Государственное автономное образовательное учреждение
профессионального образования города Севастополя
«Институт развития образования»
(ГАОУ ПО ИРО)

ПРИКАЗ

«22» июля 2024 г. № 516

«О назначении ответственных лиц»

С целью организации и проведения мероприятий по предупреждению нарушений правил эксплуатации средств хранения, обработки или передачи компьютерной и иной информации и информационно-телекоммуникационных сетей, обеспечения и выполнения обязательных требований хранения информации и персональных данных в ГАОУ ПО «Институт развития образования» в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», требованиями к эксплуатации СКЗИ в соответствии с ЭТД к ним (приказ ФСБ России от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и использовании шифровальных (криптографических) средств защиты информации и иных нормативных документов в области защиты персональных данных при их обработке в информационных системах персональных данных», приказа 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 содержащей сведений, составляющих государственную тайну» **приказываю:**

1. Назначить ответственными за организацию и контроль соблюдения в ГАОУ ПО «Институт развития образования» правил эксплуатации и хранения СКЗИ, ключевых документов, аппаратных средств, с которыми осуществляется штатное функционирование СКЗИ: главного специалиста по защите информации Дементьева Александра Витольдовича, специалиста по защите информации Воронова Евгения Сергеевича.

2. Ответственным лицам, указанным в п. 1 Приказа. в процессе проведения контрольных мероприятий:

2.1. Проводить ежедневную проверку соблюдения правил:

2.1.1. Эксплуатации СКЗИ в соответствии с требованиями приказа ФСБ России от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и использовании шифровальных (криптографических) средств защиты информации и иных нормативных документов в области защиты персональных данных при их обработке в информационных системах персональных данных». (Приложение № 1)

2.1.2. Хранения СКЗИ и ключевых документов, исключающего бесконтрольный доступ к ним, а также их неправомерное уничтожение в соответствии с п. 30 приказа 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 содержащей сведений, составляющих государственную тайну». (Приложение № 2)

2.2. Оборудовать аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, и их хранилища, места хранения и обработки персональных данных, конфиденциальной информации, информации с ограниченным доступом средствами контроля за их вскрытием (склейки, опечатывающие устройства и т.п.), в соответствии с п. 31 приказа 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 содержащей сведений, составляющих государственную тайну». (Приложение № 2)

2.3. Принять другие необходимые (правовые, организационные, технические) меры для защиты и обеспечения безопасности персональных данных и информации от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных и информации, а также иных неправомерных действий в отношении персональных данных и информации.

2.4. Результаты проведения контрольных мероприятий оформлять актом (Приложение № 3).

2.5. При необходимости подготовить заявку на закупку необходимых материалов, оборудования, приспособлений, средств контроля за вскрытием (склейки, опечатывающие устройства и т.п.) аппаратных средств, с которыми осуществляется штатное функционирование СКЗИ, и их хранилищ, мест хранения и обработки персональных данных, конфиденциальной информации, информации с ограниченным доступом.

2.6. Завести журнал учета средств контроля за вскрытием аппаратных средств, с которыми осуществляется штатное функционирование СКЗИ, и их хранилищ, мест хранения и обработки персональных данных, конфиденциальной информации, информации с ограниченным доступом. Приложение № 4).

2.7. О проведенных контрольных мероприятиях еженедельно (каждую пятницу) докладывать заместителю директора по безопасности и финансово-экономической деятельности Котельникову Д.В., а в случае его отсутствия (нахождение в отпуске, временная нетрудоспособность, командировка) лицу, его замещающему.

3. Отделу по закупочной деятельности (Воронина Ю.Ю.) осуществить закупку в соответствии с заявкой (п. 2.5 Приказа) в пределах доведенных лимитов денежных средств.

4. Центру кадрового учета, делопроизводства и канцелярии (Коптенко Е.И.) приказ довести до заинтересованных лиц.

5. Центру информационно-программного обеспечения (Гладких И.Ю.) разместить данный приказ на сайте ГАОУ ПО «Институт развития образования».

6. Предупреждаю о персональной ответственности за невыполнение требований данного приказа.

7. Контроль за исполнением настоящего приказа возложить на начальника Центра информационно-программного обеспечения Гладких И.Ю.

Исполняющий обязанности директора Д.В. Котельников

Приложение № 1
к приказу ГАОУ ПО ИРО
№ _____ от _____

Приказ ФСБ РФ от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)" (с изменениями и дополнениями)

С изменениями и дополнениями от:

12 апреля 2010 г.

В целях определения порядка разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, приказываю:

1. Утвердить прилагаемое Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

2. Приказ ФАПСИ от 23 сентября 1999 года N 158 (зарегистрирован Минюстом России 28 декабря 1999 года, регистрационный N 2029) не применять с даты вступления в силу настоящего приказа.

Директор Н. Патрушев

Зарегистрировано в Минюсте РФ 3 марта 2005 г.
Регистрационный N 6382

Приложение
к приказу ФСБ РФ
от 9 февраля 2005 г. N 66

Положение
о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)

С изменениями и дополнениями от:

12 апреля 2010 г.

Настоящее Положение разработано во исполнение Федерального закона от 3 апреля 1995 года N 40-ФЗ "О федеральной службе безопасности"*(1) и Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 года N 960*(2).

I. Общие положения

1. Положение регулирует отношения, возникающие при разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (далее - информация конфиденциального характера).

Приказ ФСБ РФ от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и...

2. Шифровальные (криптографические) средства защиты информации конфиденциального характера в настоящем Положении именуются средствами криптографической защиты информации (далее - СКЗИ). К СКЗИ относятся*(3):

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).

3. Настоящим Положением необходимо руководствоваться при разработке, производстве, реализации и эксплуатации средств криптографической защиты информации конфиденциального характера в следующих случаях:

если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;

при организации криптографической защиты информации конфиденциального характера в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации (далее - государственные органы);

при организации криптографической защиты информации конфиденциального характера в организациях независимо от их организационно-правовой формы и формы собственности при выполнении ими заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд (далее - организации, выполняющие государственные заказы);

если обязательность защиты информации конфиденциального характера возлагается законодательством Российской Федерации на лиц, имеющих доступ к этой информации или наделенных полномочиями по распоряжению сведениями, содержащимися в данной информации;

при обрабатывании информации конфиденциального характера, обладателем которой являются государственные органы или организации, выполняющие государственные заказы, в случае принятия ими мер по охране ее конфиденциальности путем использования средств криптографической защиты;

при обрабатывании информации конфиденциального характера в государственных органах и в организациях, выполняющих государственные заказы, обладатель которой принимает меры к охране ее конфиденциальности путем установления необходимости криптографической защиты данной информации.

4. Требования Положения ПКЗ-2005 носят рекомендательный характер при разработке, производстве, реализации и эксплуатации:

средств криптографической защиты информации, доступ к которой ограничивается по решению обладателя, пользователя (потребителя) данной информации, собственника (владельца) информационных ресурсов (информационных систем) или уполномоченных ими лицами, не

являющихся государственными органами или организациями, выполняющими государственные заказы;

средств криптографической защиты информации открытых и общедоступных государственных информационных ресурсов Российской Федерации;

средств электронной цифровой подписи, предназначаемых для использования в электронном документообороте, информация которого не относится к информации конфиденциального характера;

информационно-телекоммуникационных систем, реализующих функции криптографической защиты информации, не относящейся к информации конфиденциального характера.

5. Настоящее Положение не регулирует отношения, связанные с экспортом и импортом СКЗИ, и не распространяется на использование шифровальных (криптографических) средств иностранного производства.

6. Режим защиты информации путем использования СКЗИ устанавливается обладателем информации конфиденциального характера, собственником (владельцем) информационных ресурсов (информационных систем) или уполномоченными ими лицами на основании законодательства Российской Федерации.

7. При организации обмена информацией конфиденциального характера, участниками которого являются государственные органы и организации, выполняющие государственные заказы, необходимость криптографической защиты информации и выбор применяемых СКЗИ определяются государственными органами или организациями, выполняющими государственные заказы.

8. При организации обмена информацией, доступ к которой ограничивается по решению обладателя, пользователя (потребителя) данной информации, собственника (владельца) информационных ресурсов (информационных систем), не являющихся организациями, выполняющими государственные заказы, или уполномоченными ими лицами (за исключением информации, содержащей сведения, к которым в соответствии с законодательством Российской Федерации не может быть ограничен доступ), необходимость ее криптографической защиты и выбор применяемых СКЗИ определяются соглашениями между участниками обмена.

9. Необходимость криптографической защиты информации конфиденциального характера при ее обработке и хранении без передачи по каналам связи, а также выбор применяемых СКЗИ определяются обладателем или пользователем (потребителем) данной информации.

10. СКЗИ должны удовлетворять требованиям технических регламентов, оценка выполнения которых осуществляется в порядке, определяемом Федеральным законом от 27 декабря 2002 года N 184-ФЗ "О техническом регулировании"*(4).

11. Качество криптографической защиты информации конфиденциального характера, осуществляемой СКЗИ, обеспечивается реализацией требований по безопасности информации, предъявляемых к СКЗИ, ключевой системе СКЗИ, а также к сетям связи (системам), используемым СКЗИ с целью защиты информации при ее передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении (далее - сети (системы) конфиденциальной связи) и условиям размещения СКЗИ при их использовании (далее - требования по безопасности информации).

12. Для криптографической защиты информации конфиденциального характера должны использоваться СКЗИ, удовлетворяющие требованиям по безопасности информации, устанавливаемым в соответствии с законодательством Российской Федерации.

Реализация в конкретных образцах СКЗИ и сетях (системах) конфиденциальной связи требований по безопасности информации возлагается на разработчика СКЗИ.

II. Порядок разработки СКЗИ

Приказ ФСБ РФ от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и...

13. Задание разработки СКЗИ для федеральных государственных нужд осуществляется государственным заказчиком по согласованию с ФСБ России.

14. Разработка СКЗИ в интересах негосударственных организаций может осуществляться по заказу конкретного потребителя информации конфиденциального характера или по инициативе разработчика СКЗИ. При этом в качестве заказчика СКЗИ может выступать любое лицо.

15. Разработка СКЗИ осуществляется путем постановки и проведения необходимых научно-исследовательских работ (далее - НИР) по исследованию возможности создания нового образца СКЗИ и опытно-конструкторских работ (далее - ОКР) по созданию нового образца СКЗИ или модернизации действующего образца СКЗИ.

16. НИР по исследованию возможности создания нового образца СКЗИ проводится в соответствии с тактико-техническим заданием (далее - ТТЗ) или техническим заданием (далее - ТЗ), разработанным на основе национальных стандартов на проведение НИР.

Допускается проведение исследований возможности создания нового образца СКЗИ в рамках составной части НИР. При этом функции заказчика возлагаются на головного исполнителя НИР, составной частью которой# являются проведение исследований возможности создания нового образца СКЗИ.

17. В ТТЗ или ТЗ на проведение НИР рекомендуется дополнительно включать сведения:

о заказчике СКЗИ (для юридического лица - наименование юридического лица с указанием номера лицензии на право осуществления отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами, при ее наличии, и срока ее действия, адрес юридического лица, телефон; для индивидуального предпринимателя - фамилия, имя, отчество, данные документа, удостоверяющего личность, номер лицензии на право осуществления отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами, при ее наличии, срок ее действия, адрес индивидуального предпринимателя и телефон);

о предполагаемой области применения планируемого к разработке нового образца СКЗИ (указывается система связи, в составе которой планируется использование создаваемого образца СКЗИ, ее основные технические характеристики, в том числе требования по безопасности информации, а также вид защищаемой информации (речевая, данные и т.д.);

о предполагаемом исполнителе НИР (приводятся данные о предполагаемом исполнителе (наименование юридического лица, его адрес, телефон) и соисполнителе (при его наличии) с указанием номеров лицензий на право осуществления отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами, и сроков их действия (при их наличии).

18. ТТЗ (ТЗ) на проведение НИР (составной части НИР) по исследованию возможности создания нового образца СКЗИ заказчик СКЗИ направляет на рассмотрение в ФСБ России, которая в течение двух месяцев с момента получения документов обязана согласовать ТТЗ (ТЗ) на проведение НИР (составной части НИР) или дать мотивированный отказ.

Письменное согласование с ФСБ России ТТЗ (ТЗ) на проведение НИР (составной части НИР) является основанием для проведения НИР (составной части НИР).

19. ТТЗ (ТЗ) на проведение НИР (составной части НИР), согласованное с ФСБ России, утверждается заказчиком СКЗИ. Экземпляр утвержденного ТТЗ (ТЗ) на проведение НИР (составной части НИР) направляется заказчиком СКЗИ в ФСБ России.

20. Результатом НИР (составной части НИР) являются проект ТТЗ (ТЗ) на проведение ОКР по созданию нового образца СКЗИ или модернизации действующего образца СКЗИ и технико-экономическое обоснование данной ОКР.

ТЗ разрабатывается на составную часть ОКР, в рамках которой создается новый образец СКЗИ или проводится модернизация действующего образца СКЗИ. При этом функции заказчика выполняет головной исполнитель ОКР, составной частью которой являются создание нового или модернизация действующего образца СКЗИ.

21. ОКР (составная часть ОКР) по созданию нового образца СКЗИ или модернизации

действующего образца СКЗИ проводится в соответствии с ТТЗ (ТЗ), разработанным на основе действующих стандартов на проведение ОКР (составной части ОКР).

22. Разработка ТТЗ (ТЗ) на проведение ОКР (составной части ОКР) может осуществляться без предварительного выполнения НИР.

23. В ТТЗ (ТЗ) на проведение ОКР (составной части ОКР) должны указываться следующие дополнительные сведения:

по криптографической защите информации - цель криптографической защиты информации с описанием предполагаемой модели нарушителя, определяющей возможные угрозы, которым должно противостоять разрабатываемое (модернизируемое) СКЗИ;

по условиям использования СКЗИ - требования, предъявляемые к условиям использования создаваемого нового образца СКЗИ или модернизируемого действующего образца СКЗИ в типовой схеме организации конфиденциальной связи, или исходные данные по сети (системе) конфиденциальной связи, в составе которой планируется использование создаваемого нового образца СКЗИ или модернизируемого действующего образца СКЗИ (типы каналов связи, скорость передачи информации, предполагаемое количество пользователей сети (системы) конфиденциальной связи, планируемая интенсивность информационного обмена, планирование размещения СКЗИ в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну, и т.д.);

по ключам СКЗИ - количество ключей, используемых в СКЗИ, предполагаемый срок их действия, организация их смены, тип ключевого носителя и т.д.;

по системе изготовления (распределения) ключей - вид системы изготовления ключей (встроенная в СКЗИ или внешняя), требования по безопасности информации, которые должны обеспечиваться применяемой системой изготовления (распределения) ключей и т.п.;

по предполагаемому ходу выполнения работ - сведения по планируемому порядку и срокам проведения работ, включая проведение экспертных криптографических, инженерно-криптографических, специальных исследований СКЗИ и работ по выявлению в технических средствах, входящих в состав СКЗИ электронных устройств, предназначенных для негласного получения информации, разработку тактико-технических требований на ключевые документы (если предполагается изготовление ключевых документов внешней по отношению к СКЗИ системой изготовления) с указанием этапов ОКР, на которых должны быть проведены планируемые работы.

Кроме того, в ТТЗ (ТЗ) на проведение ОКР (составной части ОКР) рекомендуется включать сведения:

о заказчике СКЗИ: для юридического лица - наименование юридического лица с указанием номера лицензии на право осуществления отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами (при ее наличии) и срока ее действия, адрес юридического лица и телефон; для индивидуального предпринимателя - фамилия, имя, отчество, данные документа, удостоверяющего личность, номер лицензии на право осуществления отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами (при ее наличии), и срок ее действия, адрес индивидуального предпринимателя и телефон;

о предполагаемой области применения создаваемого (модернизируемого) образца СКЗИ: указывается система связи, в составе которой планируется использование создаваемого (модернизируемого) образца СКЗИ, ее основные технические характеристики, а также вид защищаемой информации (речевая, данные и т.д.). При модернизации СКЗИ также приводится полное наименование и индекс серийно выпускаемого или разрабатываемого образца СКЗИ;

о предполагаемом разработчике и изготовителе создаваемых (модернизируемых) образцов СКЗИ: приводятся данные о предполагаемом разработчике (наименование юридического лица, его адрес, телефон) и соразработчике (при его наличии), а также изготовителе СКЗИ с указанием номеров лицензий на право осуществления отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами, и сроков их действия;

Приказ ФСБ РФ от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и...

о предполагаемом разработчике и изготовителе ключевых документов (в случае внешней системы изготовления): приводятся данные о предполагаемом разработчике (наименование юридического лица, его адрес, телефон) и соразработчике (при его наличии), а также изготовителе ключевых документов с указанием номеров лицензий на право осуществления отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами, и сроков их действия;

о планируемом объеме выпуска создаваемых (модернизируемых) образцов СКЗИ: указывается количество планируемых к выпуску создаваемых (модернизируемых) образцов СКЗИ;

о планируемом объеме выпуска ключевых документов: указывается планируемое среднегодовое количество изготавливаемых ключевых документов (в случае внешней системы изготовления) для создаваемых (модернизируемых) образцов СКЗИ;

о планируемой стоимости единичного создаваемого (модернизируемого) образца СКЗИ: приводятся данные о планируемой стоимости единичного образца СКЗИ при организации серийного выпуска;

о планируемой стоимости ключевых документов: приводятся данные о планируемой стоимости ключевых документов для создаваемого (модернизируемого) образца СКЗИ при организации их серийного выпуска;

о реализации создаваемых (модернизируемых) образцов СКЗИ: указывается перечень юридических лиц и индивидуальных предпринимателей, с помощью которых планируется осуществлять реализацию создаваемых (модернизируемых) образцов СКЗИ, с указанием номеров лицензий на право осуществления отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами, и сроков их действия;

о сервисном обслуживании СКЗИ: указывается перечень юридических лиц и индивидуальных предпринимателей, с помощью которых планируется осуществлять сервисное (техническое) обслуживание создаваемых (модернизируемых) образцов СКЗИ в процессе их использования, с указанием номеров лицензии на право осуществления отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами, и сроков их действия;

о предложениях по сопряжению с государственными сетями (системами) конфиденциальной связи: приводятся в случае необходимости организации обмена защищаемой информацией с государственными органами и (или) организациями, выполняющими государственные заказы.

24. Требования к СКЗИ (цель криптографической защиты информации с описанием предполагаемой модели нарушителя, определяющей возможные угрозы, которым должно противостоять разрабатываемое (модернизируемое) СКЗИ, требования к аппаратным, программно-аппаратным и программным средствам сети (системы) конфиденциальной связи, совместно с которыми предполагается использование создаваемого нового образца СКЗИ или модернизируемого действующего образца СКЗИ, требования к условиям размещения СКЗИ при их эксплуатации, требования к ключевой системе СКЗИ и т.д.) могут оформляться специальным техническим заданием (далее - СТЗ), которое является неотъемлемой частью общего ТТЗ (ТЗ) на проведение ОКР (составной части ОКР).

25. ТТЗ (ТЗ) на проведение ОКР (составной части ОКР) или СТЗ заказчик СКЗИ направляет на рассмотрение в ФСБ России, которая в течение двух месяцев с момента получения документов обязана согласовать ТТЗ (ТЗ) или дать мотивированный отказ с указанием конкретного образца СКЗИ, рекомендуемого заказчику СКЗИ к использованию или модернизации.

Письменное согласование с ФСБ России ТТЗ (ТЗ) на проведение ОКР (составной части ОКР) является основанием для проведения ОКР (составной части ОКР).

26. ТТЗ (ТЗ) на проведение ОКР (составной части ОКР) или СТЗ, согласованное с ФСБ России, утверждается заказчиком СКЗИ. Один экземпляр утвержденного ТТЗ (ТЗ) на проведение ОКР (составной части ОКР) или СТЗ представляется заказчиком СКЗИ в экспертную организацию.

27. При разработке СКЗИ рекомендуется использовать криптографические алгоритмы, утвержденные в качестве национальных стандартов или определенные перечнями, утверждаемыми в порядке, установленном постановлением Правительства Российской Федерации от 23 сентября 2002 г. N 691*(5).

28. Выбор носителя ключевой информации должен производиться с учетом возможности его приобретения изготовителем ключевых документов в течение всего предполагаемого срока эксплуатации СКЗИ. Оценка эксплуатационных характеристик применяемого носителя осуществляется разработчиком СКЗИ.

В случае использования внешней системы изготовления ключей разработанные тактико-технические требования на ключевые документы направляются в экспертную организацию для проведения экспертизы и утверждения.

На основе утвержденных тактико-технических требований выполняются работы, необходимые для организации серийного выпуска ключевых документов (включая разработку или приобретение аппаратно-программных средств, обеспечение требований по безопасности информации, подготовку технической, конструкторско-технологической и эксплуатационной документации и т.п.). В рамках этих работ создаются опытные образцы (макеты) ключевых документов, используемые при испытаниях штатного функционирования СКЗИ.

ФСБ России проводит экспертизу результатов разработки внешней системы изготовления ключей и подготавливает заключение о соответствии изготавливаемых с ее использованием ключевых документов требованиям по безопасности информации.

Разработка ключевых документов может осуществляться путем задания и проведения отдельной ОКР.

29. Правила пользования создаваемым новым образцом СКЗИ или модернизируемым действующим образцом СКЗИ составляются разработчиком СКЗИ и согласовываются с ФСБ России. О согласовании с ФСБ России на последней странице правил пользования СКЗИ разработчик СКЗИ делает соответствующую запись.

30. При разработке СКЗИ создается рабочая конструкторская документация (далее - РКД) на СКЗИ и опытный образец (опытные образцы) СКЗИ, разработанный (разработанные) в соответствии с РКД на него (них).

31. Составной частью разработки СКЗИ является проведение криптографических, инженерно-криптографических и специальных исследований СКЗИ (далее - тематические исследования СКЗИ), целью которых является оценка достаточности мер противодействия возможным угрозам безопасности информации, определенным моделью нарушителя, изложенной в СТЗ или ТТЗ (ТЗ) на проведение ОКР (составной части ОКР).

32. Тематические исследования СКЗИ выполняются в процессе всего цикла создания, производства и эксплуатации СКЗИ организациями, имеющими право на осуществление отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами (далее - специализированные организации).

33. Экспертиза результатов тематических исследований СКЗИ осуществляется ФСБ России, по результатам которой определяется возможность допуска СКЗИ к эксплуатации.

34. Тематические исследования СКЗИ и экспертиза их результатов являются отдельным этапом опытно-конструкторской работы, составляют ее неотъемлемую часть и не могут быть объединены с другими этапами выполнения ОКР.

35. Состав аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование создаваемого нового образца СКЗИ или модернизируемого действующего образца СКЗИ, влияющих на выполнение заданных требований к СКЗИ, определяется разработчиком СКЗИ и согласовывается с заказчиком СКЗИ, специализированной организацией и ФСБ России.

Оценка влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к ним требований осуществляется разработчиком СКЗИ совместно со специализированной организацией.

Приказ ФСБ РФ от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и...

36. Результаты тематических исследований и оценки влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к ним требований, а также опытные образцы СКЗИ и аппаратные, программно-аппаратные и программные средства, необходимые для штатного функционирования СКЗИ, передаются в ФСБ России для проведения экспертизы.

Аппаратные, программно-аппаратные и программные средства, необходимые для штатного функционирования СКЗИ, и опытные образцы СКЗИ для проведения тематических исследований и экспертизы передаются специализированной организации и ФСБ России на время выполнения указанных исследований.

Дальнейшее использование указанных опытных образцов СКЗИ и аппаратных, программно-аппаратных и программных средств определяется заказчиком СКЗИ.

37. РКД на СКЗИ передается в производство при наличии:

положительных результатов испытаний функционирования СКЗИ в штатных режимах;

положительных результатов экспертизы тематических исследований СКЗИ;

правил пользования СКЗИ, согласованных с ФСБ России.

III. Порядок производства СКЗИ

38. Принятие решения о производстве СКЗИ осуществляется после утверждения акта о завершении корректировки РКД на СКЗИ, доработки опытных образцов по результатам испытаний штатного функционирования СКЗИ и оценки их соответствия требованиям по безопасности информации.

39. Производство СКЗИ осуществляется в соответствии с техническими условиями, согласованными с ФСБ России и специализированной организацией, проводившей тематические исследования СКЗИ.

40. СКЗИ изготавливаются в полном соответствии с конструкцией и технологией изготовления опытных образцов СКЗИ, прошедших испытания на функционирование опытного образца СКЗИ в штатных режимах и имеющих положительное заключение экспертизы тематических исследований СКЗИ.

41. Все изменения в конструкции СКЗИ и технологии их изготовления изготовитель СКЗИ должен согласовывать со специализированной организацией и ФСБ России. Согласование внесения изменений в конструкцию СКЗИ и технологию их изготовления осуществляется путем представления изготовителем СКЗИ в специализированную организацию и ФСБ России обоснованного перечня предполагаемых изменений и получения от них соответствующих положительных заключений.

42. Производство ключевых документов с использованием внешней системы изготовления осуществляется с использованием программно-аппаратных средств, созданных разработчиком ключевых документов, в соответствии с технической, конструкторско-технологической и эксплуатационной документацией при наличии положительного заключения ФСБ России о соответствии изготавливаемых с использованием данной системы ключевых документов заданным требованиям по безопасности информации.

IV. Порядок реализации (распространения) СКЗИ

43. СКЗИ реализуются (распространяются) вместе с правилами пользования ими,

согласованными с ФСБ России.

44. Реализация (распространение) СКЗИ и (или) РКД на них осуществляется юридическим лицом или индивидуальным предпринимателем, имеющим право на осуществление данного вида деятельности, связанного с шифровальными (криптографическими) средствами.

45. Приобретение РКД на СКЗИ (включая тиражирование программных СКЗИ) осуществляют юридические лица, являющиеся разработчиками и (или) изготовителями СКЗИ.

V. Порядок эксплуатации СКЗИ

ГАРАНТ:

См. Инструкцию 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, утвержденную приказом ФАПСИ РФ от 13 июня 2001 г. N 152

46. СКЗИ эксплуатируются в соответствии с правилами пользования ими. Все изменения условий использования СКЗИ, указанных в правилах пользования ими, должны согласовываться с ФСБ России и специализированной организацией, проводившей тематические исследования СКЗИ.

В случае планирования размещения СКЗИ в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну, технические средства, входящие в состав СКЗИ, должны быть подвергнуты проверкам по выявлению устройств, предназначенных для негласного получения информации.

47. СКЗИ, находящиеся в эксплуатации, должны подвергаться контрольным тематическим исследованиям, конкретные сроки проведения которых определяются заказчиком СКЗИ по согласованию с разработчиком СКЗИ, специализированной организацией и ФСБ России.

48. СКЗИ и их опытные образцы подлежат поэкземплярному учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов (условных наименований) и регистрационных номеров поэкземплярного учета СКЗИ и их опытных образцов определяет ФСБ России.

Организация поэкземплярного учета опытных образцов СКЗИ возлагается на разработчика СКЗИ.

Организация поэкземплярного учета изготовленных СКЗИ возлагается на изготовителя СКЗИ.

Организация поэкземплярного учета используемых СКЗИ возлагается на заказчика СКЗИ.

49. Организация централизованного (количественного) поэкземплярного учета опытных образцов СКЗИ, а также изготовленных и используемых СКЗИ, осуществляется ФСБ России.

Информация об изменениях:

Приказом ФСБ России от 12 апреля 2010 г. N 173 в пункт 50 настоящего приложения внесены изменения

См. текст пункта в предыдущей редакции

50. Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, а также условий производства ключевых документов осуществляется в соответствии с требованиями Федерального закона от 26 декабря 2008 г. N 294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля"*(6).

51. Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, осуществляется:

обладателем, пользователем (потребителем) защищаемой информации, установившим режим защиты информации с применением СКЗИ;

собственником (владельцем) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ;

ФСБ России в рамках контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи.

Контроль за соблюдением условий производства ключевых документов, указанных в технической, конструкторско-технологической и эксплуатационной документации к внешней системе изготовления ключей, осуществляется изготовителем ключевых документов, а также ФСБ России в рамках контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи.

52. С целью оценки обоснованности и достаточности мер, принятых для защиты информации конфиденциального характера, обладатель, пользователь (потребитель) данной информации, установивший режим ее защиты с применением СКЗИ, а также собственник (владелец) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ, вправе обратиться в ФСБ России с просьбой о проведении контроля за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования СКЗИ.

---

*(1) Собрание законодательства Российской Федерации, 1995, N 15, ст. 1269; 2000, N 1, ст. 9; N 46, ст. 4537; 2002, N 19, ст. 1794; N 30, ст. 3033; 2003, N 2, ст. 156; Российская газета от 1 июля 2003 г. N 126 (3240).

*(2) Российская газета, 2003, N 161 (3275).

*(3) Постановление Правительства Российской Федерации от 23 сентября 2002 г. N 691 "Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами" (Собрание законодательства Российской Федерации, 2002 г., N 39, ст. 3792).

*(4) Собрание законодательства Российской Федерации, 2002, N 52 (часть I), ст. 5140.

*(5) Собрание законодательства Российской Федерации, 2002, N 39, ст. 3792.

Информация об изменениях:

Приказом ФСБ России от 12 апреля 2010 г. N 173 настоящая сноска изложена в новой редакции

См. текст сноски в предыдущей редакции

*(6) Собрание законодательства Российской Федерации, 2008, N 52 (ч. I), ст. 6249; 2009, N 18 (ч. I), ст. 2140; N 29, ст. 3601; N 48, ст. 5711; N 52 (ч. I), ст. 6441.

Приложение № 2
к приказу ГАОУ ПО ИРО
№ _____ от _____

Приказ ФАПСИ от 13 июня 2001 г. N 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"

В соответствии с Федеральным законом от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации"*, Законом Российской Федерации от 19 февраля 1993 г. N 4524-1 "О федеральных органах правительственной связи и информации"** и Положением о порядке разработки, производства, реализации и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (Положение ПКЗ-99), утвержденным приказом ФАПСИ от 23 сентября 1999 г. N 158, зарегистрированным Министерством юстиции Российской Федерации 28 декабря 1999 г., регистрационный N 2029***, с целью определения порядка организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну приказываю:

Утвердить Инструкцию 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 (прилагается).

Генеральный директор Агентства В.Матюхин

---

* Собрание законодательства Российской Федерации, 1995, N 8, ст.609.

** Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1993, N 12, ст.423.

*** "Российская газета", 2000, 26 января.

Зарегистрировано в Минюсте РФ 6 августа 2001 г.
Регистрационный N 2848

Приказ ФАПСИ от 13 июня 2001 г. N 152 "Об утверждении Инструкции об организации и обеспечении безопасности...

Приложение
к приказу ФАПСИ РФ
от 13 июня 2001 г. N 152

Инструкция
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

I. Общие положения

1. Настоящая Инструкция определяет единый на территории Российской Федерации порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных ФАПСИ средств криптографической защиты (шифровальных средств) подлежащей в соответствии с законодательством Российской Федерации обязательной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну*(1).

Данным порядком рекомендуется руководствоваться также при организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных ФАПСИ средств криптографической защиты*(2) не подлежащей обязательной защите конфиденциальной информации, доступ к которой ограничивается в соответствии с законодательством Российской Федерации или по решению обладателя конфиденциальной информации*(3) (за исключением информации, содержащей сведения, к которым в соответствии с законодательством Российской Федерации не может быть ограничен доступ).

2. Настоящая Инструкция не регламентирует порядка организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации в учреждениях Российской Федерации за границей.

II. Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации

3. Безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации в сетях конфиденциальной связи*(4) организуют и обеспечивают операторы конфиденциальной связи*(5).

Безопасность хранения и обработки с использованием СКЗИ конфиденциальной информации, передаваемой вне сетей конфиденциальной связи, организуют и обеспечивают лица, имеющие лицензию ФАПСИ*(6).

Лица, оказывающие возмездные услуги по организации и обеспечению безопасности хранения и обработки с использованием СКЗИ конфиденциальной информации, передаваемой вне сетей конфиденциальной связи, должны иметь лицензию ФАПСИ на деятельность по предоставлению услуг в области шифрования информации.

4. Безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, обладатели которой не имеют лицензий ФАПСИ, лицензиаты ФАПСИ организуют и обеспечивают либо по указанию вышестоящей организации, либо на основании договоров на оказание услуг по криптографической защите конфиденциальной информации.

5. Лицензиаты ФАПСИ несут ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности хранения, обработки и передачи по

каналам связи с использованием СКЗИ конфиденциальной информации лицензионным требованиям и условиям, эксплуатационной и технической документации к СКЗИ, а также положениям настоящей Инструкции.

При этом лицензиаты ФАПСИ должны обеспечивать комплексность защиты конфиденциальной информации, в том числе посредством применения некриптографических средств защиты.

6. Для разработки и осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ конфиденциальной информации лицензиат ФАПСИ создает один или несколько органов криптографической защиты*(7), о чем письменно уведомляет ФАПСИ.

Допускается возложение функций органа криптографической защиты на специальное структурное подразделение по защите государственной тайны, использующее для этого шифровальные средства.

Количество органов криптографической защиты и их численность устанавливает лицензиат ФАПСИ.

7. Орган криптографической защиты осуществляет:

проверку готовности обладателей конфиденциальной информации к самостоятельному использованию СКЗИ и составление заключений о возможности эксплуатации СКЗИ (с указанием типа и номеров используемых СКЗИ, номеров аппаратных, программных и аппаратно-программных средств, где установлены или к которым подключены СКЗИ, с указанием также номеров печатей (пломбиров), которыми опечатаны (опломбированы) технические средства, включая СКЗИ, и результатов проверки функционирования СКЗИ);

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;

обучение лиц, использующих СКЗИ, правилам работы с ними;

поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним;

учет обслуживаемых обладателей конфиденциальной информации, а также физических лиц, непосредственно допущенных к работе с СКЗИ*(8);

подачу заявок в ФАПСИ или лицензиату, имеющему лицензию ФАПСИ на деятельность по изготовлению ключевых документов*(9) для СКЗИ, на изготовление ключевых документов или исходной ключевой информации. Изготовление из исходной ключевой информации ключевых документов, их распределение, рассылку и учет;

контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатом ФАПСИ и настоящей Инструкцией;

расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты конфиденциальной информации; разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

разработку схемы организации криптографической защиты конфиденциальной информации (с указанием наименования и размещения нижестоящих органов криптографической защиты, если таковые имеются, обладателей конфиденциальной информации, реквизитов договоров на оказание услуг по криптографической защите конфиденциальной информации, а также с указанием типов применяемых СКЗИ и ключевых документов к ним, видов защищаемой информации, используемых совместно с СКЗИ технических средств связи, прикладного и общесистемного программного обеспечения и средств вычислительной техники). Указанную схему утверждает лицензиат ФАПСИ.

8. Обладатели конфиденциальной информации, если они приняли решение о необходимости криптографической защиты такой информации или если решение о необходимости ее

криптографической защиты в соответствии с Положением ПКЗ-99 принято государственными органами или государственными организациями, обязаны выполнять указания соответствующих органов криптографической защиты по всем вопросам организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

9. Для организации взаимодействия обладателей конфиденциальной информации, безопасность хранения, обработки и передачи по каналам связи которой с использованием СКЗИ организуют и обеспечивают различные лицензиаты ФАПСИ, из созданных этими лицензиатами ФАПСИ органов криптографической защиты выделяется координирующий орган криптографической защиты. Все органы криптографической защиты, образованные этими лицензиатами ФАПСИ, обязаны выполнять указания координирующего органа криптографической защиты по обеспечению такого взаимодействия.

10. Инструкции, регламентирующие процессы подготовки, ввода, обработки, хранения и передачи защищаемой с использованием СКЗИ конфиденциальной информации, должны согласовываться с лицензиатом ФАПСИ. Такие инструкции подготавливаются согласно эксплуатационной и технической документации на соответствующие сети связи, автоматизированные и информационные системы, в которых передается, обрабатывается или хранится конфиденциальная информация, с учетом используемых СКЗИ и положений настоящей Инструкции.

11. Лицензиаты ФАПСИ с учетом особенностей своей деятельности могут разрабатывать методические рекомендации по применению настоящей Инструкции, не противоречащие ее требованиям.

12. Ключевые документы для СКЗИ или исходная ключевая информация для выработки ключевых документов изготавливаются ФАПСИ на договорной основе или лицами, имеющими лицензию ФАПСИ на деятельность по изготовлению ключевых документов для СКЗИ.

Изготовлять ключевые документы из исходной ключевой информации могут координирующий орган криптографической защиты (при его наличии), органы криптографической защиты или непосредственно обладатели конфиденциальной информации, применяя штатные СКЗИ, если такая возможность предусмотрена эксплуатационной и технической документацией к СКЗИ.

13. К выполнению обязанностей сотрудников органов криптографической защиты лицензиатами ФАПСИ допускаются лица, имеющие необходимый уровень квалификации для обеспечения защиты конфиденциальной информации с использованием конкретного вида (типа) СКЗИ.

14. Лиц, оформляемых на работу в органы криптографической защиты, следует ознакомить с настоящей Инструкцией под расписку.

15. Обязанности, возлагаемые на сотрудников органа криптографической защиты, могут выполняться штатными сотрудниками или сотрудниками других структурных подразделений, привлекаемыми к такой работе по совместительству.

16. При определении обязанностей сотрудников органов криптографической защиты лицензиаты ФАПСИ должны учитывать, что безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации обеспечивается:

соблюдением сотрудниками органов криптографической защиты режима 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 сотрудниками органов криптографической защиты требований к обеспечению безопасности конфиденциальной информации;

надежным хранением сотрудниками органов криптографической защиты СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, носителей

конфиденциальной информации;

своевременным выявлением сотрудниками органов криптографической защиты попыток посторонних лиц получить сведения о защищаемой конфиденциальной информации, об используемых СКЗИ или ключевых документах к ним;

немедленным принятием сотрудниками органов криптографической защиты мер по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

17. Обучение и повышение квалификации сотрудников органов криптографической защиты осуществляют организации, имеющие лицензию на ведение образовательной деятельности по соответствующим программам.

18. Сотрудники органа криптографической защиты должны иметь разработанные в соответствии с настоящей Инструкцией и утвержденные лицензиатом ФАПСИ функциональные обязанности. Объем и порядок ознакомления сотрудников органов криптографической защиты с конфиденциальной информацией определяется обладателем конфиденциальной информации.

Обязанности между сотрудниками органа криптографической защиты должны быть распределены с учетом персональной ответственности за сохранность СКЗИ, ключевой документации и документов, а также за порученные участки работы.

19. Физические лица допускаются к работе с СКЗИ согласно перечню пользователей СКЗИ, утверждаемому соответствующим обладателем конфиденциальной информации. До такого утверждения техническая возможность использования СКЗИ лицами, включенными в данный перечень, должна быть согласована с лицензиатом ФАПСИ.

Лицензиаты ФАПСИ в рамках согласованных с обладателями конфиденциальной информации полномочий по доступу к конфиденциальной информации имеют право утверждать такой перечень в отношении подчиненных им должностных лиц.

20. Пользователи СКЗИ обязаны:

не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения о криптоключах;

соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;

сообщать в орган криптографической защиты о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

21. Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения.

Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники соответствующего органа криптографической защиты. Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение, составленное комиссией соответствующего органа криптографической защиты на основании принятых от этих лиц зачетов по программе обучения.

III. Порядок обращения с СКЗИ и криптоключами к ним. Мероприятия при компрометации криптоключей*(10)

Приказ ФАПСИ от 13 июня 2001 г. N 152 "Об утверждении Инструкции об организации и обеспечении безопасности...

22. Предназначенные для обеспечения безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации СКЗИ, а также ключевые документы к ним не должны содержать сведений, составляющих государственную тайну.

23. В федеральных органах исполнительной власти ключевые документы, СКЗИ с введенными криптоключами относятся к материальным носителям, содержащим служебную информацию ограниченного распространения. При этом должны выполняться требования настоящей Инструкции и иных документов, регламентирующих порядок обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти.

Иным обладателям конфиденциальной информации при обращении с ключевыми документами, СКЗИ с введенными криптоключами необходимо руководствоваться настоящей Инструкцией.

24. Для организации и обеспечения безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации следует использовать СКЗИ, позволяющие реализовать принцип абонентского шифрования и предусматривающие запись криптоключей на электронные ключевые носители многократного (долговременного) использования (дискеты, компакт-диски (CD-ROM), Data Key, Smart Card, Touch Memory и т.п.).

25. При необходимости передачи по техническим средствам связи служебных сообщений, касающихся организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, соответствующие указания необходимо передавать, только применяя СКЗИ. Передача по техническим средствам связи криптоключей не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

26. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету по установленным формам в соответствии с требованиями Положения ПКЗ-99. При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами.

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

Журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (приложения 1, 2 к Инструкции) ведут органы криптографической защиты и обладатели конфиденциальной информации.

27. Все полученные обладателем конфиденциальной информации экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.

Органы криптографической защиты заводят и ведут на каждого пользователя СКЗИ лицевой счет, в котором регистрируют числящиеся за ним СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы.

28. 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 (приложение 3 к Инструкции), ведущемся непосредственно пользователем СКЗИ. В техническом (аппаратном) журнале отражают также данные об эксплуатации СКЗИ и другие сведения,

предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на СКЗИ не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к СКЗИ).

29. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ и (или) сотрудниками органа криптографической защиты под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями СКЗИ должна быть санкционирована соответствующим органом криптографической защиты.

Обладатель конфиденциальной информации с согласия органа криптографической защиты может разрешить передачу СКЗИ, документации к ним, ключевых документов между допущенными к СКЗИ лицами по актам без обязательной отметки в журнале поэкземплярного учета.

30. Пользователи СКЗИ хранят 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.

Пользователи СКЗИ предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей.

31. 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 указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

32. СКЗИ и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными нарочными из числа сотрудников органа криптографической защиты или пользователей СКЗИ, для которых они предназначены, при соблюдении мер, исключающих бесконтрольный доступ к ним во время доставки.

Эксплуатационную и техническую документацию к СКЗИ можно пересылать заказными или ценными почтовыми отправлениями.

33. Для пересылки СКЗИ ключевые документы должны быть помещены в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. СКЗИ пересылают отдельно от ключевых документов к ним. На упаковках указывают орган криптографической защиты или пользователя СКЗИ, для которых эти упаковки предназначены. На упаковках для пользователя СКЗИ делают пометку "Лично". Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.

Оформленную таким образом упаковку, при предъявлении фельдсвязью дополнительных требований, помещают во внешнюю упаковку, оформленную согласно предъявляемым требованиям. До первоначальной высылки (или возвращения) адресату сообщают отдельным письмом описание высылаемых ему упаковок и печатей, которыми они могут быть опечатаны.

34. Для пересылки СКЗИ, эксплуатационной и технической документации к ним, ключевых документов следует подготовить сопроводительное письмо, в котором необходимо указать, что посылается и в каком количестве, учетные номера изделий или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывают в одну из упаковок.

35. Полученные упаковки вскрывают только в органе криптографической защиты или лично пользователи СКЗИ, для которых они предназначены. Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получатель составляет акт, который высылает отправителю, а при необходимости информирует об этом соответствующий орган криптографической защиты. Полученные с такими отправлениями СКЗИ и ключевые документы до получения указаний от отправителя и органа криптографической защиты применять не разрешается.

Приказ ФАПСИ от 13 июня 2001 г. N 152 "Об утверждении Инструкции об организации и обеспечении безопасности...

36. При обнаружении бракованных ключевых документов или криптоключей один экземпляр бракованного изделия следует возвратить изготовителю через соответствующий орган криптографической защиты для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний от органа криптографической защиты или изготовителя.

37. Лицензиат ФАПСИ, допустивший брак при изготовлении ключевых документов, с целью выявления причин случившегося может обратиться в ФАПСИ для проведения на договорной основе экспертизы бракованных ключевых документов.

38. Получение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должно быть подтверждено отправителю в соответствии с порядком, указанным в сопроводительном письме. Отправитель обязан контролировать доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель должен направить ему запрос и принять меры к уточнению местонахождения отправлений.

39. Заказ на изготовление очередных ключевых документов, их изготовление и рассылку на места использования для своевременной замены действующих ключевых документов следует производить заблаговременно. Указание о вводе в действие очередных ключевых документов может быть дано только после поступления в орган криптографической защиты подтверждений от всех заинтересованных пользователей СКЗИ о получении ими очередных ключевых документов.

40. Рассылка изготавливаемых ФАПСИ ключевых документов или исходной ключевой информации на места использования может производиться федеральными органами правительственной связи и информации. Такая рассылка осуществляется по заявкам органа криптографической защиты или заявкам координирующего органа криптографической защиты (при его наличии) на договорной основе.

41. Неиспользованные или выведенные из действия ключевые документы подлежат возвращению в орган криптографической защиты или по его указанию должны быть уничтожены на месте.

42. 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).

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 СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

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 уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

43. СКЗИ уничтожают (утилизируют) в соответствии с требованиями Положения ПКЗ-99 по решению обладателя конфиденциальной информации, владеющего СКЗИ, и по согласованию с лицензиатом ФАПСИ.

Намеченные к уничтожению (утилизации) 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 СКЗИ процедура удаления программного обеспечения СКЗИ и они полностью отсоединены от аппаратных средств.

44. 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 (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

45. Ключевые документы должны быть уничтожены 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 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета. В эти же сроки с отметкой в техническом (аппаратном) 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.

46. 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 расписку в техническом (аппаратном) журнале.

Ключевые документы уничтожаются либо пользователями СКЗИ, либо сотрудниками органа криптографической защиты под расписку в соответствующих журналах 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 (телефонограммой, устным сообщением по телефону и т.п.) соответствующий орган криптографической защиты для списания уничтоженных документов с их лицевых счетов. Не реже одного раза в год пользователи СКЗИ должны направлять в орган криптографической защиты письменные отчеты об уничтоженных ключевых документах. Орган криптографической защиты вправе устанавливать периодичность представления указанных отчетов чаще одного раза в год.

Уничтожение по акту производит комиссия в составе не менее двух человек из числа сотрудников органа криптографической защиты. 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 СКЗИ 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 в соответствующих журналах поэкземплярного учета.

47. Криптоключи, в отношении которых возникло подозрение в компрометации, а также

Приказ ФАПСИ от 13 июня 2001 г. N 152 "Об утверждении Инструкции об организации и обеспечении безопасности...

действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ. О выводе криптоключей из действия сообщают в соответствующий орган криптографической защиты. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению лицензиата ФАПСИ, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а передаваемая информация как можно менее ценной.

48. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать в соответствующий орган криптографической защиты. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

49. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет обладатель скомпрометированной конфиденциальной информации.

50. Порядок оповещения пользователей СКЗИ о предполагаемой компрометации криптоключей и их замене устанавливается соответствующим органом криптографической защиты или ФАПСИ.

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

51. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним*(11), должны обеспечивать сохранность конфиденциальной информации*(12), СКЗИ, ключевых документов.

При оборудовании спецпомещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

Перечисленные в настоящей Инструкции требования к спецпомещениям могут не предъявляться, если это предусмотрено правилами пользования СКЗИ, согласованными с ФАПСИ.

52. Спецпомещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Окна спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

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

54. Режим охраны спецпомещений органов криптографической защиты, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает лицензиат ФАПСИ по согласованию, при необходимости, с обладателем конфиденциальной информации, в помещениях которого располагается соответствующий орган криптографической защиты.

Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящей Инструкции.

55. Двери спецпомещений органов криптографической защиты должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам органов криптографической защиты под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких спецпомещений следует хранить в сейфе руководителя органа криптографической защиты. Хранение дубликатов ключей вне помещений органа криптографической защиты не допускается.

56. Для предотвращения просмотра извне спецпомещений органов криптографической защиты их окна должны быть защищены.

57. Спецпомещения органов криптографической защиты, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически необходимо проверять руководителю органа криптографической защиты или по его поручению другому сотруднику этого органа совместно с представителем службы охраны или дежурным по организации с отметкой в соответствующих журналах.

58. Каждый орган криптографической защиты для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей должен иметь необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у сотрудника, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в сейфе руководителя органа криптографической защиты.

Дубликат ключа от хранилища руководителя органа криптографической защиты в опечатанной упаковке должен быть передан на хранение должностному лицу, назначаемому лицензиатом ФАПСИ, под расписку в соответствующем журнале.

59. По окончании рабочего дня спецпомещения органа криптографической защиты и установленные в них хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале руководителю органа криптографической защиты или лицу, им уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище.

Ключи от спецпомещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ органа криптографической защиты, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службе охраны или дежурному по организации одновременно с передачей под охрану самих спецпомещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у сотрудников органа криптографической защиты, ответственных за эти хранилища.

60. При утрате ключа от хранилища или от входной двери в спецпомещение органа криптографической защиты 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 руководитель органа криптографической защиты.

61. В обычных условиях спецпомещения органа криптографической защиты, находящиеся в них опечатанные хранилища могут быть вскрыты только сотрудниками органа криптографической защиты.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти спецпомещения или хранилища посторонних лиц, о случившемся должно

быть немедленно сообщено руководителю органа криптографической защиты. Прибывшие сотрудники органа криптографической защиты должны оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации конфиденциальной информации и к замене скомпрометированных криптоключей.

62. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в спецпомещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае пользователи СКЗИ по согласованию с органом криптографической защиты обязаны предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами в их отсутствие.

63. Режим охраны спецпомещений пользователей СКЗИ, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает обладатель конфиденциальной информации по согласованию с соответствующим органом криптографической защиты. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящей Инструкции, специфику и условия работы конкретных пользователей СКЗИ.

64. В спецпомещениях пользователей СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ.

65. При утрате ключа от хранилища или от входной двери в спецпомещение пользователя СКЗИ 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 орган криптографической защиты.

66. В обычных условиях опечатанные хранилища пользователей СКЗИ могут быть вскрыты только самими пользователями.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти спецпомещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено руководству обладателя конфиденциальной информации и руководителю органа криптографической защиты. Прибывшие сотрудники органа криптографической защиты должны оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации конфиденциальной информации и к замене скомпрометированных криптоключей.

V. Контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации

67. Контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации - государственный контроль осуществляют федеральные органы правительственной связи и информации*(13). 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.

68. При организации безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ подлежащей в соответствии с законодательством Российской Федерации обязательной защите конфиденциальной информации государственному контролю подлежит деятельность лицензиатов ФАПСИ, а также обладателей конфиденциальной информации, если необходимость криптографической защиты такой информации в соответствии с Положением ПКЗ-99 определяется государственными органами или государственными организациями.

При организации безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ не подлежащей обязательной защите конфиденциальной информации государственному контролю подлежит деятельность лицензиатов ФАПСИ. Обладатели конфиденциальной информации в этом случае могут быть проверены федеральными органами правительственной связи и информации лишь по их просьбе или с их согласия.

Возможность и форму доступа государственных контрольных органов к содержанию конфиденциальной информации определяет руководитель проверяемой организации.

Сроки и периодичность государственного контроля определяет ФАПСИ.

69. Лицензиаты ФАПСИ обязаны контролировать выполнение обладателями конфиденциальной информации данных им указаний по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, а также соблюдение такими обладателями условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатом ФАПСИ и настоящей Инструкцией.

70. В целях координации государственного контроля и контроля, проводимого лицензиатами ФАПСИ, федеральные органы правительственной связи и информации могут планировать и проводить проверки совместно с заинтересованными органами криптографической защиты, рекомендовать лицензиатам ФАПСИ объекты проверок.

71. Непосредственный допуск к проверке комиссии или уполномоченного федеральных органов правительственной связи и информации осуществляет руководство проверяемых лиц при предъявлении проверяющими удостоверения (предписания) на право проверки, заверенного печатью, и документов, удостоверяющих личность.

Удостоверения (предписания) на право проверки подписывают генеральный директор ФАПСИ, его заместители, а также по их указанию - руководители федеральных органов правительственной связи и информации. Допуск к проверке возможен на основании указаний этих лиц, переданных по техническим каналам связи.

72. По результатам государственного контроля составляется подробный или краткий акт, справка. С актом проверки (справкой) под расписку должно быть ознакомлено руководство проверяемых лиц. Акт (справку) высылают в соответствующий орган криптографической защиты, координирующий орган криптографической защиты (при его наличии) и федеральный орган правительственной связи и информации. Если в ходе проверки выявлены нарушения требований и условий лицензий и сертификатов ФАПСИ, то федеральные органы правительственной связи и информации сообщают в Лицензионный и сертификационный центр ФАПСИ об этих нарушениях и принятых мерах.

Если в использовании СКЗИ обнаружены недостатки, то лицензиаты ФАПСИ, обладатели конфиденциальной информации обязаны принять безотлагательные меры к устранению вскрытых проверкой недостатков и выполнению рекомендаций, изложенных в акте проверки. Сообщения о принятых мерах должны быть представлены в установленные проверяющими сроки. При необходимости может быть составлен план мероприятий, где предусматривается решение соответствующих вопросов.

Приказ ФАПСИ от 13 июня 2001 г. N 152 "Об утверждении Инструкции об организации и обеспечении безопасности...

73. Органы криптографической защиты (координирующие органы криптографической защиты) должны обобщать результаты всех видов контроля, анализировать причины выявленных недостатков, разрабатывать меры по их профилактике, контролировать выполнение рекомендаций, содержащихся в актах проверок.

74. Если в использовании СКЗИ выявлены серьезные нарушения, из-за чего становится реальной утечка конфиденциальной информации, безопасность которой обеспечивается с использованием СКЗИ, то федеральные органы правительственной связи и информации, лицензиаты ФАПСИ вправе дать указание о немедленном прекращении использования СКЗИ до устранения причин выявленных нарушений. В этом случае федеральные органы правительственной связи и информации могут направить в Лицензионный и сертификационный центр ФАПСИ представление об отзыве (приостановлении действия) лицензий ФАПСИ.

75. Обладатель конфиденциальной информации вправе обратиться в федеральные органы правительственной связи и информации с просьбой о проведении на договорной основе государственного контроля с целью оценки достаточности и обоснованности принимаемых лицензиатом ФАПСИ мер защиты его конфиденциальной информации.

---

*(1) Информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, в настоящей Инструкции именуется - конфиденциальная информация.

*(2) Сертифицированные ФАПСИ средства криптографической защиты конфиденциальной информации в настоящей Инструкции именуются - СКЗИ. К СКЗИ относятся:

- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи, включая СКЗИ;

- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении;

- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и "электронной подписи";

- аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации.

*(3) Обладателями конфиденциальной информации могут быть государственные органы, государственные организации и другие организации независимо от их организационно-правовой формы и формы собственности, индивидуальные предприниматели и физические лица.

*(4) Сети конфиденциальной связи - сети связи, предназначенные для передачи конфиденциальной информации.

*(5) Операторы конфиденциальной связи - операторы связи, предоставляющие на основании лицензии ФАПСИ услуги конфиденциальной связи с использованием СКЗИ.

*(6) Операторы конфиденциальной связи и лица, имеющие лицензию ФАПСИ и не являющиеся операторами конфиденциальной связи, в настоящей Инструкции именуются лицензиаты ФАПСИ.

*(7) Органом криптографической защиты может быть организация, структурное подразделение организации - лицензиата ФАПСИ, обладателя конфиденциальной информации. Функции органа криптографической защиты могут быть возложены на физическое лицо.

*(8) Физические лица, непосредственно допущенные к работе с СКЗИ, в настоящей Инструкции именуются - пользователи СКЗИ.

*(9) В настоящей Инструкции используются следующие понятия и определения:

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

- **ключевая информация** - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

- **исходная ключевая информация** - совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

- **ключевой документ** - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию;

- **ключевой носитель** - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации). Различают разовый ключевой носитель (таблица, перфолента, перфокарта и т.п.) и ключевой носитель многократного использования (магнитная лента, дискета, компакт-диск, Data Key, Smart Card, Touch Memory и т.п.);

- **ключевой блокнот** - набор бумажных ключевых документов одного вида (таблиц, перфолент, перфокарт и т.п.), сброшюрованных и упакованных по установленным правилам.

*(10) Под компрометацией криптоключей в настоящей Инструкции понимается хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

*(11) Помещения, где установлены СКЗИ или хранятся ключевые документы к ним, в настоящей Инструкции именуются - спецпомещения.

*(12) Требования к обеспечению сохранности конфиденциальной информации в спецпомещениях аналогичны требованиям к помещениям, где выполняются работы, связанные с хранением (обработкой) такой информации, и устанавливаются обладателем конфиденциальной информации;

*(13) Под федеральными органами правительственной связи и информации в настоящей Инструкции понимаются главные управления ФАПСИ, управления ФАПСИ в федеральных округах, региональные управления правительственной связи и информации, центры правительственной связи.

Приложение 1
к Инструкции (пункт 26),
утвержденной приказом **ФАПСИ**
от 13 июня 2001 г. N 152

Типовая форма
журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для органа криптографической защиты)

N п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о рассылке (передаче)		
				От кого получены или Ф.И.О. сотрудника органа криптографической защиты, изготовившего ключевые документы	Дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении	Кому разосланы (переданы)	Дата и номер сопроводительного письма	Дата и номер подтверждения или расписка в получении
1	2	3	4	5	6	7	8	9

Отметка о возврате		Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении СКЗИ, ключевых документов		Примечание
Дата и номер сопроводительного письма	Дата и номер подтверждения			Дата уничтожения	Номер акта или расписка об уничтожении	
10	11	12	13	14	15	16

Приложение 2
к Инструкции (пункт 26),
утвержденной приказом **ФАПСИ РФ**
от 13 июня 2001 г. N 152

Типовая форма
журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)

N п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные 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 СКЗИ	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. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение 3
к Инструкции (пункт 28),
утвержденной приказом **ФАПСИ**
от 13 июня 2001 г. N 152

Типовая форма технического (аппаратного) журнала

N 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 № 3
к приказу ГАОУ ПО ИРО
№ 516 от 22.07.24

АКТ
проверки соблюдения правил эксплуатации и хранения СКЗИ, ключевых документов, аппаратных средств, с которыми осуществляется штатное функционирование СКЗИ

г. Севастополь **«__» _____ 202__ г.**

_____
(должность, фамилия, имя, отчество)

в соответствии с приказом ГАОУ ПО «Институт развития образования» № _____ от _____ в период времени с ____по _____ провел контрольное мероприятие по проверке соблюдения правил эксплуатации и хранения СКЗИ, ключевых документов, аппаратных средств, с которыми осуществляется штатное функционирование СКЗИ в помещении административного здания/учебного корпуса, по адресу: г. Севастополь, ул. _____ дом _____.

В случае выявления нарушений

В процессе проведения мероприятия выявлены следующие нарушения, в кабинете № _____ не опечатано, не имеет средств контроля за вскрытием СКЗИ, металлический шкаф, место хранения *(указать нарушение)* Рабочее место (кабинет) закреплены за *указать должность фамилию, имя, отчество работника,* что является нарушением *указать нормативно-правовой акт (статья, пункт, часть).*

В случае отсутствия нарушений

В процессе проведения мероприятия нарушения не выявлены.

Должность *Подпись* *И.О. Фамилия*

Дата

Приложение № 4
к приказу ГАОУ ПО ИРО
№ 516 от 22.07.24

ЖУРНАЛ

учета средств контроля за вскрытием аппаратных средств, с которыми осуществляется штатное функционирование СКЗИ, и их хранилищ, мест хранения и обработки персональных данных, конфиденциальной информации, информации с ограниченным доступом

Начат _____
Окончен _____

г. Севастополь

№ п/п	Учетный № склейки	Учетный № печати	СКЗИ, хранилище, кабинет	Адрес	№ каб.	Ответственное лицо	Подпись ответственного лица	Примечание