ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция № 10. Средства криптографической защиты информации

Лекция № 10.
Средства криптографической защиты информации

ЦЕЛЬ ЗАНЯТИЯ: **рассмотреть уровни защиты, понятийный аппарат в сфере разработки, производства, реализации и эксплуатации СКЗИ, также требования к порядку разработки, производства, реализации использования СКЗИ**

Учебные вопросы:

ВОПРОС 1. Основные уровни защиты информации на предприятии

ВОПРОС 2. Уровень криптографической защиты персональных данных, уровни специальной защиты от утечки по каналам побочных излучений и наводок и уровни защиты от несанкционированного доступа.

ВОПРОС 3. Терминология в сфере разработки, производства, реализации и эксплуатации СКЗИ

ВОПРОС 4. Требования к порядку разработки СКЗИ

ВОПРОС 5. Требования к порядку производства СКЗИ

ВОПРОС 6. Требования к порядку реализации СКЗИ

ВОПРОС 1.

Основные уровни защиты информации на предприятии

ВОПРОС 1.
Основные уровни защиты информации на предприятии

Ранее контроль доступа к конфиденциальной информации и защита её от влияний извне был задачей технических администраторов.

Сегодня же защита информации становится обязанностью каждого пользователя системы, что требует не только навыков обращения с системой безопасности, но и знаний о способах неправомерного доступа для предотвращения такового.

Надежный контроль над информацией обеспечивает безопасность бизнеса, а так же позволяет качественно и своевременно устранять ошибки, возникающие в течение производственных процессов, облегчая работу персонала.

ВОПРОС 1.
Основные уровни защиты информации на предприятии

Можно выделить три основных уровня защиты информации:

- защита информации на уровне рабочего места пользователя;
- защита информации на уровне подразделения предприятия;
- защита информации на уровне предприятия.

Информация первоначально создается на конкретном рабочем месте рядового пользователя системы предприятия.

Очень часто именно там информация хранится и первично обрабатывается.

ВОПРОС 1.
Основные уровни защиты информации на предприятии

Рабочие места чаще всего объединяются в локальную сеть для совместной работы и обмена информацией.

В данном случае речь идет о локальной сети подразделения, пользователи которой находятся друг от друга на достаточно небольших расстояниях.

Уровни защиты информации локальной сети подразделения отличаются более сложными механизмами, чем на рабочем месте пользователя.

Защита данных на различных уровнях имеет как общие, так и специальные способы защиты.

Локальные сети подразделений часто объединены в общую сеть предприятия, которая кроме рабочих мест рядовых пользователей имеет в своем составе также серверное оборудование и специализированные устройства, которые отвечают за функционирование и защиту всей сети предприятия.

Кроме того локальные сети предприятия могут быть географически удалены друг от друга.

ВОПРОС 1.
Основные уровни защиты информации на предприятии

Организация системы безопасности осуществляется также по уровням.

В системе безопасности существуют следующие уровни защиты информации:

- физическая защита информации;
- контроль доступа и персональная идентификация;
- применение ключей для шифрования данных;
- защита от излучения кабельных линий.

ВОПРОС 1.
Основные уровни защиты информации на предприятии

Для правильного построения защитных механизмов системы безопасности следует изучить не только функционирование информационных потоков внутри предприятия, но и возможности неправомерного доступа к информации извне.

В зависимости от типа угрозы, применяются определенные меры по защите информации.

ВОПРОС 1.
Основные уровни защиты информации на предприятии

В соответствии с механизмами реагирования на угрозы, определяют следующие уровни защиты информации:

- **ПРЕДОТВРАЩЕНИЕ** — внедрение служб контроля доступа к информации и технологии;
- **ОБНАРУЖЕНИЕ** — раннее обнаружение угрозы, даже в случае обхода механизмов защиты;
- **ОГРАНИЧЕНИЕ** — уменьшение размера информационных потерь, в случае уже произошедшего преступления;
- **ВОССТАНОВЛЕНИЕ** — обеспечение эффективного восстановления информации в случае её утраты или уничтожения.

ВОПРОС 2.

Уровень криптографической защиты персональных данных, уровни специальной защиты от утечки по каналам побочных излучений и наводок и уровни защиты от несанкционированного доступа

ВОПРОС 2. Уровень криптографической защиты персональных данных, уровни специальной защиты от утечки по каналам побочных излучений и наводок и уровни защиты от несанкционированного доступа.

Уровень криптографической защиты персональных данных, уровни специальной защиты от утечки по каналам побочных излучений и наводок и уровни защиты от несанкционированного доступа сформулированы в

Методических рекомендациях ФСБ России по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации

(21 февраля 2008 года №149/54-144)

ВОПРОС 2. Уровень криптографической защиты персональных данных, уровни специальной защиты от утечки по каналам побочных излучений и наводок и уровни защиты от несанкционированного доступа.

Различают шесть уровней КС1, КС2, КС3, КВ1, КВ2, КА1 криптографической защиты персональных данных, не содержащих сведений, составляющих государственную тайну, определенных в порядке возрастания количества и жесткости предъявляемых к криптосредствам требований, и, соответственно, шесть классов криптосредств, также обозначаемых через КС1, КС2, КС3, КВ1, КВ2, КА1.

ВОПРОС 2. Уровень криптографической защиты персональных данных, уровни специальной защиты от утечки по каналам побочных излучений и наводок и уровни защиты от несанкционированного доступа.

Уровень криптографической защиты персональных данных, обеспечиваемой криптосредством, определяется оператором путем отнесения нарушителя, действиям которого должно противостоять криптосредство, к конкретному типу.

При отнесении заказчиком нарушителя к типу Н1 криптосредство должно обеспечить криптографическую защиту по уровню КС1,
к типу Н2 – КС2,
к типу Н3 – КС3,
к типу Н4 – КВ1,
к типу Н5 – КВ2,
к типу Н6 – КА1.

ВОПРОС 2. Уровень криптографической защиты персональных данных, уровни специальной защиты от утечки по каналам побочных излучений и наводок и уровни защиты от несанкционированного доступа.

Различают три уровня КС, КВ и КА специальной защиты от утечки по каналам побочных излучений и наводок при защите персональных данных с использованием криптосредств.

При отнесении нарушителя:

— к типу Н1-Н3 должна быть обеспечена специальная защита по уровню КС,

— к типу Н4-Н5 – по уровню КВ,

— к типу Н6– по уровню КА.

ВОПРОС 2. Уровень криптографической защиты персональных данных, уровни специальной защиты от утечки по каналам побочных излучений и наводок и уровни защиты от несанкционированного доступа.

В случае принятия оператором решения о защите персональных данных в информационной системе (ИСПДн) от НСД в соответствии с нормативными документами ФСБ России различают шесть уровней АК1, АК2, АК3, АК4, АК5, АК6 защиты от НСД к персональным данным в ИСПДн, определенных в порядке возрастания количества и жесткости предъявляемых к системам защиты требований, и, соответственно, шесть классов ИСПДн, также обозначаемых через АК1, АК2, АК3, АК4, АК5, АК6.

ВОПРОС 2. Уровень криптографической защиты персональных данных, уровни специальной защиты от утечки по каналам побочных излучений и наводок и уровни защиты от несанкционированного доступа.

При отнесении в соответствии с нормативными документами ФСБ России заказчиком нарушителя:

— к типу Н1 в информационной системе должна быть обеспечена защита от НСД к персональным данным по уровню АК1,

— к типу Н2 – по уровню АК2,

— к типу Н3 – по уровню АК3,

— к типу Н4 – по уровню АК4,

— к типу Н5 – по уровню АК5,

— к типу Н6 – по уровню АК6.

ВОПРОС 3.

Терминология в сфере разработки, производства, реализации и эксплуатации шифровальных средств защиты информации

ВОПРОС 3.
Терминология в сфере разработки, производства, реализации и эксплуатации шифровальных средств защиты информации

Средство криптографической защиты информации — средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. 1992

ВОПРОС 3.
Терминология в сфере разработки, производства, реализации и эксплуатации шифровальных средств защиты информации

КРИПТОСРЕДСТВО –
шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну

«Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации».
ФСБ России от 21 февраля 2008 года № 149/54-144

ВОПРОС 3.
Терминология в сфере разработки, производства, реализации и эксплуатации шифровальных средств защиты информации

К криптосредствам относятся средства криптографической защиты информации (СКЗИ) — шифровальные (криптографические) средства защиты информации с ограниченным доступом, **не содержащей сведений, составляющих государственную тайну .**

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

ВОПРОС 3.
Терминология в сфере разработки, производства, реализации и эксплуатации шифровальных средств защиты информации

СКЗИ — Сертифицированные средства криптографической защиты конфиденциальной информации.
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;

ВОПРОС 3.
Терминология в сфере разработки, производства, реализации и эксплуатации шифровальных средств защиты информации

СКЗИ — Сертифицированные средства криптографической защиты конфиденциальной информации.

К СКЗИ относятся:

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

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

Приказ ФАПСИ от 13 июня 2001 г. № 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»)

Приказ ФАПСИ от 13 июня 2001 г. № 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»

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.

ВОПРОС 4.
Требования к порядку разработки средств криптографической защиты информации

ВОПРОС 4.
Требования к порядку разработки средств криптографической защиты информации

Приказ ФСБ РФ от 9 февраля 2005 г. № 66

"Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)«

ВОПРОС 4. Требования к порядку разработки средств криптографической защиты информации

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

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

ВОПРОС 4.
Требования к порядку разработки средств криптографической защиты информации

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

Оглавление

ВОПРОС 4.
Требования к порядку разработки средств криптографической защиты информации

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.

ВОПРОС 4.

Требования к порядку разработки средств криптографической защиты информации

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. 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.

ВОПРОС 4.

Требования к порядку разработки средств криптографической защиты информации

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.

ВОПРОС 4.
Требования к порядку разработки средств криптографической защиты информации

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 СКЗИ, 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 СКЗИ, срок ее действия, адрес индивидуального предпринимателя и телефон);

ВОПРОС 4.
Требования к порядку разработки средств криптографической защиты информации

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

— **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.

ВОПРОС 4.

Требования к порядку разработки средств криптографической защиты информации

В 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).

ВОПРОС 4.

Требования к порядку разработки средств криптографической защиты информации

В 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.

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.

ВОПРОС 4.

Требования к порядку разработки средств криптографической защиты информации

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).

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

ВОПРОС 4.

Требования к порядку разработки средств криптографической защиты информации

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).

ВОПРОС 4.

Требования к порядку разработки средств криптографической защиты информации

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).

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).

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

ВОПРОС 4.

Требования к порядку разработки средств криптографической защиты информации

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.

ВОПРОС 4.

Требования к порядку разработки средств криптографической защиты информации

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.

ВОПРОС 5.
Требования к порядку производства средств криптографической защиты информации

ВОПРОС 5.
Требования к порядку производства средств криптографической защиты информации

Рабочая конструкторская документация 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.

ВОПРОС 5.
Требования к порядку производства средств криптографической защиты информации

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.

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

ВОПРОС 5.

Требования к порядку производства средств криптографической защиты информации

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.

Все изменения в конструкции СКЗИ и технологии их изготовления изготовитель СКЗИ **должен согласовывать со специализированной организацией и ФСБ России.**

ВОПРОС 5.
Требования к порядку производства средств криптографической защиты информации

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.

ВОПРОС 5.

Требования к порядку производства средств криптографической защиты информации

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.

ВОПРОС 5.
Требования к порядку производства средств криптографической защиты информации

Разработка и производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем регламентируется ФСБ России.

С этой целью разработан и утвержден Административный регламент Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

Лекция № 10.
Средства криптографической защиты информации

Приказ ФСБ РФ от 30 августа 2012 г. N 440
"Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по осуществлению лицензирования 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)"

ВОПРОС 6.

Требования к порядку реализации СКЗИ

ВОПРОС 6.

Требования к порядку реализации средств криптографической защиты информации

СКЗИ реализуются (распространяются) вместе с правилами пользования ими, согласованными с ФСБ России.

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.

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

ВОПРОС 6.

Требования к порядку реализации средств криптографической защиты информации

Реализация (распространение) СКЗИ и (или) РКД на них осуществляется только после получения лицензии.

ВОПРОС 6.
Требования к порядку реализации средств криптографической защиты информации

Приказ ФСБ России от 16 марта 2009 г. № 106

"Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по распространению шифровальных (криптографических) средств"