ТЕМА 1:

Законодательные и нормативные правовые акты Российской Федерации по защите информации.

Требования к специалистам по контролю защищенности объектов информатизации по требованиям безопасности

Нормативные правовые акты Российской Федерации по защите информации

Законодательные акты

Конституция Российской Федерации (1993г.)

Концепция национальной безопасности Российской Федерации (2000г.)

Доктрина информационной безопасности Российской Федерации (2000г.)

Закон Российской Федерации «О безопасности» (1993г.)

ФЗ «Об информации, информатизации и защите информации» (1995г.)

Закон Российской Федерации «О государственной тайне» (1997г.)

ФЗ «Об участии в международном информационном обмене» (1996г.)

ФЗ «О лицензировании отдельных видов деятельности» (1998г.)

ФЗ «О сертификации продукции и услуг» (1998г.)

ФЗ «О связи» (1995г.)

Нормативные правовые акты Российской Федерации по защите информации

Нормативные правовые акты Президента РФ

Об основах государственной политики в сфере информатизации 20.01.94 № 170

Вопросы межведомственной комиссии по защите государственной тайны 20.01.96 № 71

Об утверждении перечня сведений конфиденциального характера 06.03.97 № 188

О некоторых вопросах межведомственной комиссии по защите государственной тайны 14.06.97 № 594

О перечне сведений, отнесенных к государственной тайне 24.01.98 № 61

Вопросы Государственной технической комиссии при Президенте Российской Федерации 19.02.99 № 212

Об утверждении перечня должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне 17.01.00 № 6-рп

Нормативные правовые акты Российской Федерации по защите информации

Нормативные правовые акты Правительства РФ

Об установлении порядка рассекречивания и продления сроков засекречивания архивных документов Правительства СССР 20.02.95 № 170

О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны 15.04.95 № 333

О сертификации средств защиты информации 20.06.95 № 608

Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности 04.09.95 № 870

О подготовке к передаче сведений, составляющих государственную тайну, другим государствам 02.08.97 № 973

О лицензировании отдельных видов деятельности 11.02.01 № 135

Термины и определения

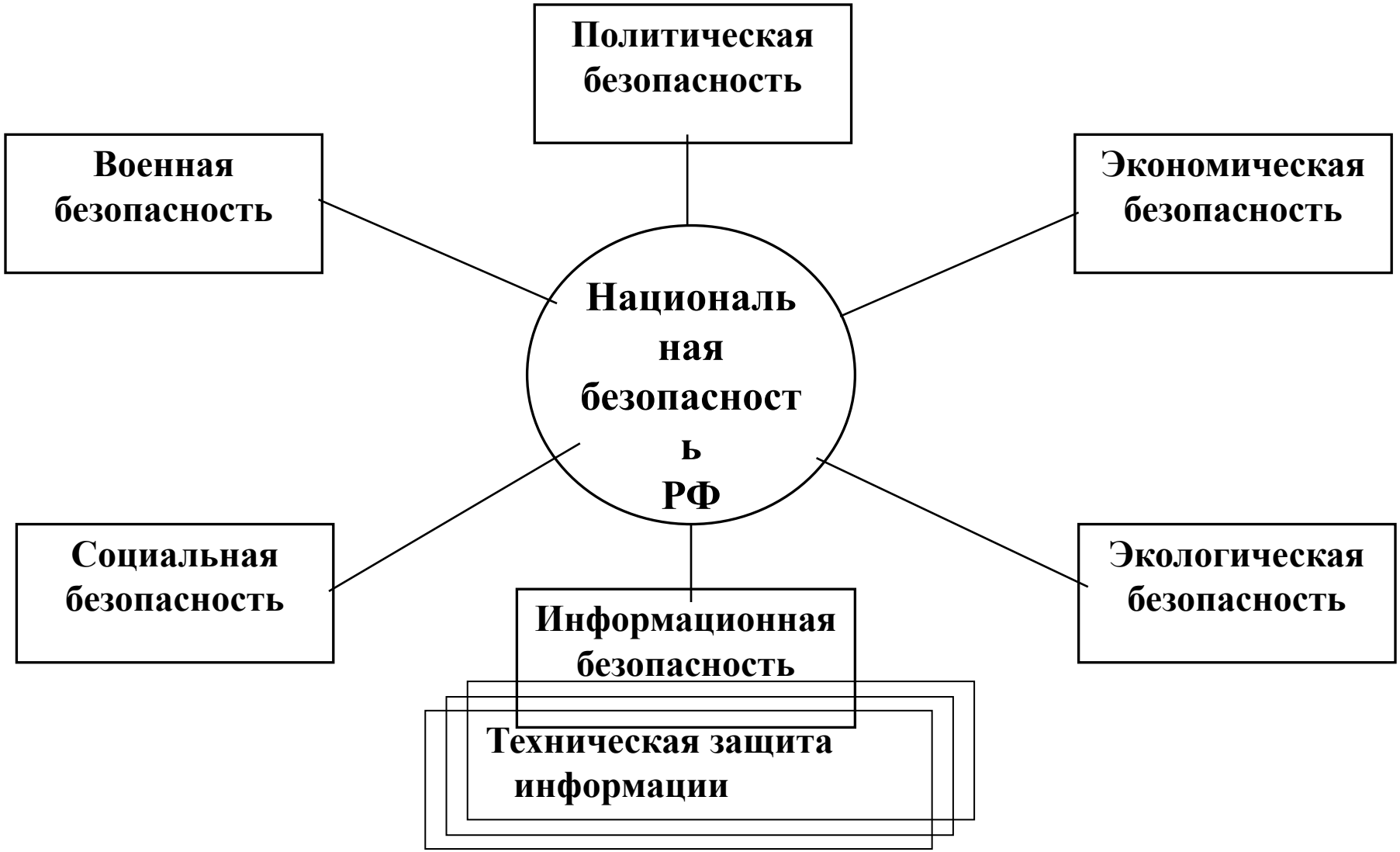
Безопасность - состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. (Закон «О безопасности»)

Информационная безопасность Российской Федерации - это состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства (Доктрина информационной безопасности РФ)

Государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации (Закон «О государственной тайне»)

Носители сведений, составляющих гостайну, - материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов (Закон «О государственной тайне»)

МЕСТО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЩЕЙ СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ



ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

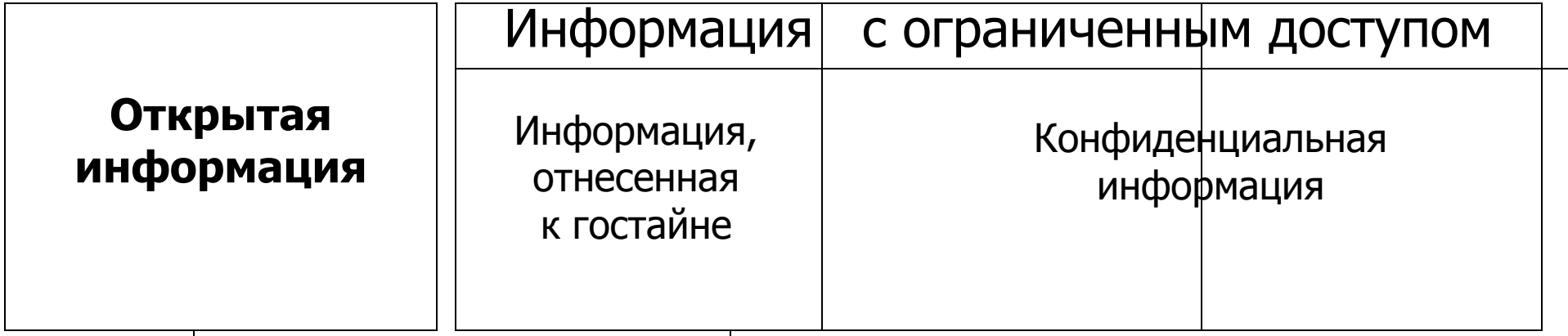
Государственная система защиты информации – совокупность органов защиты информации, используемых ими средств и методов защиты информации и ее носителей, а также мероприятий, проводимых в этих целях.

ОСНОВНЫЕ ЗАДАЧИ

- Проведение единой технической политики, организация и координация работ по защите информации в различных сферах деятельности государственных структур
- Нормативно-методическое обеспечение деятельности государственной системы защиты информации
- Оценка возможностей технической разведки, формирование модели угроз информационной безопасности
- Проведение организационно-технических мероприятий по противодействию технической разведке и технической защите информации
- Организация сил, создание средств защиты информации и средств контроля эффективности принятых мер защиты
- Контроль состояния защищенности информации в органах государственной власти и организациях

Информационные ресурсы по категориям доступа

(ФЗ «Об информации, информатизации и защите информации»)



- законодательные и другие нормативные акты…
- документы, содержащие информацию о чрезвычайных ситуациях…
- документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления…
- документы, накапливаемые в открытых фондах библиотек и архивов

«О перечне сведений, отнесенных к государственной тайне»
(24.01.98 № 61)

"Об утверждении перечня сведений конфиденциального характера"
(06.03.97 № 188)

Что подлежит защите ?

документированная информация (документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать

Ответ:

любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу ***(ст.21 ФЗ 24).***

Кто определяет возможен ли ущерб от неправомерного обращения … ?

Ответ: ФЗ № 24, разделив информационные ресурсы по категориям доступа:

- **открытая информация**

•законодательные и другие нормативные акты…
документы, содержащие информацию о чрезвычайных ситуациях…

•документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления…

•документы, накапливаемые в открытых фондах библиотек и архивов

- **информация ограниченного доступа**

 информация, отнесенная к гостайне (Указ Президента 24.01.98 № 61)

 конфиденциальная информация (Указ Президента 06.03.97 № 188)

Кто устанавливает режим защиты информации ограниченного доступа ?

Ответ:

- в отношении сведений, отнесенных к государственной тайне, - *уполномоченными органами на основании Закона Российской Федерации "О государственной тайне";*
- в отношении конфиденциальной документированной информации - *собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона* ***(именно собственник, а не владелец);***
- в отношении персональных данных - *Федеральным законом* (ст.21 ФЗ 24)

Кто определяет порядок накопления и обработки, правила защиты и порядок доступа к конфиденциальной информации?

Ответ:

Органами государственной власти, ответственными за определенный вид и массивы информации, либо непосредственно ее собственником в соответствии с законодательством (ст.12 ФЗ №24)

Кто осуществляет контроль в негосударственных структурах?

Ответ:

Органы государственной власти (в порядке, определяемом Правительством Российской Федерации).

Порядок относительно контроля определен в Постановлении № 290 и № 348

Что проверяется ?

Ответ:

- соблюдение требований к защите информации (которые устанавливает собственник, а если собственник не установил, то они изложены в СТР-К)
- соблюдение требований по эксплуатации специальных программно-технических средств защиты
- обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом

Какие права у собственника, которые он сам может реализовать ?

Ответ:

- осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований
- обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах. Соответствующие органы определяет Правительство Российской Федерации.

  Эти органы соблюдают условия конфиденциальности самой информации и результатов проверки.

Какие обязанности у владельца информационных ресурсов ?

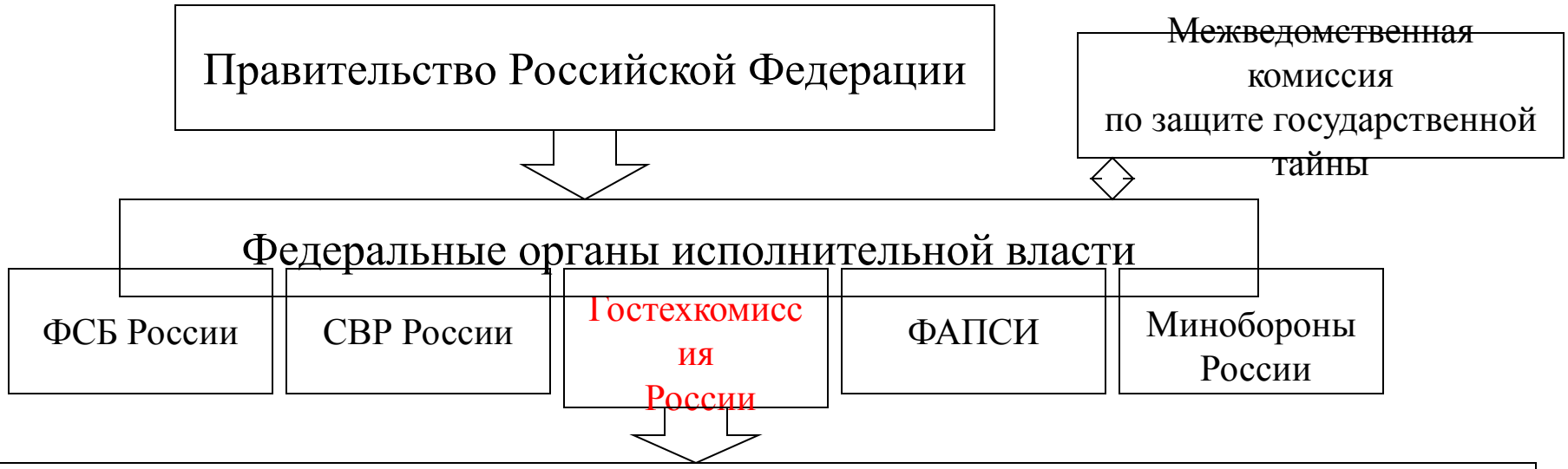
Ответ:

1. Обеспечить соблюдение режима обработки и правил предоставления информации пользователю, установленных законодательством РФ или собственником.

2. Несет юридическую ответственность за нарушение правил работы с информацией в порядке, предусмотренном законодательством (**ст.15 ФЗ №24)**

СИСТЕМА ЛИЦЕНЗИРОВАНИЯ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Лицензирование – мероприятия, связанные с выдачей лицензий на осуществление лицензируемых видов деятельности и надзором за соблюдением лицензиатами соответствующих лицензионных требований и условий



Лицензируемые виды деятельности

~ **Допуск предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну**

~ **Создание средств защиты информации**

~ **Осуществление мероприятий и (или) оказание услуг по защите государственной тайны**

РАБОТЫ И УСЛУГИ, ПОДЛЕЖАЩИЕ ЛИЦЕНЗИРОВАНИЮ, В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Работы и услуги

1.Сертификация и сертификационные испытания

3.Разработка, производство, реализация, установка, монтаж, наладка, испытания, ремонт и сервисное обслуживание

4.Проведение специсследований на побочные электромагнитные излучения и наводки технических средств обработки информации

2.Контроль защищенности информации ограниченного доступа, аттестация средств и систем на соответствие требованиям по защите информации

5.Проектирование объектов в защищенном исполнении

Объекты

- технические средства защиты информации
- защищенные технические средства обработки информации
- технические средства контроля эффективности мер защиты информации
- программные средства защиты информации от несанкционированного доступа (НСД)
- защищенные программные средств обработки информации от НСД
- программные средства контроля защищенности информации от НСД
- программные средства по требованиям безопасности

- автоматизированные системы различного уровня и назначения
- системы связи, приема, обработки и передачи данных
- системы отображения и размножения, вспомогательные технические средства и системы
- помещения со средствами (системами), подле-

ОСНОВНЫЕ ПОКАЗАТЕЛИ ДЕЯТЕЛЬНОСТИ В СИСТЕМАХ ЛИЦЕНЗИРОВАНИЯ И СЕРТИФИКАЦИИ ГОСТЕХКОМИССИИ РОССИИ

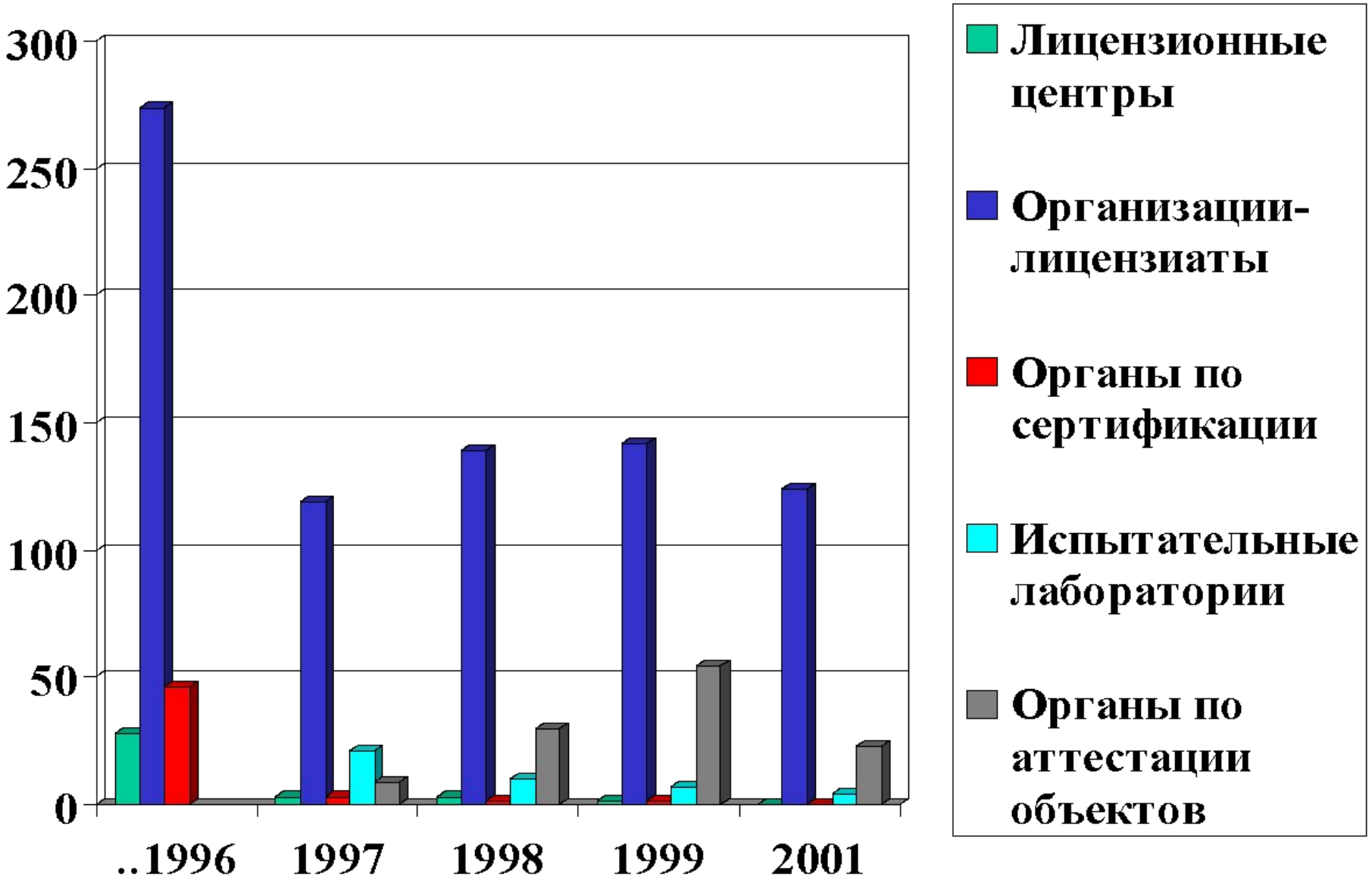
Федеральные округа :	ЛЦ	ОЛ	ОС	ИЛ	ОА
Центральный (18 субъектов РФ)	20	445	3	40	65
Северо-Западный (11 субъектов)	6	124	1	8	13
Северо-Кавказский (13 субъектов)	2	27	-	2	5
Приволжский (15 субъектов)	3	75	-	2	13
Уральский (16 субъектов)	-	49	-	1	5
Сибирский (16 субъектов)	2	29	-	1	8
Дальневосточный (10 субъектов)	2	16	-	-	-
Итого:	35	765	4	54	143

Сертифицированные средства защиты информации:

- **Программные средства** 182
- **Программно-технические средства** 244
- **Технические средства** 136
- **Другие** 30
- **Всего -** 592

ЛЦ – лицензионные центры
ОЛ – организации-лицензиаты
ОС – органы по сертификации
ИЛ – испытательные лаборатории
ОА – органы по аттестации объектов информатизации

Динамика изменения количества лицензиатов Гостехкомиссии России



Нормативная база требований к специалистам органов по аттестации объектов информатизации по требованиям безопасности

- Правила по проведению сертификации в Российской Федерации (постановление Госстандарта России от 10.05.2000 г. № 26);
- Правила проведения государственной регистрации систем сертификации и знаков соответствия, действующих в Российской Федерации (постановление Госстандарта России от 22.04.99 г. № 18);
- Правила по сертификации Системы сертификации ГОСТ Р "Требования к экспертам и порядок их аттестации" (постановление Госстандарта России от 15.09.94 г. № 224);
- ГОСТ Р 51000.9-97 "Государственная система стандартизации Российской Федерации. Система аккредитации в Российской Федерации. Общие критерии для органов, проводящих сертификацию персонала“;
- ГОСТ Р ИСО 10011-2-93 "Руководящие указания по проверке систем качества. Часть 2. Квалификационные критерии для экспертов-аудиторов»;
- Положение о сертификации средств защиты информации по требованиям безопасности информации (введено в действие приказом Председателя Гостехкомиссии России от 27.10.95 г. № 199).

Требования к специалистам органов по аттестации объектов информатизации по требованиям безопасности

Должен знать:

- **требования нормативно-методических документов по организации аттестации ОИ по требованиям безопасности информации;**
- **основные положения и требования организационно-распорядительных и нормативно-методических документов по защите информации и контролю ее защищенности;**
- **характеристики информации, циркулирующей в средствах и системах информатизации, а также в выделенных помещениях ОИ;**
- **способы и средства защиты ОИ;**
- **возможности и характеристики технических, программно-технических и программных средств защиты информации;**
- **способы и средства инструментального контроля эффективности принимаемых мер защиты информации на ОИ;**
- **каналы утечки информации на ОИ**

Требования к специалистам органов по аттестации объектов информатизации по требованиям безопасности

Должен уметь:

- определять перечень охраняемых сведений ОИ;
- анализировать и выявлять каналы утечки информации и несанкционированного доступа к ней, используя при этом инструментальные средства контроля;
- проводить анализ документов, представленных заявителем для аттестации ОИ;
- разрабатывать программу и методику проведения аттестационных испытаний ОИ;
- проводить оценку достаточности мероприятий по защите информации на ОИ;
- проводить анализ результатов аттестационных испытаний;
- оформлять протоколы, экспертные заключения и аттестаты соответствия по результатам аттестационных испытаний ОИ;
- организовывать и проводить инспекционный контроль за аттестованными ОИ

Требования к специалистам в области защиты информации

Документ / Требования	Спец. технич. требов. и рекомен. …	РД. Классификация АС…	РД. Временное положение …	Положение о лицензировании (Постан. Правит. №333)	Информ. агенство ФРГ. "Руководство…"	Станд. BSI BS7799
Проверка уровня подготовки (без описания методологии проверки)	+					+
Требования к квалификации (без описания методологии проверки)				+		
Описание методологии проверки						
Распределение ответственности среди специалистов в области ИБ	+				+	+

Документ / Требования	Спец. технич. требов. и рекомен.	РД Классификация АС…	РД Временное положение …	Положение о лицензировании …	Информ. агенство ФРГ. "Руководство…"	Станд. BSI BS7799
Выделение требований к определенному специалисту (администратору ИБ)		+			+	
Определенный порядок обучения, переподготовки кадров и повышения квалификации			+		+	+
Определенная схема выдачи документа о прохождении обучения						
Определенный порядок увольнения и замены кадров					+	
Отработка реакции специалистов на критические события					+	+