Приказ ФСБ России от 09.02.2005 № 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)"

(в ред. Приказа ФСБ России от 12.04.2010 № 173)

Зарегистрировано в Минюсте России 03.03.2005 № 6382

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 № 158 (зарегистрирован Минюстом России 28 декабря 1999 года, регистрационный № 2029) не применять с даты вступления в силу настоящего Приказа.

Директор
Н.Патрушев

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

Приложение
к Приказу ФСБ России
от 9 февраля 2005 г. № 66

Настоящее Положение разработано во исполнение Федерального закона от 3 апреля 1995 года № 40-ФЗ "О федеральной службе безопасности" и Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 года № 960.

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).

2. Шифровальные (криптографические) средства защиты информации конфиденциального характера в настоящем Положении именуются средствами криптографической защиты информации (далее - СКЗИ). К СКЗИ относятся:
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 лиц, 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 № 184-ФЗ "О техническом регулировании".

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

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;
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 года № 691.

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.

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

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.

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. № 294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля".

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.

персональные данные, техническая защита информации

From:
http://www.sps-ib.ru/ - **Справочно-правовая система по информационной безопасности**

Permanent link:
http://www.sps-ib.ru/npa:fsb66_09.02.2005

Last update: **2016/09/09 09:16**