средств криптографической защиты информации (далее - СКЗИ) в ГБПОУ РО ПУ № 5.

1.2. Ответственный за организацию работ по криптографической защите информации и эксплуатацию СКЗИ назначается приказом директора из числа работников ГБПОУ РО ПУ № 5.

1.3. Ответственный за организацию работ по криптографической защите информации и эксплуатацию СКЗИ получает указания непосредственно от директора ГБПОУ РО ПУ № 5.

1. Обязанности ответственного за организацию работ по криптографической защите информации и эксплуатацию СКЗИ

2.1. Вести поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним в соответствующем журнале.

2.2. Вести учет лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности информации в ГБПОУ РО ПУ № 5 (пользователи криптосредств), в соответствующем журнале.

2.3. Организовывать установку и ввод в эксплуатацию криптосредств в соответствии с эксплуатационной и технической документацией к этим средствам.

2.4. Осуществлять контроль соблюдения условий использования криптосредств, установленных в эксплуатационной и технической документации на СКЗИ.

2.5. Не разглашать информацию, к которой он допущен, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты.

2.6. Соблюдать требования к обеспечению безопасности информации в ГБПОУ РО ПУ № 5, требования к обеспечению безопасности криптосредств и ключевых документов к ним.

2.7. Сообщать о ставших ему известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним директору или иному уполномоченному им лицу.

2.8. Немедленно уведомлять директора или иное уполномоченное им лицо о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, печатей и о других фактах, которые могут привести к разглашению информации ограниченного доступа.

2.9. Сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств.

2.10. Осуществлять ведение журнала поэкземплярного учёта средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов и журнала учёта хранилищ с ключевыми документами.

1. Права ответственного за организацию работ по криптографической защите информации и эксплуатацию СКЗИ

3.1. Инициировать разбирательство и составление заключений по фактам нарушения условий использования криптосредств, которые могут привести к нарушению безопасности информации или другим нарушениям, приводящим к снижению уровня защищенности ГБПОУ РО ПУ № 5.

3.2. Инициировать разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

1. Ответственность

4.1. Ответственный за организацию работ по криптографической защите информации и эксплуатацию СКЗИ несет материальную, дисциплинарную и административную ответственность:

* за неисполнение либо ненадлежащее исполнение должностных обязанностей;
* за нарушение федерального законодательства по защите информации;
* за превышение должностных полномочий и злоупотребление ими;
* за разглашение информации, к которой он допущен в рамках выполнения своих функциональных обязанностей, посторонним лицам.

Приложение № 2

к приказу
ГБПОУ РО ПУ № 5
от 20.07.2018 № 77

ИНСТРУКЦИЯ
по порядку обращения с сертифицированными средствами криптографической защиты информации, предназначенными для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в ГБПОУ РО ПУ № 5,

и криптоключами к ним

1. Общие положения

1.1. Инструкция по порядку обращения с сертифицированными средствами криптографической защиты информации (далее - СКЗИ), предназначенными для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее - Информация), обрабатываемой в ГБПОУ РО ПУ № 5 (далее - Училище), и криптоключами к ним регламентирует порядок обращения с криптосредствами в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты Информации.

1.2. Под криптосредствами настоящей Инструкции понимается шифровальное (криптографическое) средство, предназначенное для защиты информации.

1.3. К криптосредствам (шифровальным, криптографическим средствам) относятся:

1.3.1. 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.

1.3.2. Средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

1.3.3 Средства электронной 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.

1.3.4 Средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

1.3.5. Средства изготовления ключевых документов (независимо от вида носителя ключевой информации).

1.3.6. Ключевые документы (независимо от вида носителя ключевой информации).

1.4. В настоящей Инструкции используются следующие понятия и определения:

1.4.1. Доступ к информации – возможность получения информации и ее использования.

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

1.4.3. Ключевой документ – физический носитель определенной структуры, содержащий криптоключи.

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

1.4.5. Контролируемая зона – пространство, в пределах которого осуществляется контроль пребывания и действий лиц и (или) транспортных средств. Границей контролируемой зоны может быть: периметр охраняемой территории ГБПОУ РО ПУ № 5, ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

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

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

1.4.8. Модель угроз – перечень возможных угроз.

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

1.4.10. Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

1.5. Для обеспечения безопасности Информации при её обработке в ИС Училища должны использоваться сертифицированные в системе сертификации ФСБ России криптосредства (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации).

1.6. Класс криптосредства определяется в соответствии с Приказом Федеральной службы безопасности Российской Федерации (ФСБ России) [от 10.07.2014 N378 «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»](http://docs.cntd.ru/document/420208484).

1. Организационная структура

Безопасность обработки Информации в Училище с использованием криптосредств организует и обеспечивает Ответственный за организацию работ по криптографической защите информации и эксплуатацию СКЗИ в Училище.

1. Обязанности пользователей криптосредств

3.1. Пользователи криптосредств допускаются к работе с ними только после ознакомления под роспись с настоящей Инструкцией, другими документами, регламентирующими организацию и обеспечение безопасности Информации при ее обработке в Училище.

3.2. При наличии двух и более пользователей криптосредств обязанности между ними должны быть распределены с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

3.3. Пользователи криптосредств обязаны:

3.3.1. Не нарушать конфиденциальность закрытых ключей.

3.3.2. Не допускать снятие копий с ключевых документов, содержащих закрытые ключи.

3.3.3. Не допускать вывод закрытых ключей на дисплей (монитор) автоматизированного рабочего места (далее - АРМ) или принтер.

3.3.4. Не допускать записи на ключевой документ посторонней информации.

3.3.5. Не допускать установки ключевых документов на другие АРМ.

3.3.6. Обеспечить конфиденциальность информации о криптосредствах, других мерах защиты.

3.3.7. Точно соблюдать требования к обеспечению безопасности Информации, требования к обеспечению безопасности криптосредств и ключевых документов к ним.

3.3.8. Хранить ключевые документы к криптосредствам в защищаемых хранилищах.

3.3.9. Сдавать ключевые документы к криптосредствам при увольнении или отстранении от исполнения обязанностей.

3.3.10. Своевременно выявлять и сообщать Ответственному за эксплуатацию СКЗИ в ГБПОУ РО ПУ № 5 о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним.

3.3.11. Немедленно уведомлять Ответственного за организацию работ по криптографической защите информации и эксплуатацию СКЗИ в ГБПОУ РО ПУ № 5 принимать меры по предупреждению нарушения конфиденциальности Информации при утрате или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, печатей, при других фактах, которые могут привести к компрометации закрытых ключей, снижению уровня защищенности обрабатываемой Информации.

1. Учет ключевых документов

4.1. Ключевые документы подлежат поэкземплярному учету. Единицей поэкземплярного учета ключевых документов считается ключевой носитель информации.

4.2. Все экземпляры ключевых документов выдаются пользователям криптосредств под подпись в соответствующем журнале поэкземплярного учета.

4.3. Передача ключевых документов допускается только между пользователями криптосредств и Ответственным за эксплуатацию СКЗИ под подпись в соответствующем Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов. Аналогичная передача между пользователями криптосредств осуществляется с письменного разрешения Ответственного за организацию работ по криптографической защите информации и эксплуатацию СКЗИ.

4.4. Для исключения компрометации ключевых документов на период отсутствия пользователя и в нерабочее время, ключевые документы убираются в защищенные хранилища (ящики, шкафы) индивидуального пользования, которые, в свою очередь, закрываются на ключ и опечатываются.

4.5. Учет эксплуатационной и технической документации к криптосредствам:

4.5.1. Эксплуатационная и техническая документация к криптосредствам подлежит поэкземплярному учету.

4.5.2. Все экземпляры эксплуатационной и технической документации к криптосредствам выдаются пользователям криптосредств под подпись.

4.5.3. Передача эксплуатационной и технической документации к криптосредствам допускается только между пользователями криптосредств и Ответственным пользователем за эксплуатацию СКЗИ под подпись. Аналогичная передача между пользователями криптосредств осуществляется с санкции Ответственного за организацию работ по криптографической защите информации и эксплуатацию СКЗИ.

4.6. Плановая смена ключевых документов:

4.6.1. Заказ на изготовление очередных ключевых документов, их изготовление и получение пользователем производится заблаговременно для своевременной замены действующих ключевых документов.

4.7. Внеплановая смена ключевых документов:

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

4.8. Уничтожение ключевых документов:

4.8.1. Ключевые документы с неиспользованными или выведенными из действия криптоключами (исходной ключевой информацией) возвращаются Ответственному за организацию работ по криптографической защите информации и эксплуатацию СКЗИ, или по его указанию уничтожаются на месте пользователями криптосредств.

4.8.2. Уничтожение ключевых документов производится путем стирания (разрушения) криптоключей без повреждения ключевого документа.

4.8.3. Бумажные и прочие сгораемые ключевые документы уничтожаются путем сжигания или с помощью любых бумагорезательных машин с составлением соответствующего акта.

4.8.4. Ключевые документы уничтожаются в сроки, указанные в эксплуатационной и технической документации соответствующих криптосредств. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы уничтожаются не позднее 10 (десяти) суток после вывода их из действия (окончания срока действия).

4.8.5. Пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) ключевые документы. После уничтожения пользователи криптосредств уведомляют об этом Ответственного за организацию работ по криптографической защите информации и эксплуатацию СКЗИ.

4.9. Уничтожение эксплуатационной и технической документации к криптосредствам:

4.9.1. Эксплуатационная и техническая документация к криптосредствам уничтожается путем сжигания или с помощью любых бумагорезательных машин с составлением соответствующего акта.

1. Техническое обслуживание криптосредств

5.1. Техническое обслуживание криптосредств, а также другого оборудования, функционирующего с криптосредствами, смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

5.2. На время отсутствия пользователей криптосредства, а также другое оборудование, функционирующее с криптосредствами, при наличии технической возможности, выключается, отключается от линии связи и убирается в опечатываемые хранилища. В противном случае необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

1. Порядок доступа к хранилищам

6.1. Эксплуатация хранилищ:

6.1.1. Пользователи криптосредств хранят эксплуатационную и техническую документацию к криптосредствам, ключевые документы в хранилищах (ящиках, шкафах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

6.1.2. Должно быть предусмотрено раздельное безопасное хранение пользователями криптосредств действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

6.2. При необходимости доступа к содержимому хранилища работник, ответственный за данное хранилище, проверяет целостность хранилища, открывает механический замок хранилища с использованием ключа.

6.3. По окончании работы работник закрывает и опечатывает хранилище, за которое он ответственен.

6.4. Печати, предназначенные для опечатывания хранилищ, должны находиться у работников, ответственных за данные хранилища.

1. Контроль безопасности криптосредств

Текущий контроль за организацией и обеспечением функционирования криптосредств возлагается на ответственного за организацию работ по криптографической защите информации и эксплуатацию СКЗИ в пределах его полномочий.

1. Ответственность за нарушение требований

8.1. Пользователи криптосредств несут персональную ответственность за сохранность полученных криптосредств, эксплуатационной и технической документации к криптосредствам, ключевых документов, за соблюдение положений настоящей Инструкции.

8.2. Ответственный за организацию работ по криптографической защите информации и эксплуатацию СКЗИ несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки Информации с использованием криптосредств лицензионным требованиям и условиям эксплуатационной и технической документации к криптосредствам, а также настоящей Инструкции.

Приложение № 3

к приказу
ГБПОУ РО ПУ № 5
от 20.07.2018 № 77

Перечень работников, допущенных к работе с сертифицированными средствами криптографической защиты информации

|  |  |  |
| --- | --- | --- |
| № п/п | Должность | Ф.И.О. |
| 1. | Директор | Греховодова Марина Николаевна |
| 2. | Заместитель директора по учебно-производственной работе | Антонова Наталья Александровна |
| 3. | Главный бухгалтер | Цагикян Лина Эдуардовна |
| 4. | Заместитель главного бухгалтера | Лебеденко Елена Юрьевна |
| 5. | Экономист | Алаторцева Римма Амаяковна |
| 6. | Заведующий учебной (учебно-производственной) мастерской | Иванова Елена Валерьевна |
| 7. | Секретарь | Миронова Марина Ивановна |

Приложение № 5

к приказу
ГБПОУ РО ПУ № 5
от 20.07.2018 № 77

ИНСТРУКЦИЯ

по восстановлению связи в случае компрометации действующих ключей к криптосредствам в Училище

1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию Владельца и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:
* утрата (хищение) носителей ключевой информации (далее - НКИ), в том числе - с последующим их обнаружением;
* увольнение (переназначение) работников, имевших доступ к ключевой информации;
* передача секретных ключей по линии связи в открытом виде;
* нарушение правил хранения криптоключей;
* вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);
* отрицательный результат при проверке наложенной электронной подписи;
* несанкционированное или безучётное копирование ключевой информации;
* все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).
1. События 1-5 п.1 должны трактоваться как безусловная компрометация действующих ключей. Остальные события требуют специального расследования в каждом конкретном случае.
2. При наступлении любого из перечисленных выше событий владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) Ответственному за эксплуатацию криптографических средств защиты информации лично, по телефону, электронной почте или другим доступным способом. В любом случае владелец ключа обязан убедиться, что его сообщение получено и прочтено адресатом.
3. При подтверждении факта компрометации действующих ключей Пользователь обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей в течение трёх рабочих дней.
4. Для восстановления конфиденциальной связи после компрометации действующих ключей Пользователь получает новые ключи.

Приложение № 6

к приказу
ГБПОУ РО ПУ № 5
от 20.07.2018 № 77

Перечень помещений, в которых эксплуатируются СКЗИ

|  |  |  |
| --- | --- | --- |
| № | Наименование помещения | Ответственный |
| 1.4. | Бухгалтерия | Цагикян Лина Эдуардовна |
| 1.5.1. | Кабинет заместителя директора по учебно-производственной работе – ответственной за эксплуатацию СКЗИ | Антонова Наталья Александровна |