A.V. Epishkina

The Course «Legal Regulation of Cryptographic Techniques Development and Implementation» for Masters

Key words: information security, cryptographic technique, lawregulation, masters' program, curriculum.

The purpose of the article was to investigate the curriculum of the course concerned with law regulation of design and application of cryptographic techniques. The main topics of the discipline is given. They are as follows: the order of design, production, realization and application of cryptographicmeans.

А.В. Епишкина

О СОЗДАНИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ «НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ РАЗРАБОТКИ И ИСПОЛЬЗОВАНИЯ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»

Введение

При обучении магистров по направлению подготовки 10.04.01 «Информационная безопасность» (профиль «Применение методов криптологии в системах обеспечения информационной безопасности») на кафедре «Криптология и дискретная математика» НИЯУ МИФИ особое внимание уделяется правильному формированию знаний о правовом поле, в котором предстоит работать выпускникам, в первую очередь, связанного с использованием средств криптографической защиты информации (СКЗИ). Автором разработан курс лекций «Нормативное регулирование разработки и использования средств криптографической защиты информации», читаемый для магистров 2-го года обучения. Данная дисциплина посвящена нормативно-правовым основам разработки и применения средства криптографической защиты информации, обеспечивает приобретение знаний и умений в соответствии с собственным образовательным стандартом НИЯУ МИФИ, содействует формированию научного мировоззрения и системного мышления. Наиболее важными темами, освещаемыми в указанном курсе, являются российские стандарты на алгоритм шифрования, электронной подписи и функцию хэширования, регулирование разработки и применения средств криптографической защиты информации в России. Знания, умения и навыки, полученные при изучении учебной дисциплины «Нормативное регулирование разработки и использования средств криптографической защиты информации», необходимы для выполнения научно-исследовательских и выпускных квалификационных работ магистров.

Календарный план дисциплины

Дисциплина «Нормативное регулирование разработки и использования средств криптографической защиты информации» читается в осеннем семестре на протяжении 16 учебных недель по два лекционных часа в неделю. Календарный план дисциплины приведен в табл. 1.

Таблица 1. Календарный план курса «Нормативное регулирование разработки и использования средств криптографической защиты информации»

Учебные недели	Содержание занятий
1-я	Основные российские стандарты, регламентирующие вопросы информационной безопасности. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
2-я	ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующиена информацию. Общие положения. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступак информации. Общие технические требования
3–4-я	ГОСТ Р ИСО 7498-2–99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации
5–6-я	Основные документы, регламентирующие разработку и применение средств криптографической защиты информации, их краткая характеристика
7–8-я	Порядок разработки СКЗИ
9–10-я	Порядок производства СКЗИ. Порядок реализации (распространения) СКЗИ. Порядок эксплуатации СКЗИ
11-я	Орган криптографической защиты и его функции. Обязанности пользователей СКЗИ
12–13-я	Особенности применения криптографических средств для защиты персональных данных
14-я	Использование электронной подписи. Основные нормативные документы
15–16я-	Виды электронной подписи. Придание юридической значимости электронному документу

Начинать знакомство с вопросами регулирования разработки и применения СКЗИ необходимо с краткой характеристики стандартов в области защиты информации, особо отметив, каково место среди них нормативных документов, посвященных непосредственно криптографическим методам. В стандартах, относящихся к области защиты информации, как правило, рассматриваются как концептуальные основы обеспечения информационной безопасности, так и некоторые технические аспекты. Одной из особенностей российской нормативной базы является то, что из-за остро стоящей проблемы обеспечения совместимости программно-аппаратных средств, основой многих российских стандартов являются их зарубежные прототипы.

Далее описываются основные нормативные документы, которыми следует руководствоваться при разработке, производстве и применении СКЗИ.

1. Положение о лицензировании разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем[1].

2. Положениео разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации [2].

3. 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 [3].

4. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных [4].

5. Методические рекомендации ФСБ России «По обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» [5].

6. Требования к средствам электронной подписи и Требования к средствам удостоверяющего центра [6].

В последующих разделах статьи кратко охарактеризуем наиболее значимые темы рассматриваемой учебной дисциплины. Основное внимание при чтении лекций по курсу «Нормативное регулирование разработки и использования средств криптографической защиты информации» уделяется порядку разработки, производства, реализации и эксплуатации СКЗИ, поскольку данными видами деятельности зачастую могут заниматься выпускаемые кафедрой магистры.

Порядок разработки СКЗИ

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

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

Схематично порядок разработки СКЗИ изображен на рис. 1.

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.

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.

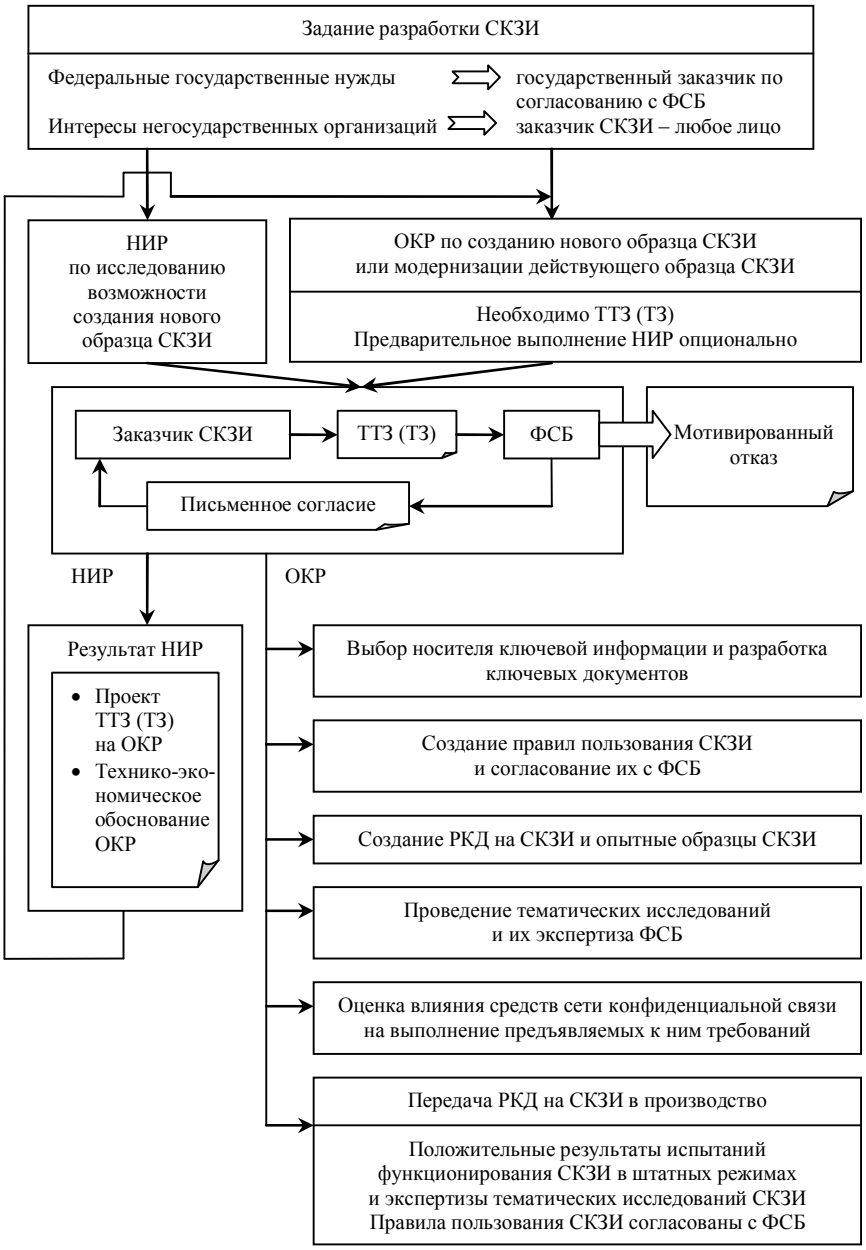

Рис. 1. Порядок разработки СКЗИ

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.

Правила пользования создаваемым новым образцом СКЗИ или модернизируемым действующим образцом СКЗИ составляются разработчиком СКЗИ и согласовываются с ФСБ России.

Составная часть разработки СКЗИ – 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).

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).

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

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.

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.

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.

Порядок производства СКЗИ

Производство СКЗИ осуществляется в соответствии с техническими условиями, согласованными с ФСБ России и специализированной организацией, проводившей тематические исследования СКЗИ. Схематично порядок производства СКЗИ изображен на рис. 2.

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.

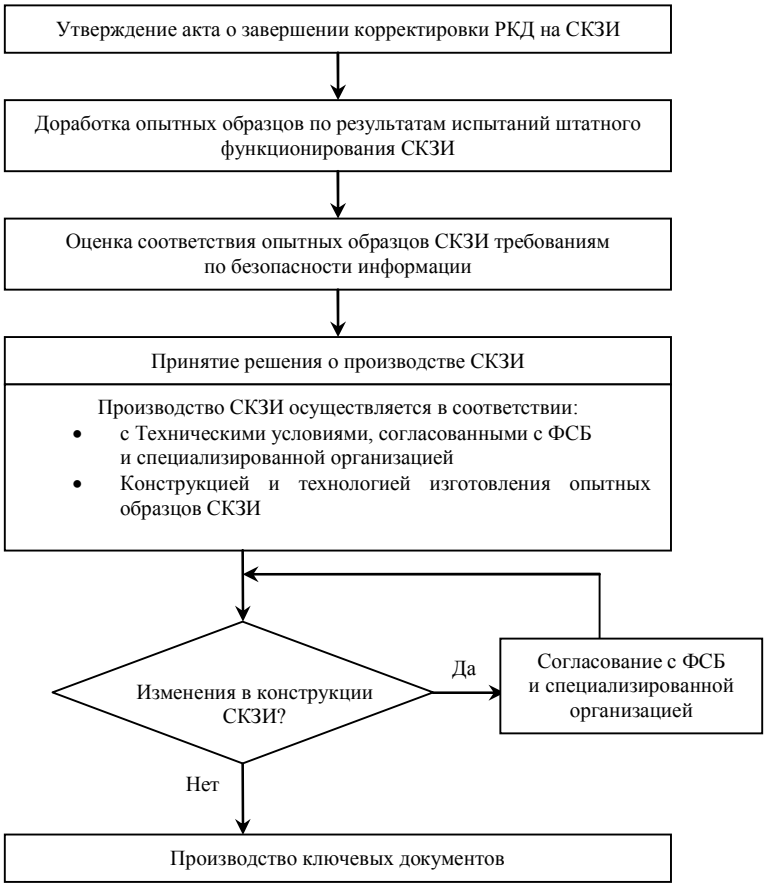

Рис. 2. Порядок производства СКЗИ

Производство ключевых документов с использованием внешней системы изготовления осуществляется с применением 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.

Порядок реализации (распространения) СКЗИ

Реализация (распространение) СКЗИ и (или) рабочей конструкторской документации (РКД) на них осуществляется юридическим лицом или индивидуальным предпринимателем, имеющим право на осуществление данного вида деятельности, связанного с шифровальными (криптографическими) средствами. Схематично порядок производства СКЗИ изображен на рис. 3.

Порядок эксплуатации СКЗИ

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. Схематично порядок эксплуатации СКЗИ изображен на рис. 4.

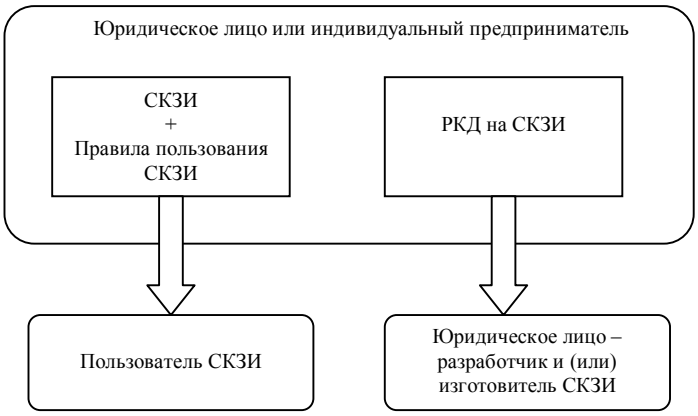

Рис. 3. Порядок реализации (распространения) СКЗИ

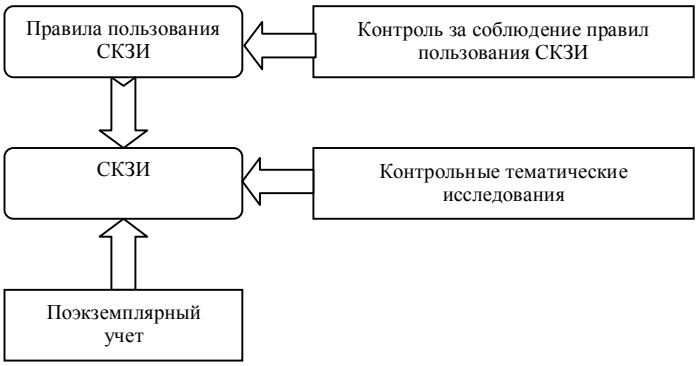

Рис. 4. Порядок эксплуатации СКЗИ

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.

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

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 8 августа 2001 года № 134-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при проведении государственного контроля (надзора)».

Заключение

В статье кратко охарактеризована учебная дисциплина «Нормативное регулирование разработки и использования средств криптографической защиты информации», читаемая магистрам, обучающимся по направлению подготовки 10.04.01 «Информационная безопасность» (профиль «Применение методов криптологии в системах обеспе-

чения информационной безопасности») на кафедре «Криптология и дискретная математика» НИЯУ МИФИ. Приведен календарный план указанного курса с привязкой преподаваемого материала к учебным неделям.

Особое внимание при чтении лекций по рассматриваемой дисциплине уделяется вопросам разработки, производства, распространения и эксплуатации СКЗИ, которые освещены в статье подробнее.

СПИСОК ЛИТЕРАТУРЫ:

1. Постановление Правительства РФ «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» от 16.04.2012 г. № 313.
2. Приказ ФСБ РФ «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» от 09.02.2005 г. № 66 (ред. от 12.04.2010 г.).
3. Приказ ФАПСИ «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» от 13.06.2001 г. № 152.
4. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных: утв. руководством 8 Центра ФСБ России 21.02.2008 г.
5. Методические рекомендации ФСБ РФ «По обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» от 21.02.2008 г. № 149/54-144.
6. Приказ ФСБ РФ «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра» от 27.12.2011 г. № 796.

REFERENCES:

1. Postanovlenie Pravitel’stva RF «Ob utverjdenii Polojenia o licenzirovanii dejatel’nosti po razrabotke, proizvodstvu, rasprostraneniu shifroval’nih (kriptograficheskih) sredstv, informacionnih system i telecommunikacionnih system, zazhizhennih s ispol’zovaniem shifroval’nih (kriptograficheskih) sredstv, vipolneniu rabot, okazaniu uslug v oblasti shifrovanija informacii, tehnicheskomu obslujivaniu shifroval’nih (kriptograficheskih) sredstv, informacionnih system i telecommunikacionnih system, zazhizhennih s ispol’zovaniem shifroval’nih (kriptograficheskih) sredstv (za iskljucheniem sluchaja, esli tehnicheskoe obslujivanie shifroval’nih (kriptograficheskih) sredstv, informacionnih system i telecommunikacionnih system, zazhizhennih s ispol’zovaniem shifroval’nih (kriptograficheskih) sredstv, osuzhestvliaetcia dlia obespechenija sobstvennih nuzhd uridicheskogo lica ili individual’nogo predprinimatelia)”ot 16.04.2012g. № 313.
2. Prikaz FSB RF «Ob utvezjdenii Polojenia o razrabotke, proizvodstve, realizacii i ekspluatacii shifroval’nih (kriptograficheskih) sredstv zazhiti informacii (PolojeniePKZ-2005)» ot 09.02.2005g. № 66 (red. ot 12.04.2010g.).
3. Prikaz FAPSI «Ob utvezjdenii Instrukcii ob organizacii i obespechenii bezopasnosti hranenia, obrabotki i peredachi po kanalam sviazi s ispol’zovaniem sredstv kriptograficheskoi zazhiti informacii s ogranichennim dostupom, ne soderjazhei svedenii, sostavliaukih gosudarstvennuju tainu» ot13.06.2001g. № 152.
4. Tipovie trebovania po organizacii i obespecheniu funkcionirivanija shifroval’nih (kriptograficheskih) sredstv, prednaznachennih dlia zazhitiinformacii, ne soderjazhei svedenii, sostavliaukih gosudarstvennuju tainu v sluchae ih ispol’zovania dlia obespechenia bezopasnosti personal’nih dannih pri ih obrabotke v informacionnih sistemah personal’nih dannih: utv. rukovodstvom 8 centraFSBRossii 21.02.2008.
5. Metodicheskie recomendacii FSBRF «Po obespecheniu s pomojiu kriptosredstv bezopasnosti personal’nih dannih pri ih obrabotke v informacionnih sistemah personal’nih dannih s ispol’zovaniem sredstv avtomatizacii» ot 21.02.2008 g. № 149/54-144.
6. Prikaz FSB RF «Ob utverjdenii Trebovanii k sredstvam elektronnoi podpisi i Trebovanii k sredstvam udostoveriaujego centra» ot 27.12.2011g. № 796.