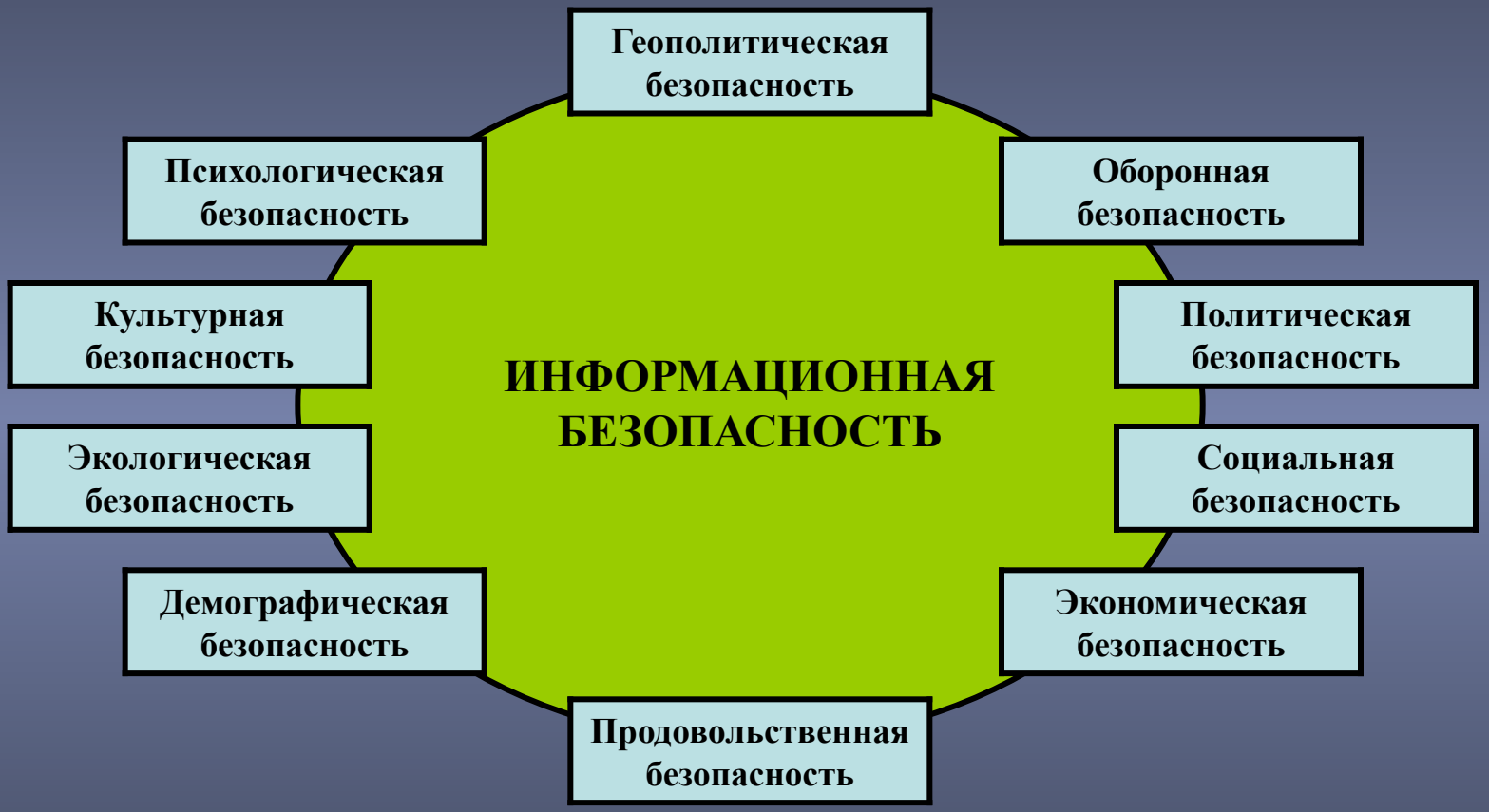
ВОЕННАЯ АКАДЕМИЯ СВЯЗИ

"Кафедра радиоэлектронной защиты, безопасности связи и информации"

Организационные основы комплексной защиты информации на объектах информатизации

Доктрина информационной безопасности РФ

Информационная безопасность является системообразующим фактором структуры национальной безопасности России



Роль и место информационной безопасности в обеспечении национальной безопасности России

Постановление Правительства Российской Федерации № 912 – 51 от 1993 года

ПОЛОЖЕНИЕ «О государственной системе защиты информации в РФ от ИТР и от ее утечки по техническим каналам»

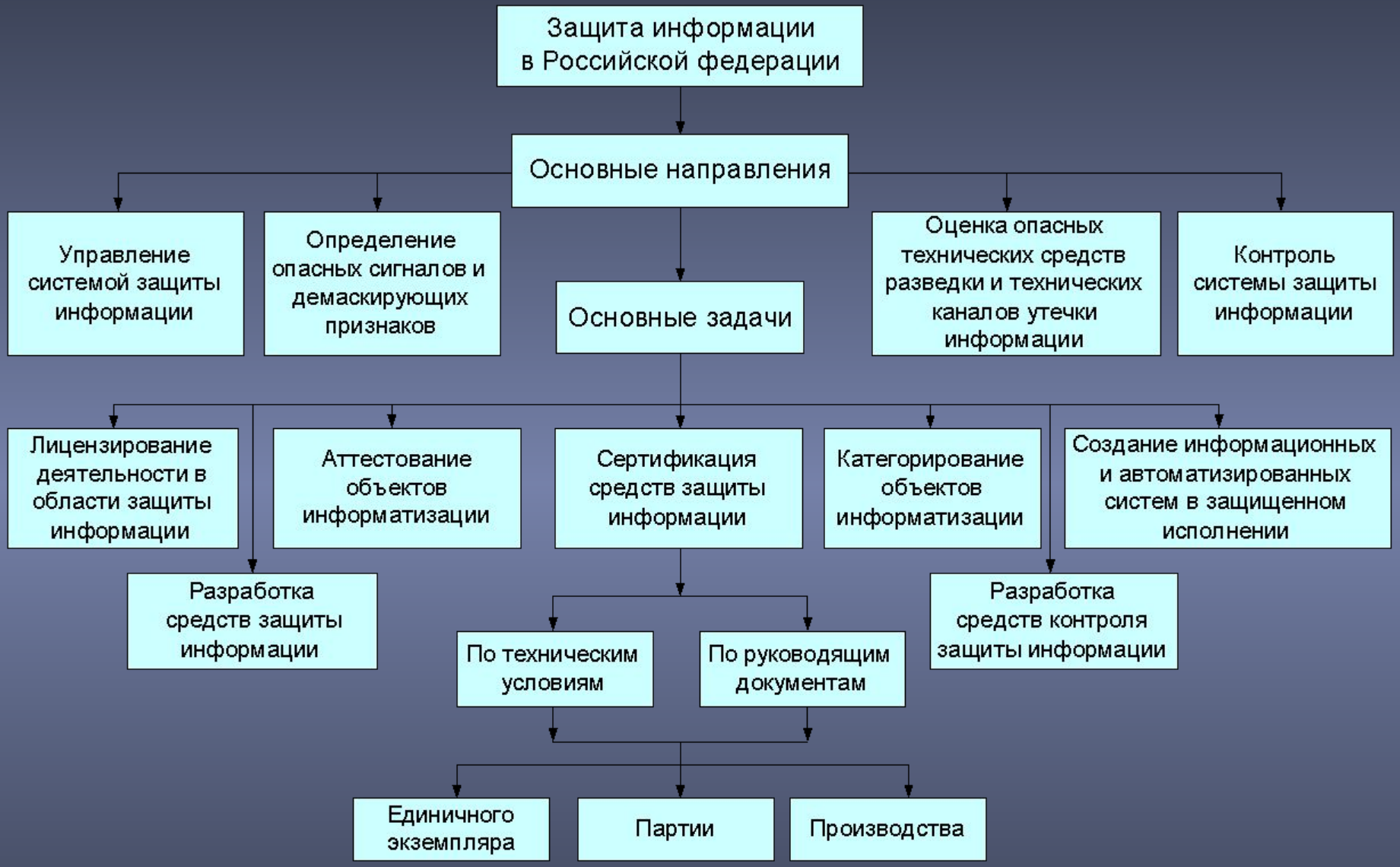
Является документом, обязательным для выполнения при проведении работ по защите информации, содержащей сведения, составляющие государственную или служебную* тайну, в органах государственной власти**, на предприятиях и в их объединениях, учреждениях и организациях независимо от их организационно-правовой формы и формы собственности.

---

* Согласно Указа Президента РФ № 188 от 1997 г. служебная тайна (информация), наряду с коммерческой, юридической и другими, является составной частью комплексной КОНФИДЕНЦИАЛЬНОЙ информации.

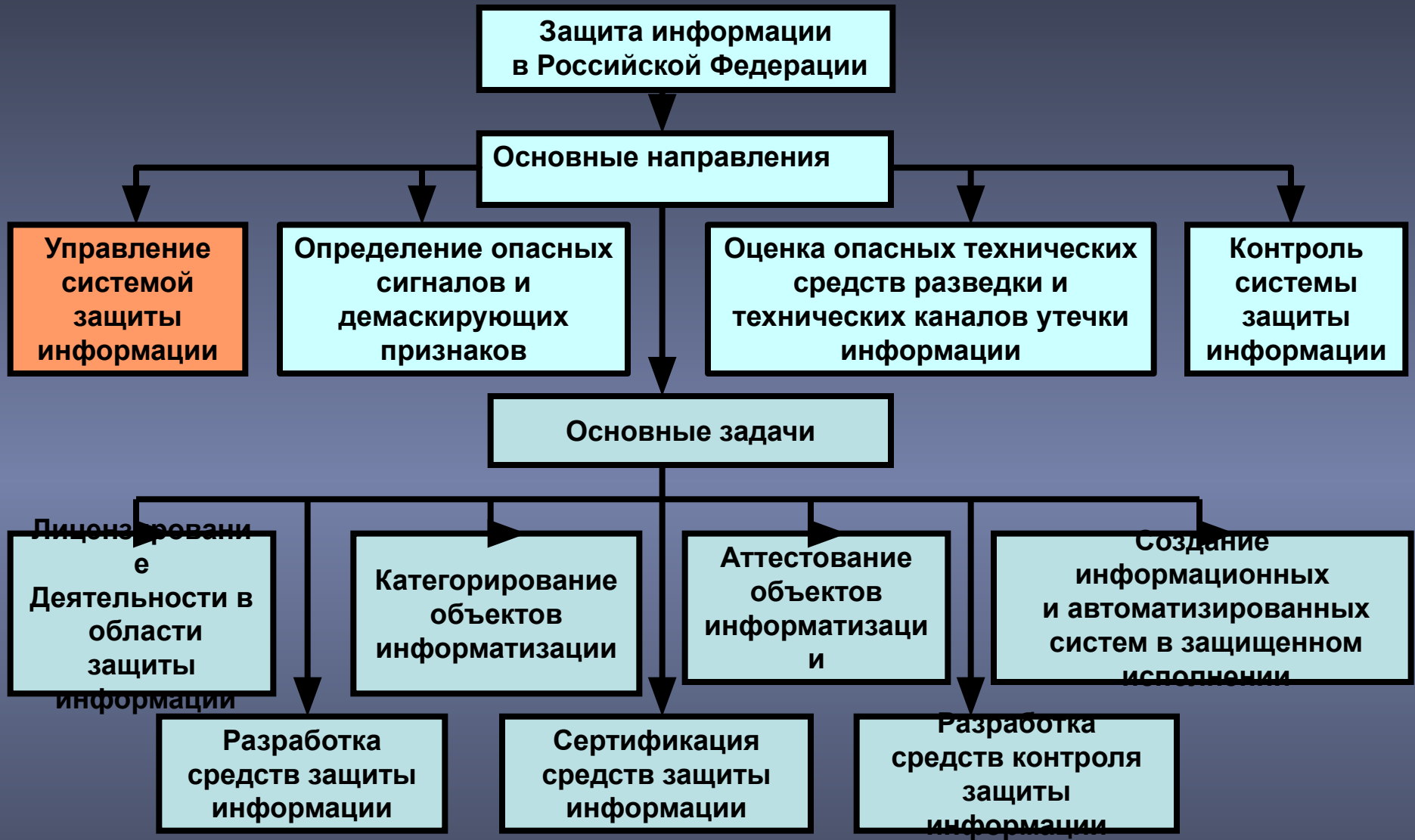
** В составе органов государственной власти рассматриваются органы власти федерального уровня; органы исполнительной и судебной власти субъектов РФ; органы местного самоуправления

СТАТУС ПОЛОЖЕНИЯ О ГОСУДАРСТВЕННОЙ системе защиты информации в Российской Федерации



Основные направления по защите информации

Обобщенная структура Государственной системы защиты информации в Российской Федерации

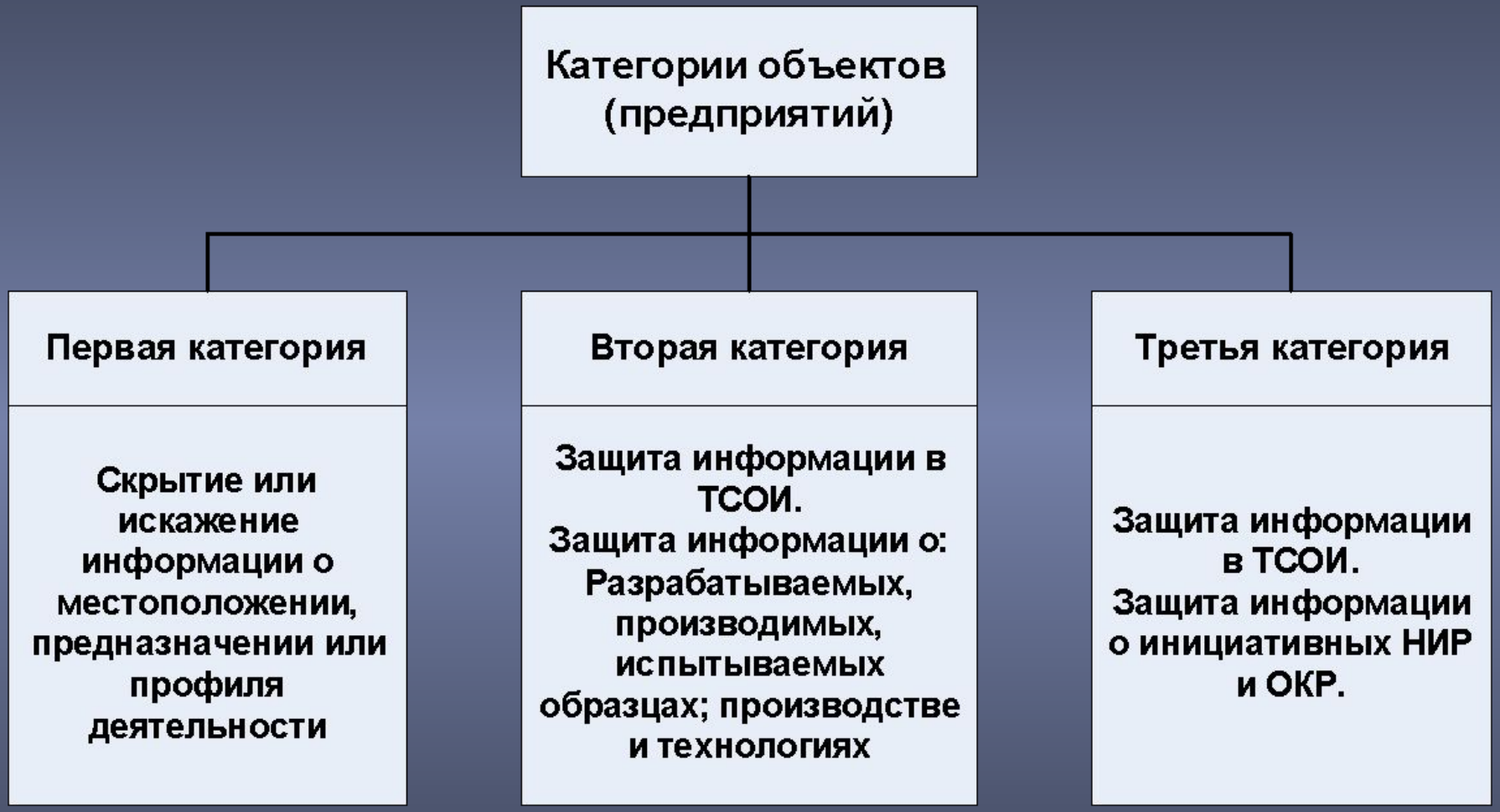


Основные направления и задачи по защите информации.

Основные угрозы материальным и информационным ресурсам предприятия

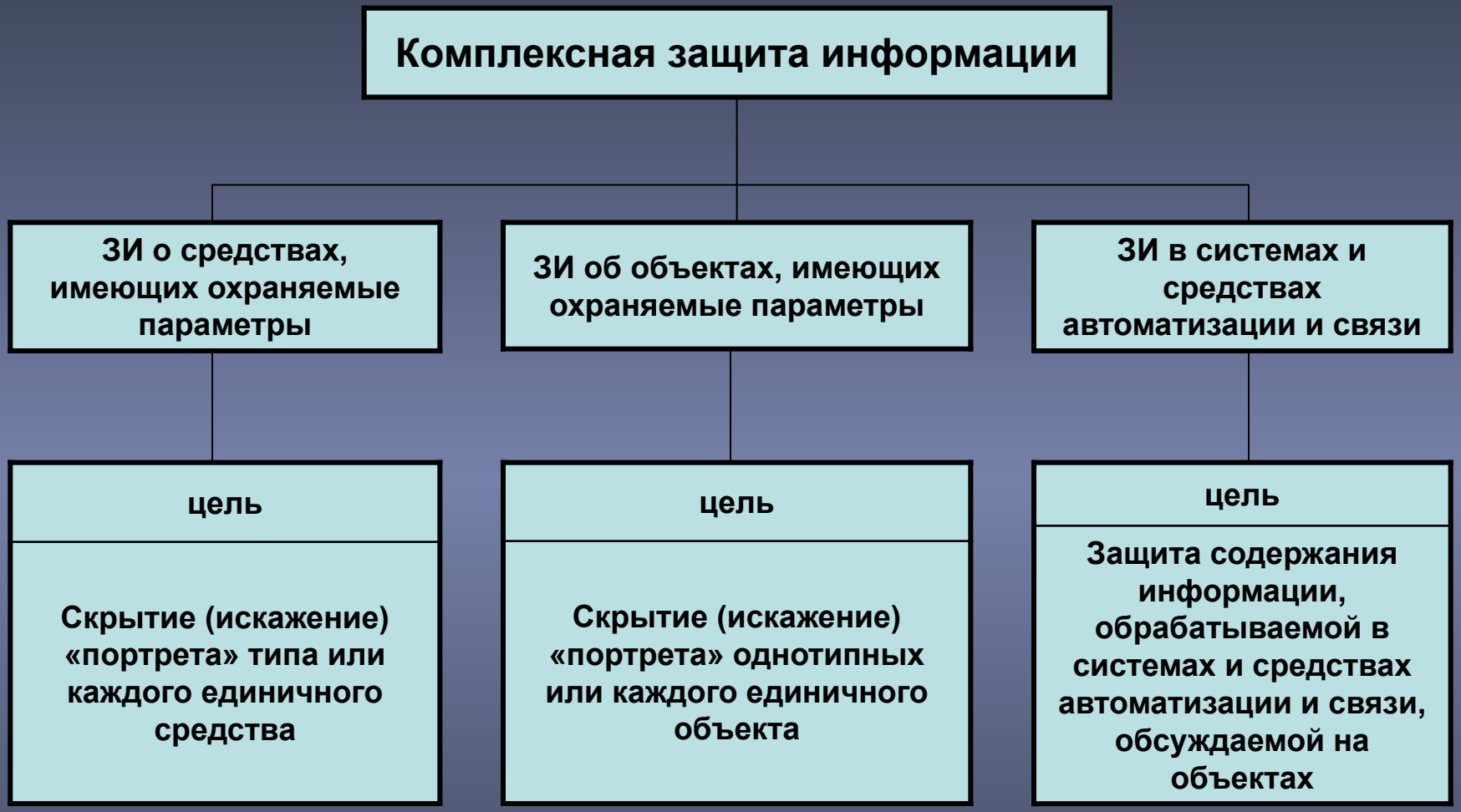
Основные угрозы информации на объектах связи и в органах управления ими

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ
№ 912 – 51 от 15.09.1993 г. (ст.41)



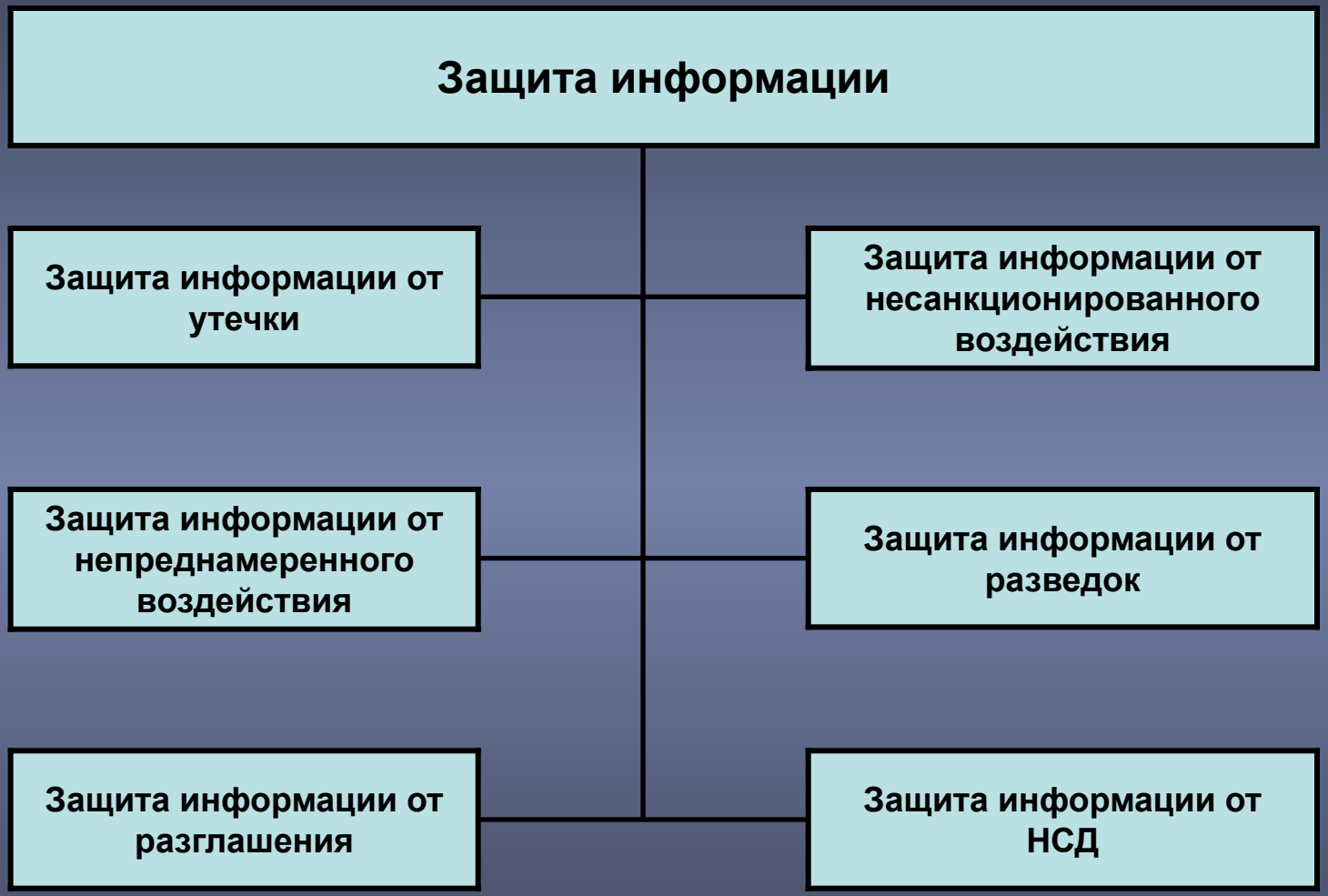
КРИТЕРИИ КАТЕГОРИРОВАНИЯ ОБЪЕКТОВ УПРАВЛЕНИЯ И ПРОМЫШЛЕННЫХ ОБЪЕКТОВ

Постановление Правительства РФ № 912-51 от 1993 года



Сущность и содержание комплексной защиты информации

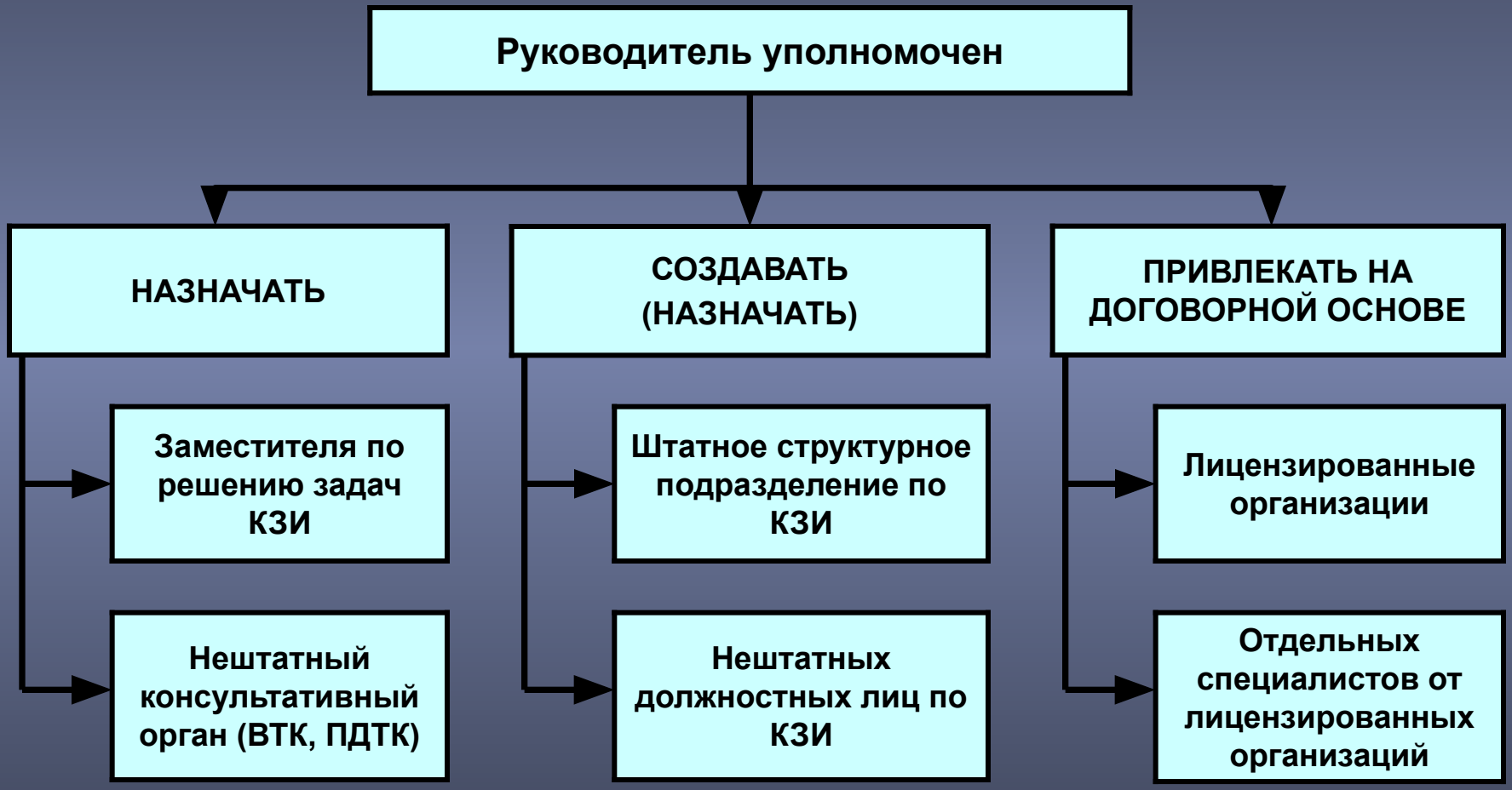
ГОСТ Р 50922 – 96 «Защита информации. Основные термины и определения»



НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТЕ

Постановление Правительства РФ № 912-51 от 1993 года

РУКОВОДИТЕЛЬ – основное должностное лицо, отвечающее за ВСЕ вопросы организации и обеспечения комплексной защиты информации на предприятии (в учреждении, организации)



ПРАВА И ПОЛНОМОЧИЯ РУКОВОДИТЕЛЯ ПО ОБЩЕЙ ОРГАНИЗАЦИИ РАБОТ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Постановление Правительства России
№ 333 от 15 апреля 1995 года.

Инструкция Гостехкомиссии России
От 17 октября 1995 года.

Руководитель должен уметь:

Знать	Уметь организовать	Быть ознакомеленым
1.Законодательные акты РФ по вопросам защиты государственной тайны. 2. Нормативные документы, утверждаемые Правительством РФ, по обеспечению защиты сведений, составляющих государственную тайну нормативно-методические документы по режиму секретности, противодействию иностранным разведкам и защите информации от утечки по техническим каналам 3. Основные охраняемые сведения о предприятии и перечень продукции, подлежащей защите от разведок. 4. Возможные каналы утечки информации по всему технологическому циклу разработки, изготовления и испытаний продукции предприятия.	1. Проведение анализа возможностей разведки по добыванию сведений, составляющих государственную тайну; разработку мероприятий по защите сведений о предприятии и выпускаемой продукции, составляющих государственную тайну, и оценку их достаточности. 2. Аттестование рабочих мест по всему технологическому циклу разработки, изготовления и испытания продукции. 3. Комплексный контроль выполнения принимаемых мер по защите сведений, составляющих государственную тайну.	1. С возможностями иностранных разведок по добыванию сведений, составляющих государственную тайну. 2. С методиками контроля выполнения норм противодействия иностранным техническим разведкам. 3. С государственной системой лицензирования деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну.

Структура и основное содержание Концепции информационной безопасности организации

ПОСЛЕДОВАТЕЛЬНОСТЬ И СОДЕРЖАНИЕ ОРГАНИЗАЦИИ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ


Защита информации
Защита информации от разглашения
Тестирование персоонала
Разграничение доступа исполнителей
Организация защищенного документооборота
От утечки по техническим каналам
Защита информации в линиях и каналах связи
Ограничение доступа к средствам связи
Введение перечня разрешенных и запрещенных сведений
Криптографические методы
От утечки по техническим каналам
Защита ОИ от НСФД
Подразделения охраны и пропуска
Отдельные технические средства и системы
Интегрирован-е автоматизированные системы
От утечки по техническим каналам
Защита информации в выделенных помещениях
От прослушивания и просматривания
От несанкционированной записи
ЗИ при использовании сотовых телефонов
От утечки по техническим каналам
Защита информации на объектах ТСОИ
От утечки по техническим каналам
От прослушивания и просматривания
ЗИ при использовании сотовых телефонов
От несанкционированной записи
Защита информации на объектах ЭВТ (АС)
От НСД
От утечки по техническим каналам
ЗИ при использовании сотовых телефонов
От несанкционированной записи

АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Объекты информатизации

Системы
- Автоматизированной обработки информации ;
- Связи;
- Отображения и размножения информации .

Вместе с помещениями
В которых они установлены

Помещения
предназначенные для :
- Переговоров ;
- Совещаний ;
- Звукозаписи и воспроизведения .

Аттестация объектов информатизации
комплекс организационно -технических мероприятий ,
в результате которых специальным документом
АТТЕСТАТОМ СООТВЕТСТВИЯ
подтверждается , что объект соответствует требованиям
стандартов и других нормативно -технических документов по безопасности информации

А т т е с т а ц и я

Обязательная	**Добровольная**
• Обработка государственной службы ; • Управление экологически опасными объектами .	• По инициативе заказчика .

Аттестат соответствия дает право

- Обработки информации с установленным уровнем конфиденциальности
- Полноправного экономического , научного и делового сотрудничества
- Гарантировать партнерам защиту их информации

СИСТЕМА АТТЕСТАЦИИ

ПОРЯДОК ПРОВЕДЕНИЯ АТТЕСТАЦИИ

В ХОДЕ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

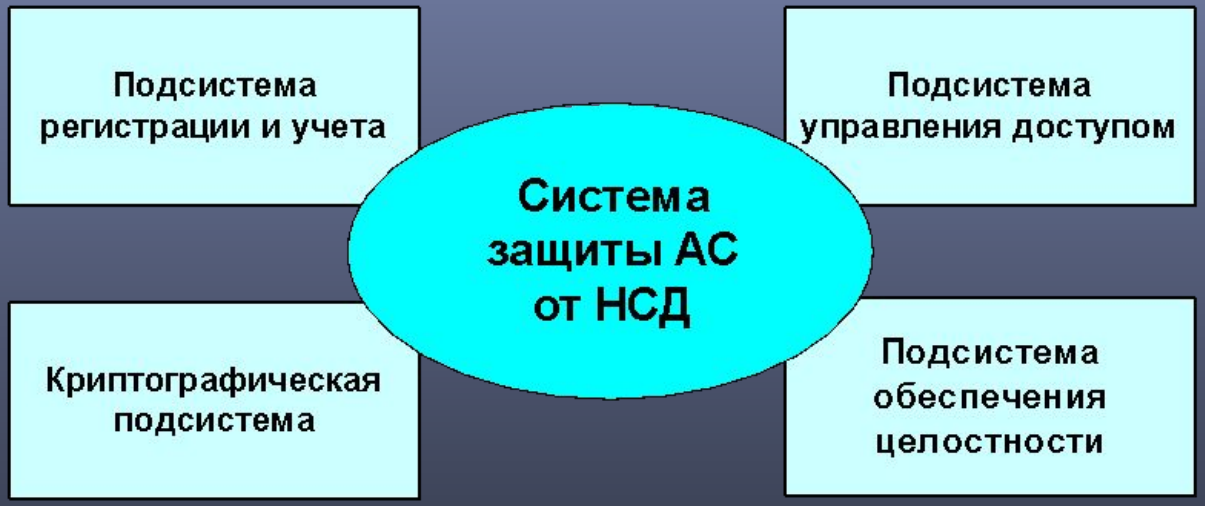
Осуществляется анализ	1. Организационной структуры объекта ; 2. Информационных потоков ; 3. Состава и структуры комплекса : - технических средств ; - программного обеспечения ; - системы защиты информации; 4. Разработанной документации и ее соответствия требованиям нормативной документации по ЗИ.
Определяется правильность	1. Категорирования объектов ВТ ; 2. Классификации АС; 3. Выбора и применения средств ЗИ .
Проводятся испытания	1. Несертифицированных средств и систем защиты информации .
Проверяется	1. Уровень подготовки кадров ; 2. Распределение ответственности за обеспечение безопасности .
Проводятся комплексные аттестационные испытания	1. Объекта информатизации в реальных условиях эксплуатации .
Оформляются	1. Протоколы испытаний ; 2. Заключения по результатам аттестации .

Категорирование объектов информатизации

	Уровень конфеденциальности информации		
Категория объекта информатизации	ОВ	СС	С
	1	2	3

Классификация защищенности АС от НСД

Режим обработки данных	Уровень полномочий пользователей	Наличие информации различного уровня конфинденциальности	Уровень конфеденциальности информации				
			ОВ	СС	С	НС	НС
Индивидуальный	Одинаковые права доступа	Один	3А			3Б	
Коллективный		Различный	2А			2Б	
	Разные права доступа		1А	1Б	1В	1Г	1Д



МЕТОДЫ ПРОВЕРОК И ИСПЫТАНИЙ

ТРЕБОВАНИЯ К ОБЪЕКТАМ РАЗЛИЧНЫХ КАТЕГОРИЙ

Подсистема	Требования	1А, 1Б, 1В	2А	3А
Подсистема **управления доступом**	В систему, к внешним устройствам	+	+	+
	К программам, к файлам	+	+	+
	Управление потоками информации	+	+	+
Подсистема **регистрации и учета**	Вход/выход в/из систему	+	+	+
	Запуск/завершение программ	+	+	+
	Выдача печатных документов	+	+	+
	Доступ программ к файлам	+	+	
	Доступ к внешним устройствам	+	+	
	Изменение полномочий	+		
	Создание защищаемых объектов	+	+	+
	Учет носителей информации	+	+	+
	Очистка освобождаемых областей памяти	+	+	+
	Сигнализация попыток нарушения защиты	+		
Подсистема **обеспечения целостности**	Программ и обрабатываемой информации	+	+	+
	Физическая охрана СВТ и носителей информации	+	+	+
	Наличие администратора (службы) защиты информации в АС	+	+	
	Периодическое тестирование системы защиты от НСД	+	+	+
	Наличие средств восстановления системы защиты от НСД	+	+	+
	Использование сертифицированных средств защиты	+	+	+

ТЕХНИЧЕСКИЙ ПАСПОРТ

На помещение _____ категории

Комната№ _____ корпус

Составил _____

(фамилия, инициалы, подпись специалиста по защите)

Начальник подразделения по защите информации

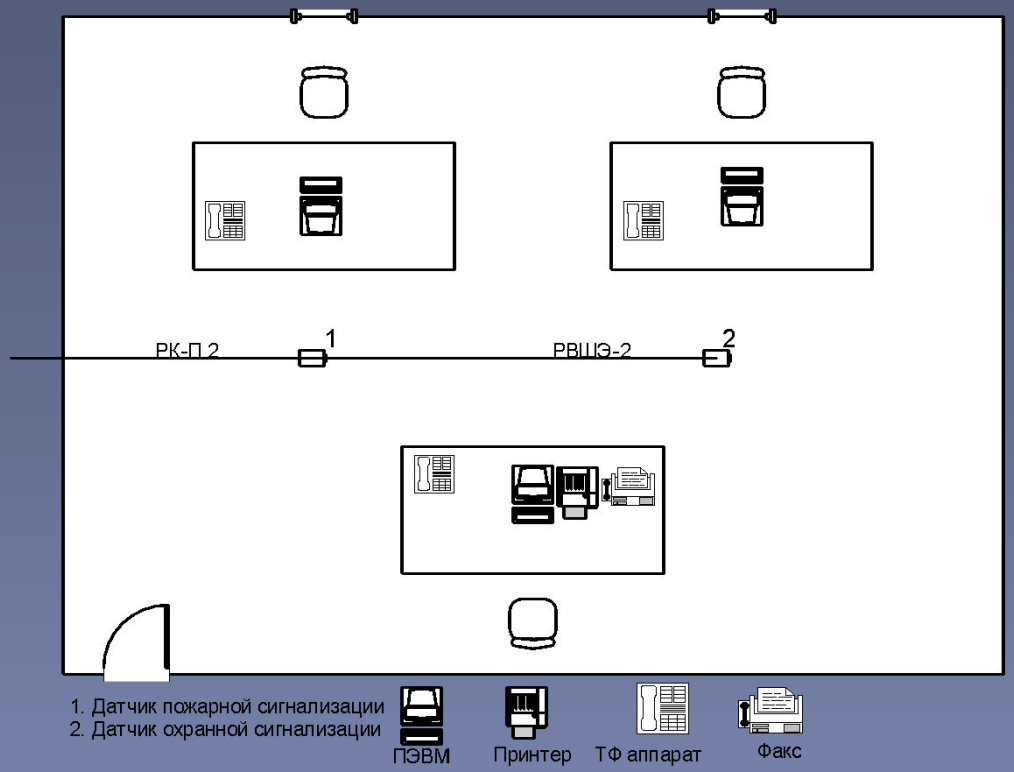
_____

(ФИО и подпись лица, ответственного за организационные мероприятия)

Ознакомлен _____

(ФИО и подпись лица, ответственного за помещение)

1.План размещения оборудования и схема кабельных соединений с указанием типа и емкость кабельных линий, выходящих за пределы объекта ТСПИ.



2. Перечень оборудования ОТСС, ВТСС и мебели, установленных на объекте ТСПИ, с указанием типа, учетного или инвентарного номера и даты установки и замены.

Вид оборудования	Тип	Учетный номер (заводской №)	Дата установки	Класс технического средства	Данные о спец исследовании и спецпроверке
Телефонный аппарат ГАТС № 556-67-74	КХ-236 "Panasonic"	№ 36 квдв 0076654	03.03.99.	ВТСС	Заключение о СП № 123 от 21.10.97г

3. Меры защиты технических средств и помещения:

1. Телефонный аппарат 556-97-14

• в линии установлен "Гранит 8" заводской № 2345;

• микрофон зашунтирован конденсатором емкостью 10 пФ;

1.Вход в помещение оборудован тамбуром, двери двойные, обиты слоем ваты и дермантина. Дверные проемы имеют резиновые уплотнения.

4. Отметка о проверке средств защиты

Вид оборудования	Учетный №	Дата проверки	Заключение по проверке	Номер документа
Сигнал-8	0152	25.0195г	Соответствует ТУ	Журнал контроля №4 ДСП

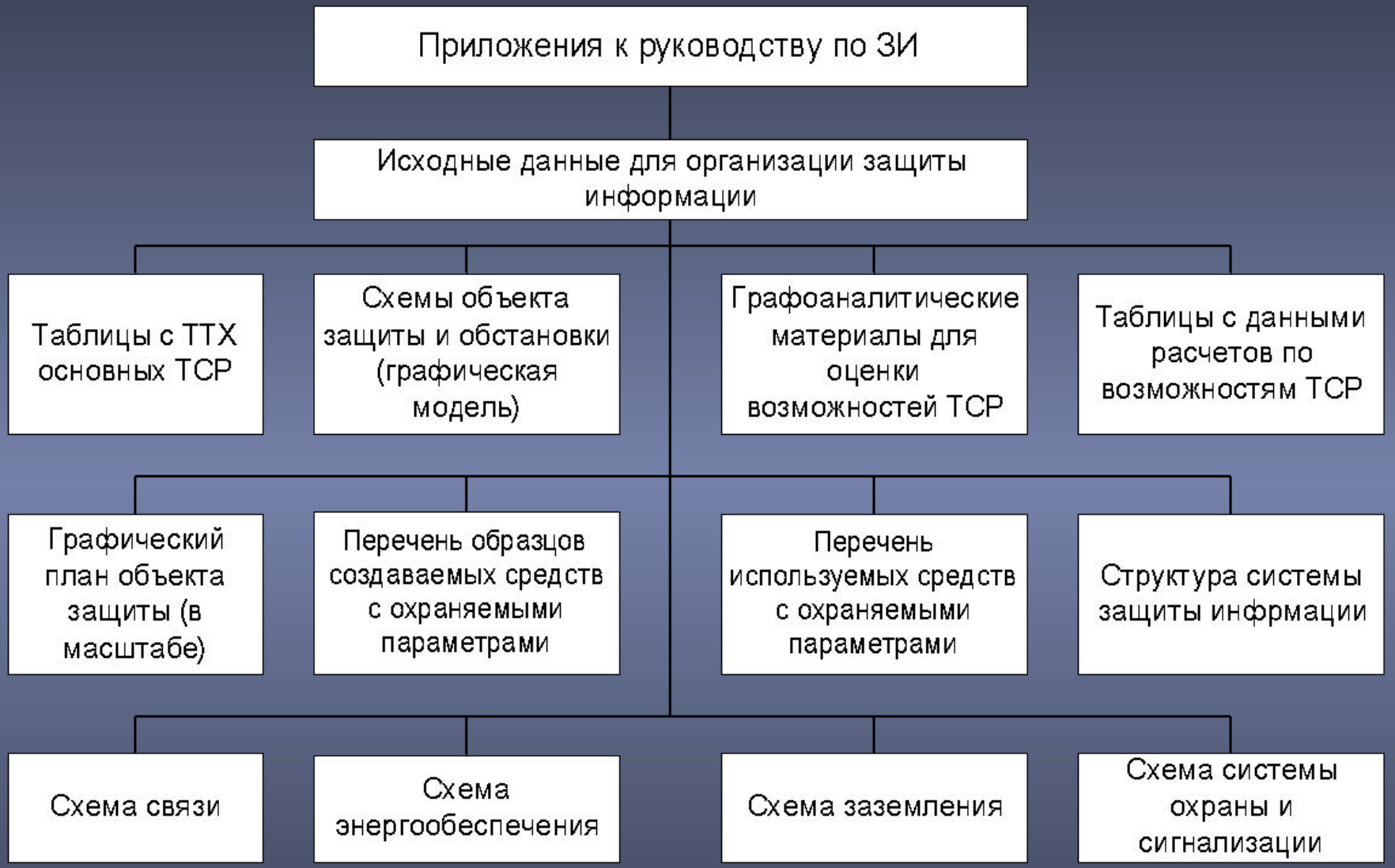
5.Результаты аттестационного и периодического контроля

Дата проведения	Результаты аттестационной или периодической проверки	Номер документа	Подпись проверяющего
10.02.99 г.	Не удовлетворяет требованиям СТР по пп 4.1.1.4. и 4.1.1.6	Протокол № 11567 от 15.02.99 г.	Ларионов В.А.

Решение Гостехкомиссии России №42 от 03.10.1995 года

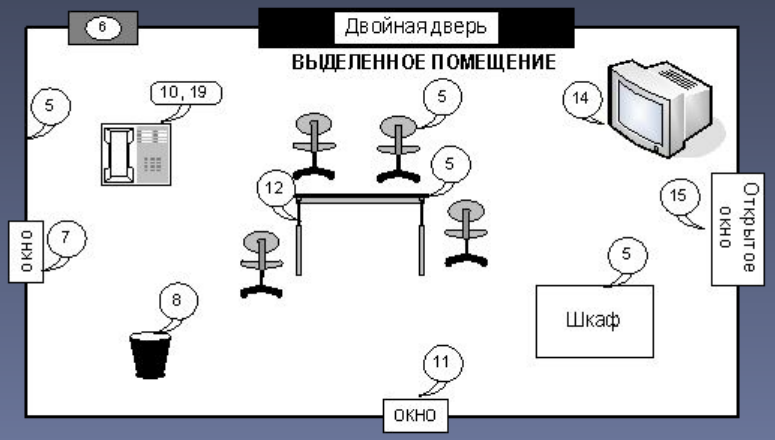
Структура руководства по защите информации

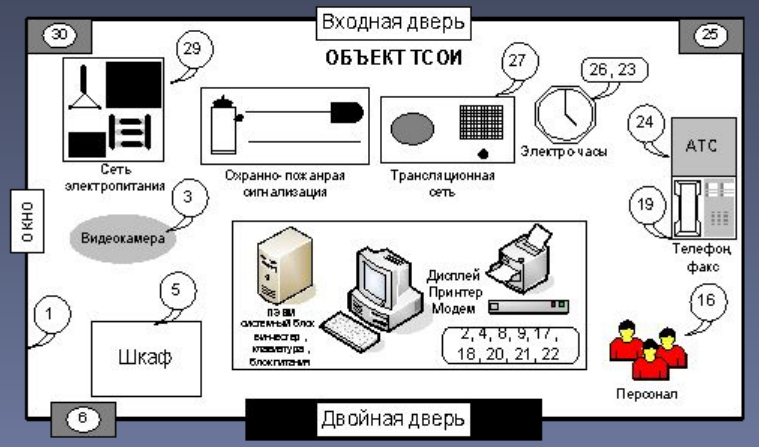
Решение Гостехкомиссии России №42 от 03.10.1995 года



Рекомендуемый состав приложений к руководству по защите информации

ОСНОВНЫЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ





1. Утечка за счет структурного звука в стенах и перекрытиях
2. Съем информации с ленты принтера, плохо стертых дискет и т.п.
3. Съем информации с использование видео - закладок
4. Программно-аппаратные закладки в ПЭВМ
5. Радио -закладки в стенах и мебели
6. Съем информации по системе вентиляции
7. Лазерный съем акустической информации с окон
8. Производственные и технологические отходы
9. Компьютерные вирусы , логические бомбы и т.п.
10. Съем информации за счет наводок и «навязывания»
11. Дистанционный съем видео -информации (оптика)
12. Съем акустической информации с использование диктофонов
13. Хищение носителей информации
14. Высокочастотный канал утечки в бытовой технике
15. Съем информации направленным микрофоном
16. Внутренние каналы утечки информации (через обслуживающий персонал)
17. Несанкционированное копирование
18. Утечка за счет побочного излучения терминала
19. Съем информации за счет использования «телефонного уха»
20. Съем с клавиатуры и принтера по акустическому каналу
21. Съем с дисплея по электромагнитному каналу
22. Визуальный съем с дисплея и принтера
23. Наводки на линии коммуникаций и сторонние проводники
24. Утечка через линии связи
25. Утечка по цепям заземления
26. Утечка по сети электрочасов
27. Утечка по трансляционной сети и ГГС
28. Утечка по охранно-пожарной сигнализации
29. Утечка по сети электропитания
30. Утечка по сети отопления, газо- и водоснабжения

Обобщенная классификация ТКУИ на объектах информатизации

Авторский коллектив

- КВН, профессор Фролов В.Ю.
- КВН полковник Ракицкий С.Н.

СПАСИБО ЗА ВНИМАНИЕ