Государственная система *защиты информации.* Отечественная нормативно-методическая база в области защиты информации

Всё об информации

Понятие «информация» давно стало общенаучной категорией. Известно большое количество различных точек зрения на сущность этого явления. Приведём наиболее распространённые определения:

- любые сведения о каких-либо ранее неизвестных событиях;
- содержательное описание объекта или явления;
- мера разнообразия;
- уменьшаемая неопределённость – энтропия;
- бесконечный законопроцесс триединства энергии, движения и массы с различными плотностями кодовых структур бесконечно-беспредельной Вселенной;
- **сведения о лицах, предметах, событиях, явлениях и процессах (независимо от формы их представления), отраженные на материальных носителях, используемые в целях получения знаний и практических решений.**

Само понятие «информация» обычно предполагает наличие по крайней мере **трёх объектов: источника, потребителя и передающей среды.**

Всё об информации

Наиболее **важными в практическом плане свойствами** информации являются:

- **ценность; достоверность; своевременность.**

Ценность информации определяется обеспечением возможности достижения цели, поставленной перед получателем, *она меняется во времени* .

Достоверность – соответствие полученной информации действительной обстановке.

Своевременность – соответствие ценности и достоверности определённому временному периоду.

Информация может быть получена: проведением научных исследований, покупкой или *противоправным добыванием*

Классификация информации по её доступности:

- *общедоступная информация;*
- *информация, доступ к которой может быть ограничен;*
- *информация с ограниченным доступом;*
- *информация, не подлежащая распространению.*

Информационная безопасность

ИБ – состояние защищённости информационной среды общества, обеспечивающее её формирование и развитие в интересах граждан, организаций и государства.

«Безопасность есть предотвращение зла» (Платон).

1.Информация становится атрибутом, от которого зависит эффективность жизнедеятельности.

2.Общество становится более открытым, что создаёт благоприятную обстановку для злоумышленников в плане доступа к информации, в т.ч. Конфиденциальной.

3.Всеобщая информатизация и компьютеризация привела к появлению нетрадиционных каналов утечки информации и НСД.

Пять выводов:

1.Проблема ИБ будет носить перманентный характер.

2.Обеспечение ИБ должно носить комплексный характер.

3.Необходимы усилия профессионалов + руководителей и специалистов.

4.Проблемы ЗИ связаны с правовым регулированием информатизации.

5.Эффективное решение проблем ИБ требует подготовки и переподготовки кадров.

Тезисы

1. Проблема ИБ сегодня стала затрагивать каждого гражданина(Швеция процесс-150 рускоязычных электронных мошеников, в США потери в 2007 г. – $ 240 мил., слушания в парламенте Брюссель – система«Эшалон» (США, Англия, Канада, Австралия – промышленный шпионаж, слежка за госслужащими, в Англии – 30000 видиокамер, Ростов – безопасный город, операторы хранят данные о перемещении абонентов, данные о Ваших покупках в Интернет).
2. Проблема ИБ становится для человечества очень дорогостоящей, съедающей сотни миллиардов $. (Администрация США в 2009 г. выделяет $376 мил.на обеспечение кибербезопасности. Вирусы «Мелисса» и «Черноболь» заразили сотни тысяч компьютеров – ущерб сотни миллионов долларов).
3. Преступность в информационной сфере растёт (1,4 млн. хакерских атак на информационные ресурсы федеральных органов власти зафиксировала и отразила Федеральная служба безопасности в 2007 году. Из них более 100 тысяч пришлось на сайт президента РФ. 140 уголовных дел/28.
4. Мир вступает в эпоху информационных войн

Информационно-справочная система по документам в области технической защиты информации

- **Правовые документы по технической защите информации**
  - Конституция Российской Федерации
  - Федеральные законы (Законы Российской Федерации)
  - Указы и распоряжения Президента Российской Федерации
  - Постановления Правительства Российской Федерации
- **Организационно-распорядительные документы по технической защите информации**
  - Концепции
  - Положения
- **Специальные нормативные документы по технической защите информации**
  - Государственные стандарты
  - Специальные нормативные документы
- **Документы по лицензированию, сертификации и аттестации в области технической защиты информации**
  - Документы

Правовые документы по технической защите информации

- Федеральные законы (Закон «О государственной тайне»)
- Указы и распоряжения Президента Российской Федерации (Указ «О перечне сведений отнесенных к государственной тайне)
- Постановления Правительства Российской Федерации

  (Постановление о подготовке к передаче сведений, составляющих гостайну, другим государствам)
- Конституция Российской Федерации

Организационно-распорядительные документы по технической защите информации

Положения

Концепции

Концепция национальной безопасности РФ

Указ президента №24 от 10.01.2000

1. Россия в мировом пространстве
2. Национальные интересы России
3. Угрозы национальной безопасности РФ
4. Обеспечение национальной безопасности РФ

Доктрина информационной безопасности

УТВЕРЖДЕНА 9 сентября 2000 г.

Раздел 6. Особенности обеспечения ИБ РФ в различных сферах общественной жизни

1.В сфере экономики
2.В сфере внутренней политики
3.В сфере внешней политики
4.В сфере обороны
5.В области науки и техники
6.В духовной жизни
7.В общегосударственных ИТС
8.В правоохранительной и судебных сферах
9.В условиях чрезвычайных ситуаций

Объекты обеспечения ИБ, угрозы ИБ, мероприятия по обеспечению ИБ

Доктрина ИБ в области науки и техники

- **Объекты:** результаты фундаментальных, поисковых и прикладных исследований важные для н-т, технологического, утрата которых может нанести ущерб для РФ.
- **Угрозы:** внешние – НСД иностранных государств к н-т ресурсам, переориентация на Запад перспективные научные коллективы, промышленный шпионаж; внутренние – сложная экономическая ситуация, слабая микроэлектронная база, проблемы в области патентной защиты результатов, сложности в ЗИ.
- **Противодействие угрозам** – совершенствование законодательства, рекомендации по предотвращению противоправного или неэффективного использования интеллектуального потенциала России

Источники конфиденциальности в ИС

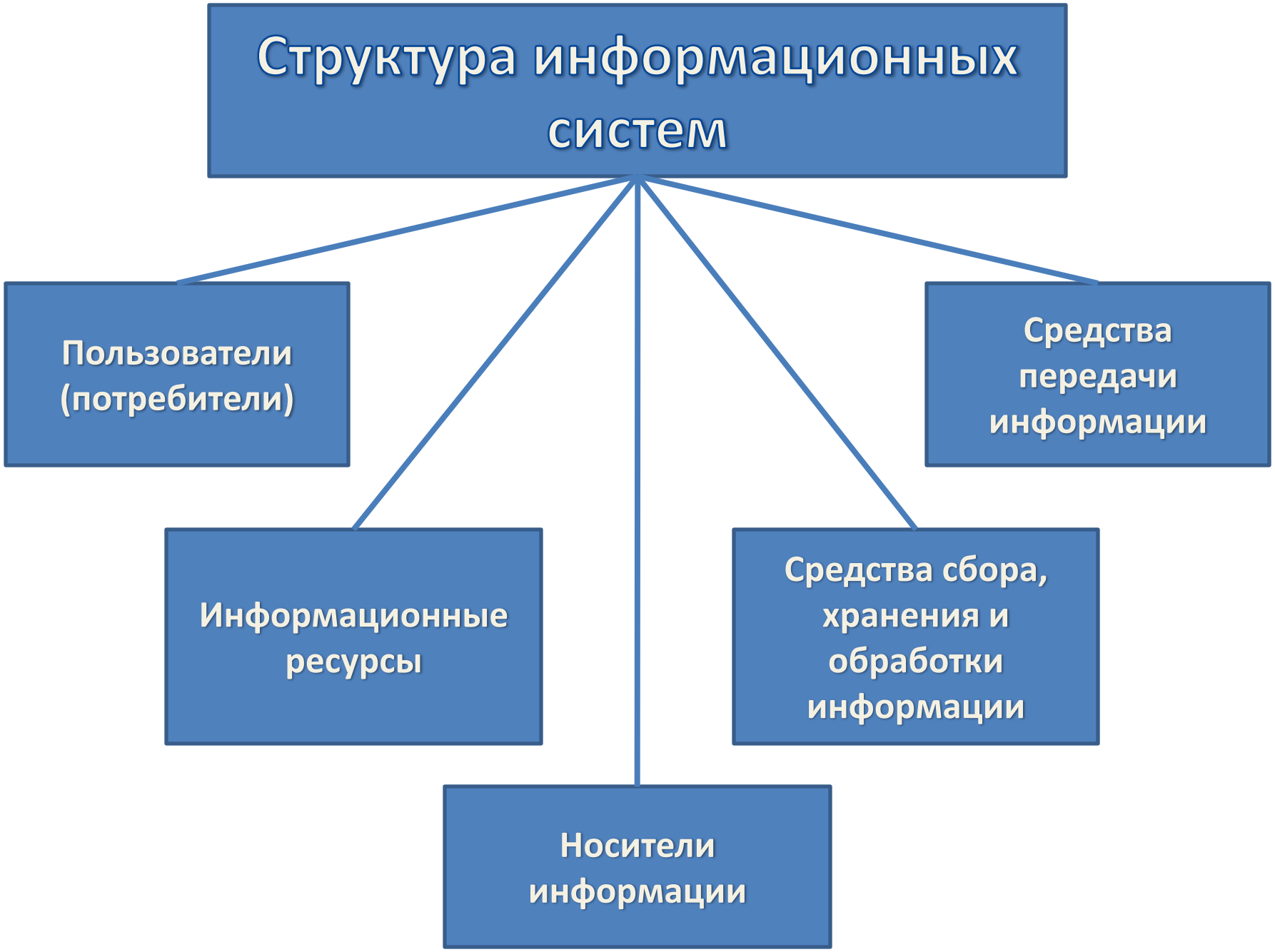
1. Люди – главные активные элементы. «Кто владеет информацией, тот владеет миром» , «Информация это – власть»
2. Документы – самая распространенная форма обмена информацией
3. Публикации – книги, статьи, отчеты, диссертации – 60% военной информации (секретов) есть в «открытых» источниках. В промышленности до 90%. Цель шпиона найти 10% !!!
4. Технические носители – колоссальные объемы информации !!
5. ТСОИ (Технические средства обработки информации)

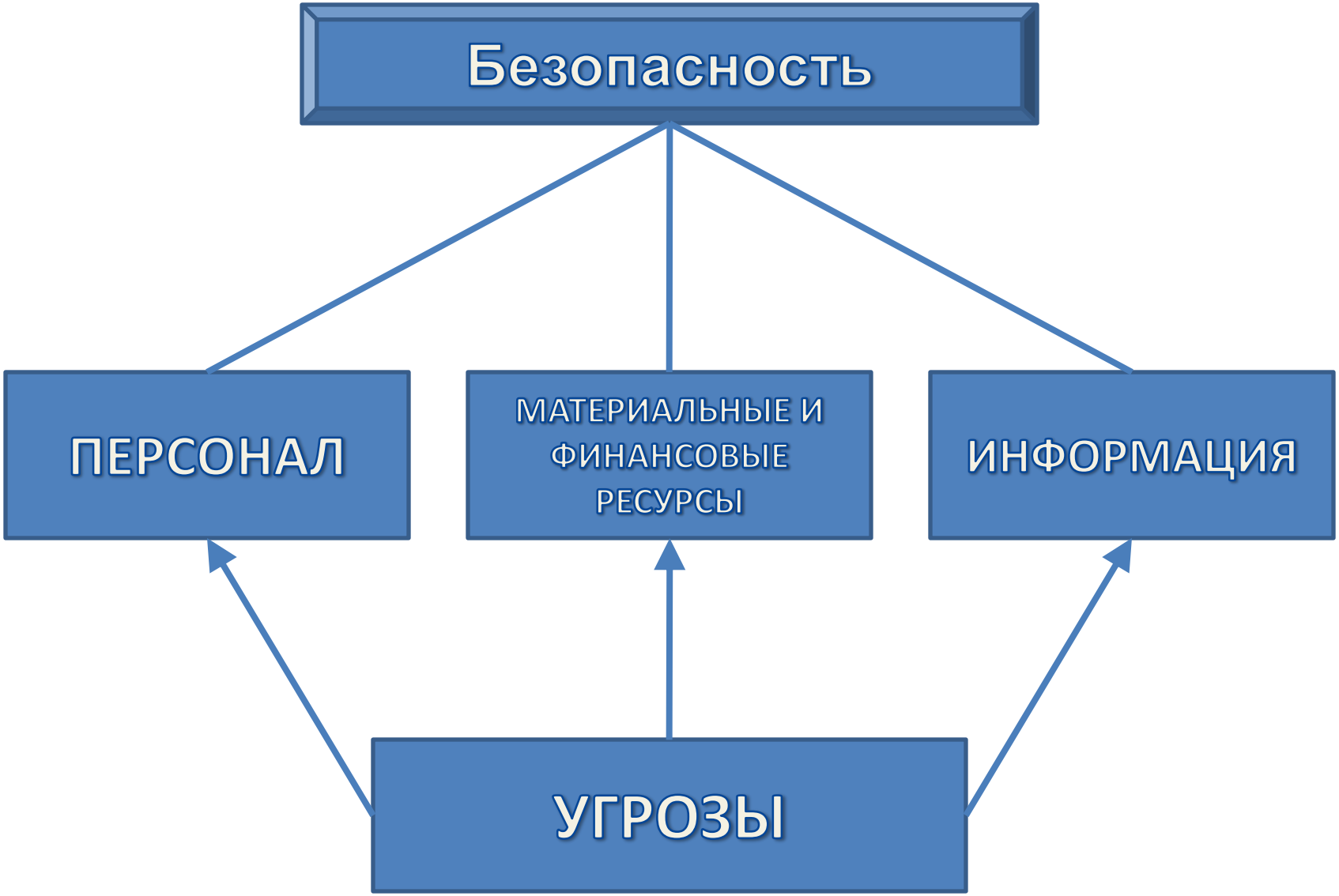
   ТС – основные, обеспечивающие обработку информации – ИС

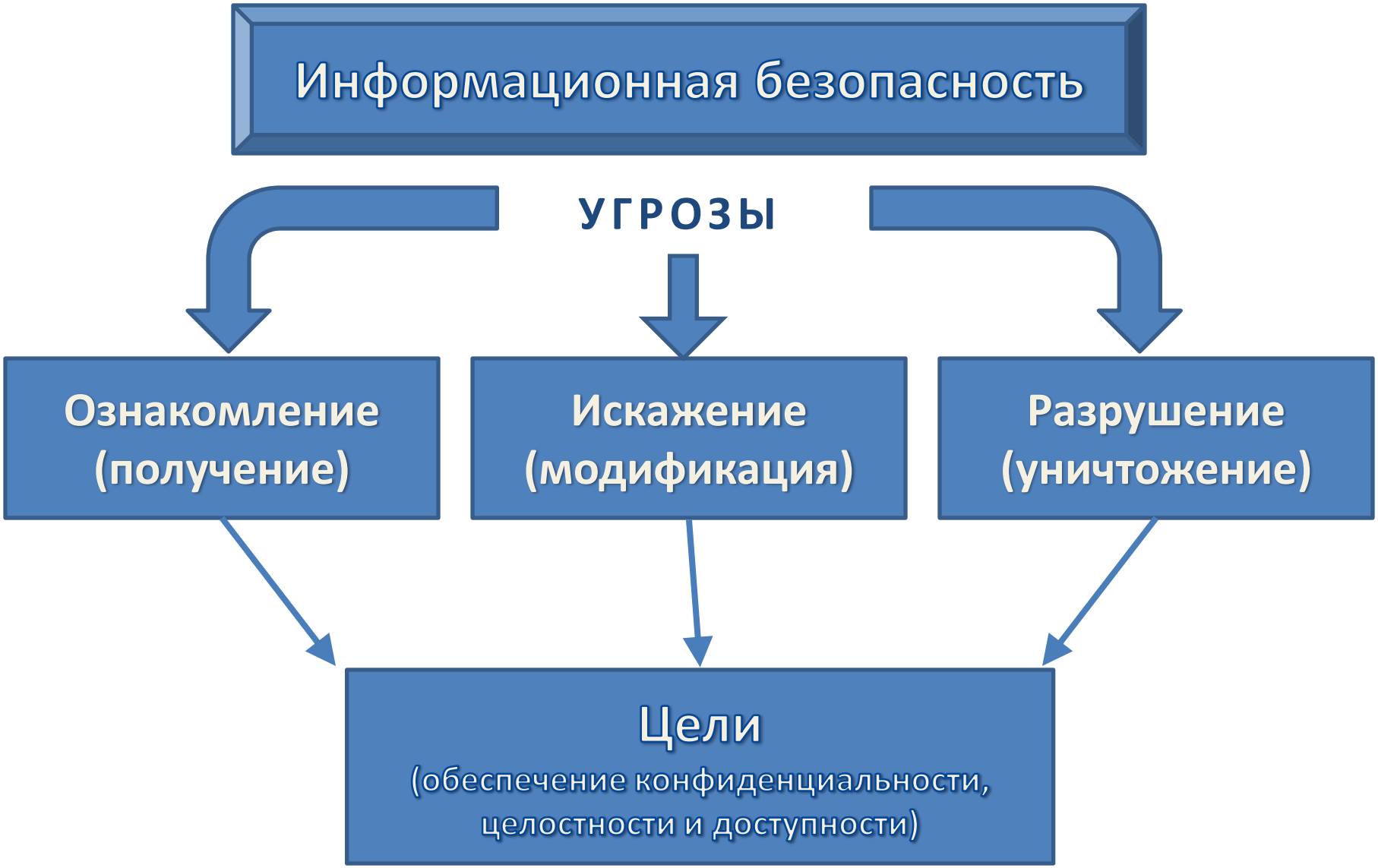
   ТС – вспомогательные (телефоны, радиосвязь, телевидение, ксероксы, принтеры.

Что такое ИС?

Информационная Система (ИС) или АС – это организационно упорядоченная совокупность информационных ресурсов, технических средств, технологий, реализующих информационные процессы в традиционном или автоматизированном режиме для удовлетворения информационных потребностей пользователя

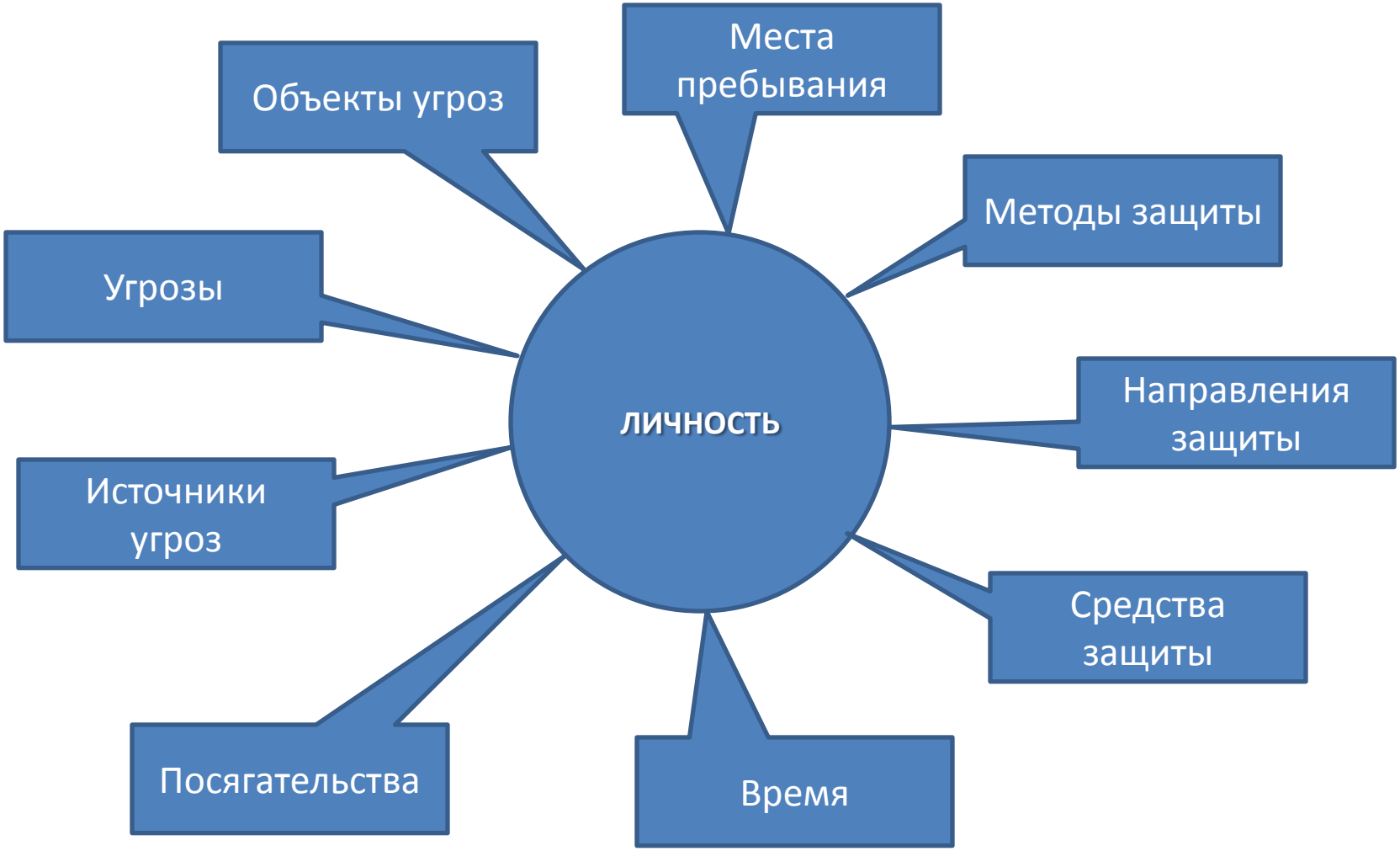

Структура информационных систем
Пользователи (потребители)
Информационные ресурсы
Носители информации
Средства сбора, хранения и обработки информации
Средства передачи информации


Безопасность
ПЕРСОНАЛ
МАТЕРИАЛЬНЫЕ И ФИНАНСОВЫЕ РЕСУРСЫ
ИНФОРМАЦИЯ
УГРОЗЫ


Информационная безопасность
УГРОЗЫ
Ознакомление (получение)
Искажение (модификация)
Разрушение (уничтожение)
Цели
(обеспечение конфиденциальности, целостности и доступности)

Концептуальная модель безопасности информации

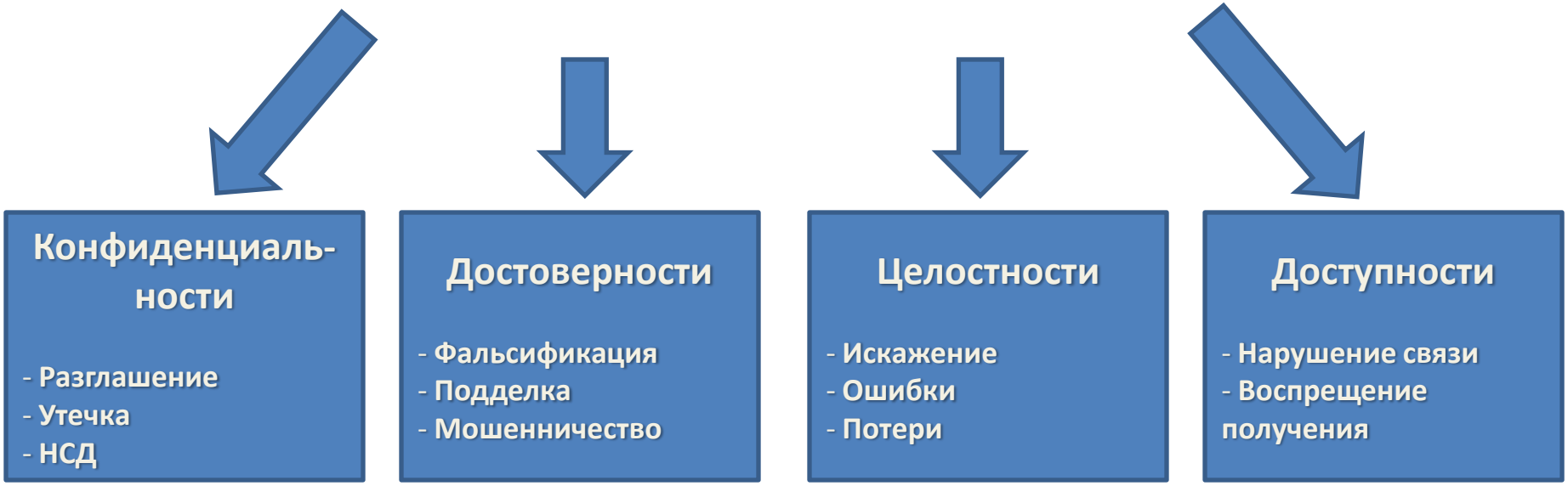
Концептуальная модель безопасности личности

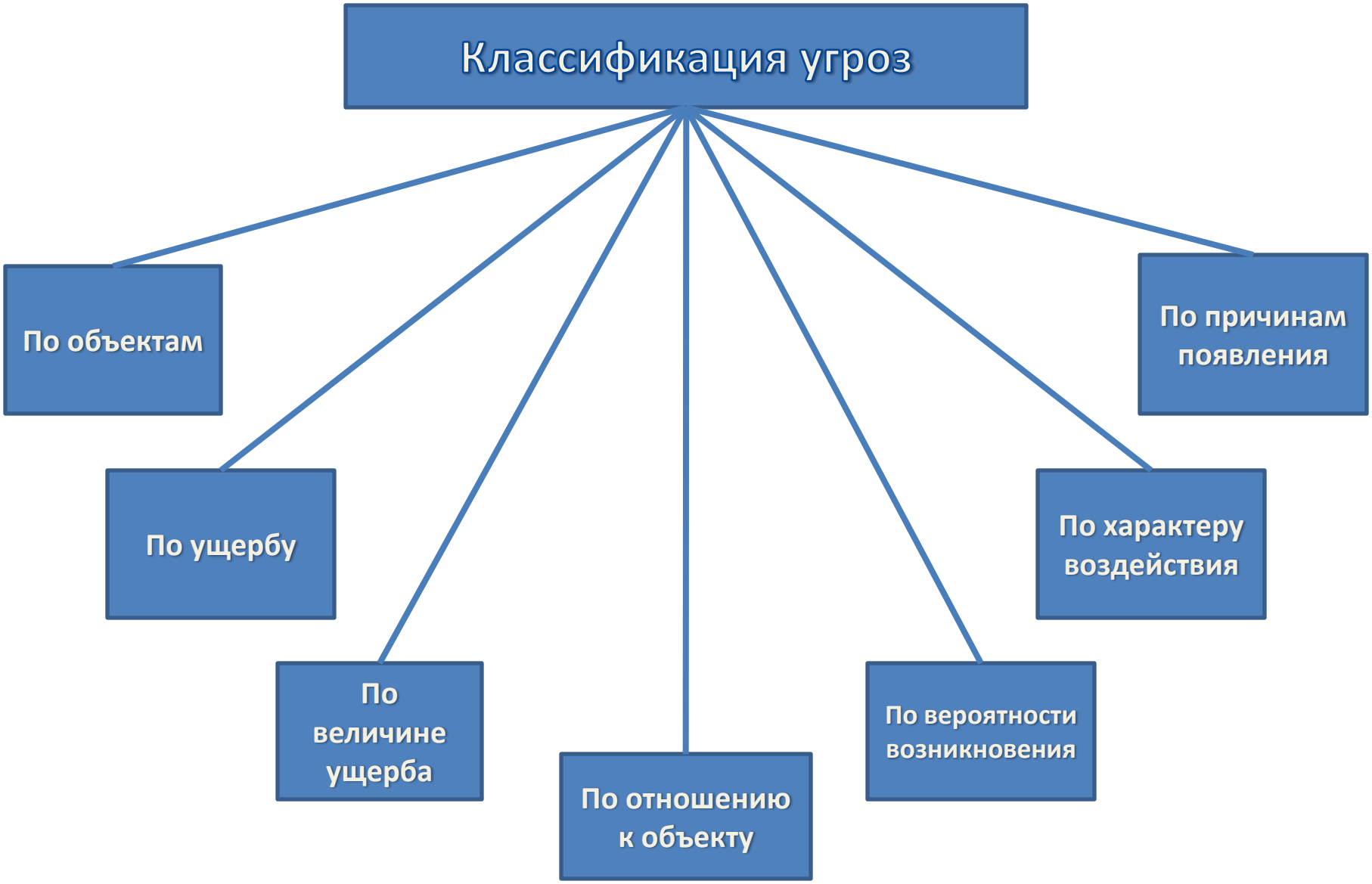


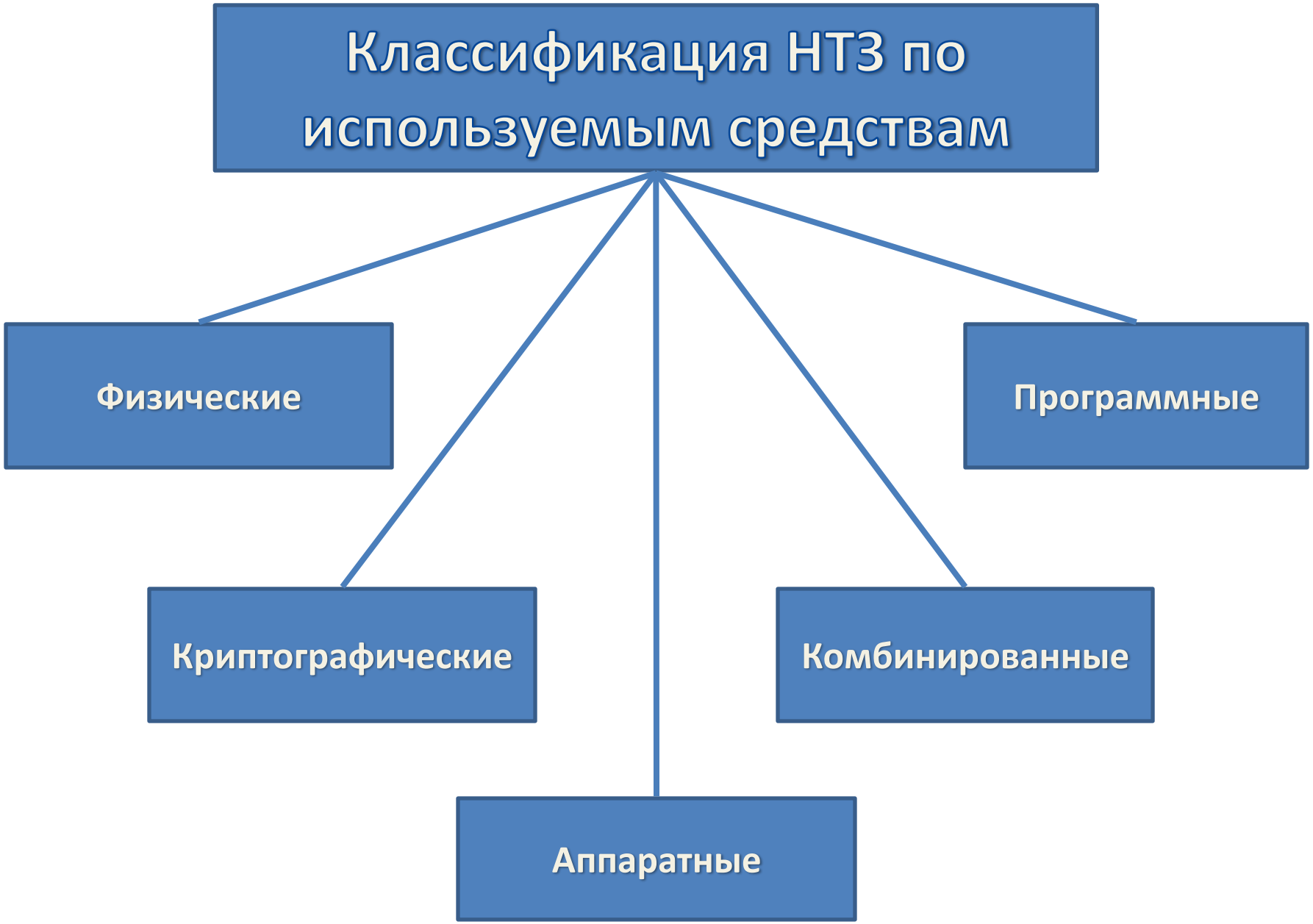
Концептуальная модель безопасности продукции

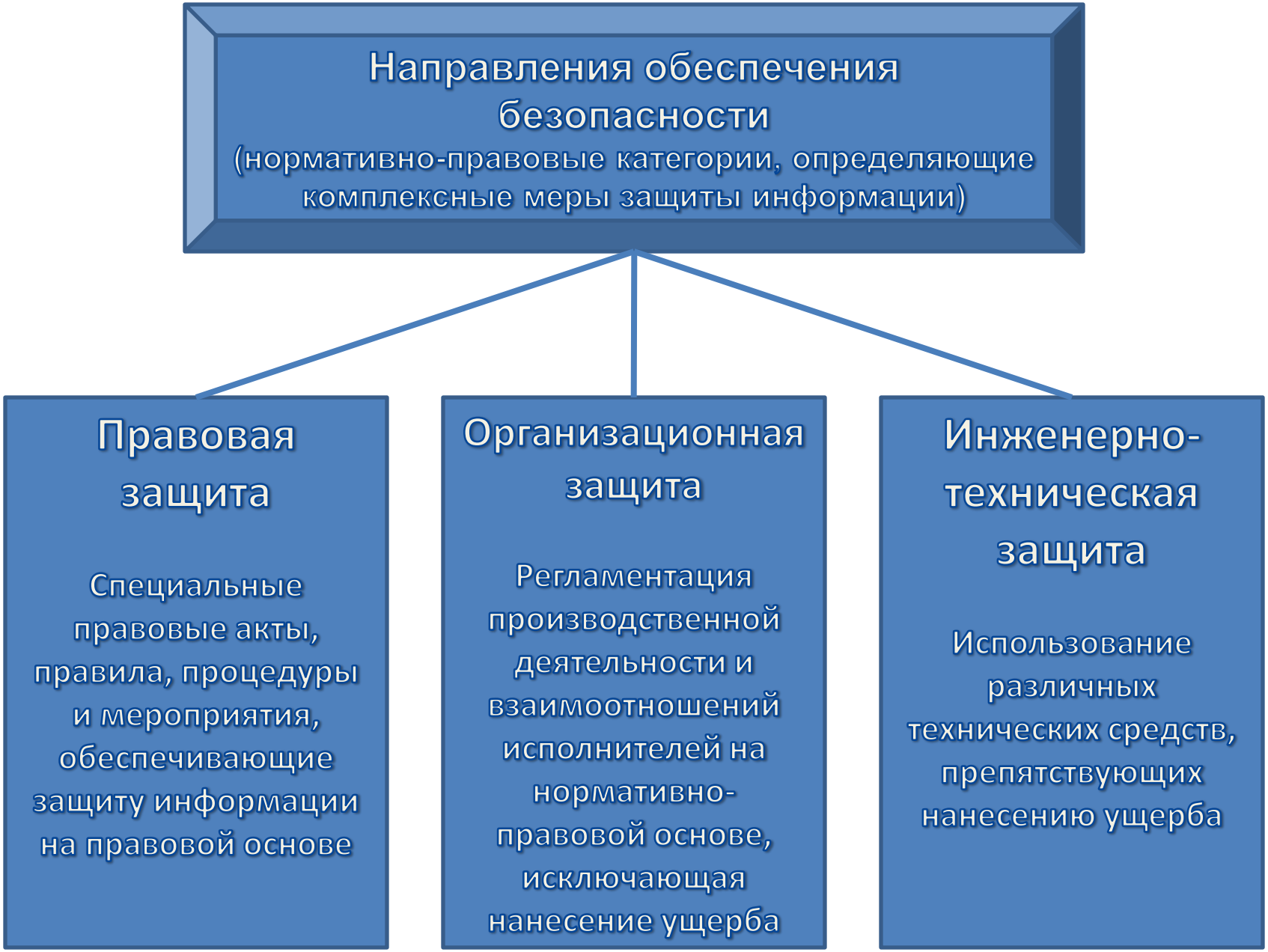
Угрозы информации

Проявляются в нарушении




Классификация угроз
По объектам
По ущербу
По величине ущерба
По отношению к объекту
По вероятности возникновения
По характеру воздействия
По причинам появления


Классификация НТЗ по используемым средствам
Физические
Программные
Криптографические
Комбинированные
Аппаратные


Направления обеспечения безопасности
(нормативно-правовые категории, определяющие комплексные меры защиты информации)
Правовая защита
Специальные правовые акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе
Организационная защита
Регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая нанесение ущерба
Инженерно-техническая защита
Использование различных технических средств, препятствующих нанесению ущерба

Специальные нормативные документы по технической защите информации

Государственные стандарты

Специальные нормативные документы

ГОСУДАРСТВЕННЫЕ СТАНДАРТЫ

ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России

ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Госстандарт России

ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России

ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России

ГОСТ Р ИСО 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Госстандарт России

ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Госстандарт России

ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Ведение и общая модель. Госстандарт России

ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России

ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России

Специальные нормативные документы

Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации	Решение председателя Гостехкомиссии России от 30 марта 1992 года
Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации	Решение председателя Гостехкомиссии России от 30 марта 1992 года
Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации	Решение председателя Гостехкомиссии России от 30 марта 1992 года
Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники	Решение председателя Гостехкомиссии России от 30 марта 1992 года
Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации	Решение председателя Гостехкомиссии России от 25 июля 1997 года
Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей	Приказ председателя Гостехкомиссии России от 4 июня 1999 года № 114
Руководство по разработке профилей защиты и заданий по безопасности	Гостехкомиссия России, 2003 год

Классификация АС

1.1. Классификация распространяется на все действующие и проектируемые АС учреждений, организаций и предприятий, обрабатывающие конфиденциальную информацию.

1.2. Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации .

Необходимыми **исходными данными для проведения классификации** конкретной АС являются:

- перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
- перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
- матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
- режим обработки данных в АС.

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС - коллективный или индивидуальный.

Классификация АС

Устанавливается **девять классов защищенности АС от НСД к информации**.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на **три группы**, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

- **Третья группа** включает АС, в которых работает **один пользователь**, допущенный ко всей информации АС, размещенной на носителях **одного уровня конфиденциальности**. Группа содержит два класса - 3Б и 3А.
- **Вторая группа** включает АС, в которых **пользователи имеют одинаковые права доступа (полномочия) ко всей информации** АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.
- **Первая группа включает многопользовательские АС**, в которых **одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности**. **Не все пользователи имеют право доступа ко всей информации АС.** Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

Требования по защите информации от НСД для АС

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих **четырех подсистем:**

- **управления доступом;**
- **регистрации и учета;**
- **криптографической;**
- **обеспечения целостности.**

Требования к АС третьей группы

Подсистемы и требования	Классы	
	3Б	3А
1. **Подсистема управления доступом**		
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:		
в систему	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	-
к программам	-	-
к томам, каталогам, файлам, записям, полям записей	-	-
1.2. Управление потоками информации		
2. **Подсистема регистрации и учета**		
2.1. Регистрация и учет:		
входа (выхода) субъектов доступа в (из) систему(ы) (узел сети)	+	+
выдачи печатных (графических) выходных документов	-	+
запуска (завершения) программ и процессов (заданий, задач)	-	-
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	-
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	-
изменения полномочий субъектов доступа	-	-
создаваемых защищаемых объектов доступа	-	-
2.2. Учет носителей информации	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+
2.4. Сигнализация попыток нарушения защиты	-	-
3. **Криптографическая подсистема**		
3.1. Шифрование конфиденциальной информации	-	-
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-
3.3. Использование аттестованных (сертифицированных) криптографических средств	-	-
4. **Подсистема обеспечения целостности**		
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+
4.3. Наличие администратора (службы) защиты информации в АС	-	-
4.4. Периодическое тестирование СЗИ НСД	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+
4.6. Использование сертифицированных средств защиты	-	+

Требования к показателям защищённости

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа	+	+	+	=	+	=
Мандатный принцип контроля доступа	-	-	+	=	=	=
Очистка памяти	-	+	+	+	=	=
Изоляция модулей	-	-	+	=	+	=
Маркировка документов	-	-	+	=	=	=
Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+	=	=	=
Сопоставление пользователя с устройством	-	-	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гарантии проектирования	-	+	+	+	+	+
Регистрация	-	+	+	+	=	=
Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
Надежное восстановление	-	-	-	+	=	=
Целостность КСЗ	-	+	+	+	=	=
Контроль модификации	-	-	-	-	+	=
Контроль дистрибуции	-	-	-	-	+	=
Гарантии архитектуры	-	-	-	-	-	+
Тестирование	+	+	+	+	+	=
Руководство для пользователя	+	=	=	=	=	=
Руководство по КСЗ	+	+	=	+	+	=
Тестовая документация	+	+	+	+	+	=
Конструкторская (проектная) документация	+	+	+	+	+	+

Межсетевые экраны

МЭ представляет собой локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Устанавливается **пять классов защищенности МЭ.**

Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации.

Самый **низкий класс защищенности - пятый,** применяемый для безопасного взаимодействия **АС класса 1Д с внешней средой, четвертый - для 1Г, третий - 1В, второй - 1Б, самый высокий - первый, применяемый для безопасного взаимодействия АС класса 1А с внешней средой.**

При включении МЭ в АС определенного класса защищенности, **класс защищенности совокупной АС, полученной из исходной путем добавления в нее МЭ, не должен понижаться.**

Для АС класса 3Б, 2Б должны применяться МЭ не ниже 5 класса.

Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов:

при обработке информации с грифом **“секретно” - не ниже 3 класса;**

при обработке информации с грифом **“совершенно секретно” - не ниже 2 класса;**

при обработке информации с грифом **“особой важности” - не ниже 1 класса.**

Требования к межсетевым экранам

Показатели защищенности	Классы защищенности				
	5	4	3	2	1
Управление доступом (фильтрация данных и трансляция адресов)	+	+	+	+	=
Идентификация и аутентификация	-	-	+	=	+
Регистрация	-	+	+	+	=
Администрирование: идентификация и аутентификация	+	=	+	+	+
Администрирование: регистрация	+	+	+	=	=
Администрирование: простота использования	-	-	+	=	+
Целостность	+	=	+	+	+
Восстановление	+	=	=	+	+
Тестирование	+	+	+	+	+
Руководство администратора защиты	+	=	=	=	=
Тестовая документация	+	+	+	+	+
Конструкторская (проектная) документация	+	=	+	=	+

Руководящий документ
Защита от несанкционированного доступа к информации
Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей

Настоящий Руководящий документ (РД) устанавливает классификацию программного обеспечения (ПО) (как отечественного, так и импортного производства) средств защиты информации (СЗИ), в том числе и встроенных в общесистемное и прикладное ПО, по уровню контроля отсутствия в нем недекларированных возможностей.

Уровень контроля определяется выполнением заданного настоящим РД набора требований, предъявляемого:

к составу и содержанию документации, представляемой заявителем для проведения испытаний ПО СЗИ;

к содержанию испытаний.

Документ предназначен для специалистов испытательных лабораторий, заказчиков, разработчиков ПО СЗИ при его контроле в части отсутствия недекларированных возможностей.

Общие положения

1.1. *Классификация* распространяется на ПО, предназначенное для защиты информации ограниченного доступа.

1.2. Устанавливается ***четыре уровня контроля*** **отсутствия недекларированных возможностей.** Каждый уровень характеризуется определенной минимальной совокупностью требований.

1.3. Для ПО, используемого при защите информации, **отнесенной к государственной тайне**, должен быть обеспечен уровень контроля не **ниже третьего.**

1.4. Самый высокий уровень контроля - ***первый***, достаточен для ПО, используемого при защите информации с грифом **«ОВ».**

Второй уровень контроля достаточен для ПО, используемого при защите информации с грифом **«СС».**

Третий уровень контроля достаточен для ПО, используемого при защите информации с грифом **«С».**

1.5 Самый низкий уровень контроля - ***четвертый***, достаточен для ПО, используемого при защите **конфиденциальной** информации .

Лицензирование и сертификация в области защиты информации

- Положение о государственном лицензировании деятельности в области ЗИ устанавливает принципы, организационную структуру системы государственного лицензирования деятельности юридических лиц – предприятий, а также порядок лицензирования и контроля.
- Система государственного лицензирования предприятий в области ЗИ является составной частью государственной системы защиты информации. Она реализуется через ФСТЭК и ФСБ.
- Лицензия выдается на конкретные виды деятельности на срок три года.
- Лицензия выдается за плату.
- Положение о сертификации СЗИ по требованиям БИ устанавливает основные принципы, организационную структуру и порядок сертификации СЗИ, а также госконтроль. Под СЗИ понимаются технические, криптографические, программные и др. средства. Под сертификацией СЗИ понимается деятельность по подтверждением их требованиям стандартам и др. нормативным документам по ЗИ.