Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа

Целью реализации программы повышения квалификации является совершенствование и (или) получение новых компетенций, необходимых для осуществления профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации специалистов (включая государственных гражданских служащих), работающих в области технической защиты информации (ТЗИ) (далее − обучающиеся), в частности разработки и применения способов и средств защиты информации от несанкционированного доступа (НСД).

Объектами профессиональной деятельности обучающихся являются:

- объекты информатизации, включающие автоматизированные (информационные) системы различного уровня и назначения, средства и системы обработки информации и средства их обеспечения;
- угрозы безопасности информации в автоматизированных (информационных) системах;
- способы и средства ТЗИ;
- система нормативных правовых актов, методических документов и национальных стандартов в области ТЗИ.

Задачами профессиональной деятельности обучающихся являются:

а) в проектной деятельности:

- определение угроз безопасности информации в автоматизированных (информационных) системах;
- формирование требований к обеспечению ТЗИ от НСД на объектах информатизации (формирование требований к системе защиты информации объекта информатизации);
- разработка способов и средств для обеспечения ТЗИ от НСД на объектах информатизации (разработка системы защиты информации объектов информатизации);
- внедрение способов и средств для обеспечения ТЗИ от НСД на объектах информатизации (внедрение системы защиты информации на объектах информатизации);

б) в эксплуатационной деятельности:

- обеспечение ТЗИ от НСД в ходе эксплуатации объектов информатизации;
- обеспечение ТЗИ от НСД при выводе из эксплуатации объектов информатизации.

МОДУЛЬ 1. ОРГАНИЗАЦИЯ РАБОТ ПО ТЗИ
РАЗДЕЛ 1.1. ЦЕЛИ И ЗАДАЧИ ТЗИ.

Задачи технической защиты информации – задачи противоборства органов и специалистов по информационной безопасности, с одной стороны, и злоумышленников, с другой стороны.

Данные задачи являются слабоформализуемыми – т.к. не имеют формальных методов решения, и основу методологии их решения составляют системный подход и системный анализ.

Термины и определения

Техническое средство обработки информации (ТСОИ) – техническое средство, предназначенное для приема, хранения, поиска, преобразования, отображения и (или) передачи информации по каналам связи. К ТСОИ относятся средства вычислительной техники, средства и системы связи, средства звукозаписи, звукоусиления и звуковоспроизведения, средства видеозаписи и видеовоспроизведения, средства изготовления и размножения документов и другие технические средства, связанные с приемом, накоплением, хранением, поиском, преобразованием, отображением и (или) передачей информации по каналам связи.

Основные технические средства обработки информации (ОТС) – средства вычислительной техники и их коммуникации, входящие в состав объекта информатизации и осуществляющие обработку, хранение и передачу важной информации.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для обработки важной информации, но на которые могут воздействовать электромагнитные поля побочных излучений основных технических средств, в результате чего на ВТСС наводится опасный сигнал, который может распространяться за пределы контролируемой зоны. К ВТСС относятся средства и системы связи, измерительное оборудование, системы пожарной и охранной сигнализации, системы электрочасофикации, системы радиотрансляции, системы электроосвещения, бытовые электроприборы и т.д. ВТСС играют роль “случайных антенн”.

Термины и определения.

Техническая разведка – деятельность по получению важной (защищаемой) информации с помощью технических средств.

Средство технической разведки – аппаратура технической разведки, размещенная на стационарном или мобильном объекте (помещении, транспортном средстве и т.д.), и обслуживаемая соответствующим персоналом.

Аппаратура технической разведки – совокупность технических устройств, предназначенных для обнаружения, приема (перехвата), регистрации и обработки сигналов, содержащих важную (защищаемую) информацию.

Возможности технической разведки – характеристики способности обнаружения, распознавания, приема и регистрации информативных сигналов (ПЭМИН) средствами технической разведки.

Зона разведдоступности – пространство вокруг объекта, в пределах которого реализуются возможности технической разведки.

Модель технической разведки – описание средств технической разведки, содержащее их технические характеристики и тактику применения в объеме, достаточном для оценки возможностей технической разведки.

Информативный (опасный) сигнал – электрические или электромагнитные сигналы и поля, по параметрам которых может быть раскрыта информация, обрабатываемая с помощью технических средств.

ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Реализация конституционных прав и свобод акционеров в сфере информационной деятельности по защите персональных данных, банковской тайны и других норм финансовых регуляторов в части информационной безопасности кредитных организаций и мер контроля защищенности, содействие в обеспечении защищенности акционеров и клиентов, контрагентов, поставщиков продуктов и услуг, информирование о факторах рисков информационной безопасности и возможным мерам противодействия

Формирование и реализация требований соблюдения государственной тайны и, в соответствии с потребностями и возможностями, по режиму коммерческой тайны

Выявление угроз в информационной сфере и защита информации от несанкционированного доступа, выбор мер противодействия угрозам в информационной сфере и использования средств контроля (защитных мер) в технологических процессах, планирование, реализация и контроль использования защитных мер информационной безопасности, прогнозирование развития событий на основе мониторинга и менеджмента инцидентов информационной безопасности

Совершенствование и защита информационной инфраструктуры предприятия, содействие в обеспечении защищенности реализуемых технологических процессов и предоставляемых продуктов и услуг

Своевременное информирование руководства и акционеров по состоянию информационной безопасности, согласование с руководством планов и стратегий развития и совершенствования обеспечения информационной безопасности

Координация всех видов деятельности в целях обеспечения информационной безопасности, в том числе и через инициирование/согласование/принятие внутренних документов информационной безопасности, реализацию программ по осведомленности и обучению персонала

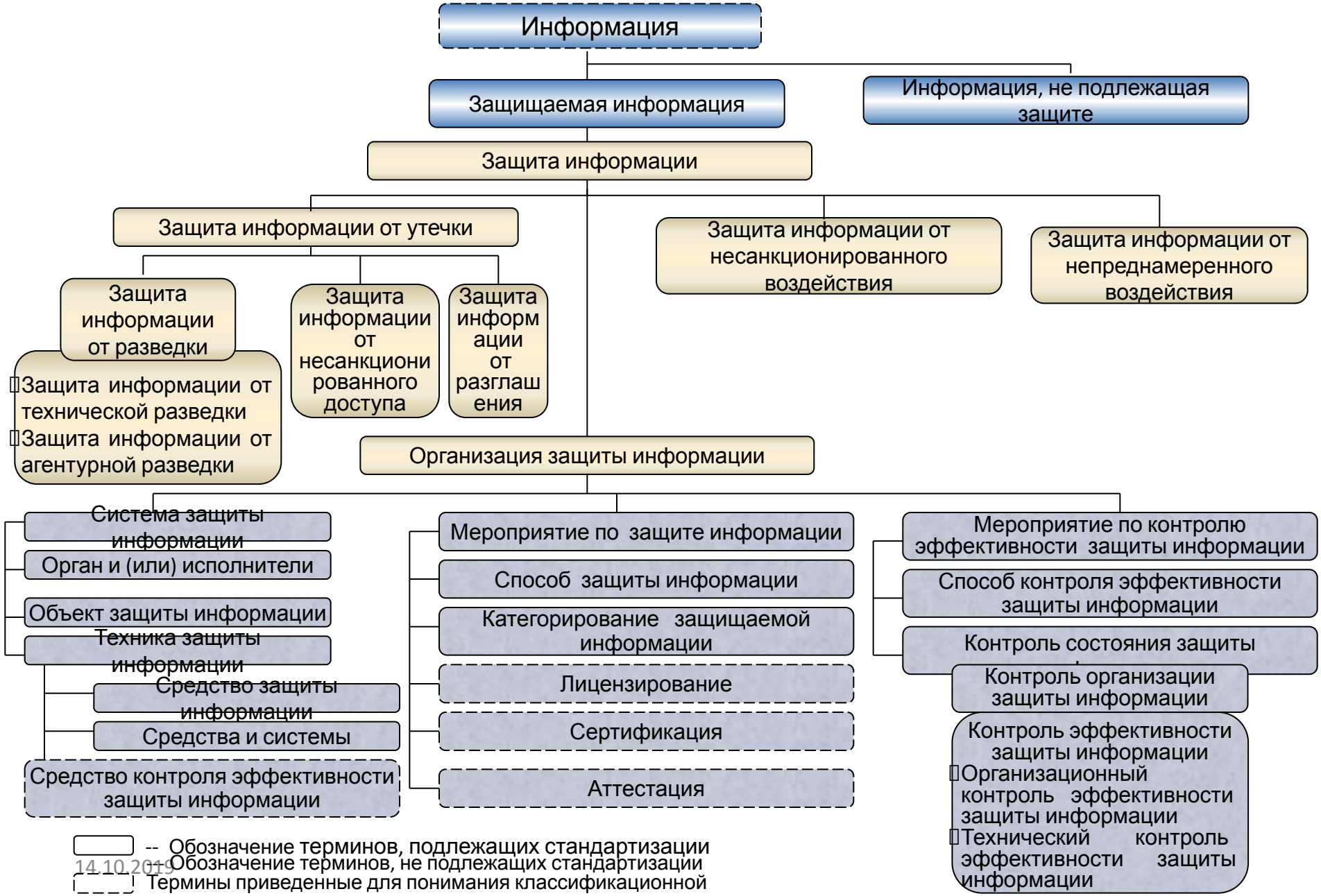
Содействие минимизации ущерба и быстрейшему восстановлению деятельности пострадавших в результате кризисных ситуаций в информационной сфере, участие в расследовании причин возникновения таких ситуаций и принятие соответствующих мер по их предотвращению

Сущность системного подхода

Системный подход - это исследование объекта или процесса с помощью модели, называемой системой:

- совокупность сил и средств, обеспечивающих решение задачи, представляется в виде модели, называемой системой;
- система описывается совокупностью параметров;
- любая система рассматривается как подсистема более сложной системы, влияющей на структуру и функционирование рассматриваемой;
- любая система имеет иерархическую структуру;
- при анализе системы необходим учет внешних и внутренних влияющих факторов;
- свойства системы превышают сумму свойств ее элементов.

Классификационная схема понятий предметной области «Защита информации»



Принципы организации ТЗИ

- **Принцип системности** предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ИТКС.
- **Принцип комплексности** предполагает согласованное применение разнородных средств при построении целостной системы защиты.
- **Принцип непрерывности** предполагает, что защита информации - это непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер в ходе всего рассматриваемого периода защиты информации.
- **Разумная достаточность** предполагает то, что важно правильно выбрать тот достаточный уровень зашиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.
- **Принцип гибкости** системы защиты направлен на обеспечение возможности варьирования уровнем защищенности.
- **Принцип открытости алгоритмов и механизмов защиты** предполагает, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. При этом знание алгоритмов работы системы защиты не должно давать возможности ее преодоления.

Понятие системы защиты информации на объекте информатизации

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА - комплекс организационных мер и программных, физических, аппаратных, программно-аппаратных средств защиты от несанкционированного доступа к информации в автоматизированных системах.

Понятие системы защиты информации на объекте информатизации (продолжение)

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ - совокупность органов и/или исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно - распорядительными и нормативными документами в области защиты информации. ГОСТ Р 50922-96. Защита информации. Основные термины и определения

Основная цель защиты информации – обеспечение заданного уровня ее безопасности

Заданный уровень **безопасности информации** – такое состояние защищенности информации от угроз, при котором обеспечивается допустимый риск ее уничтожения, изменения и хищения.

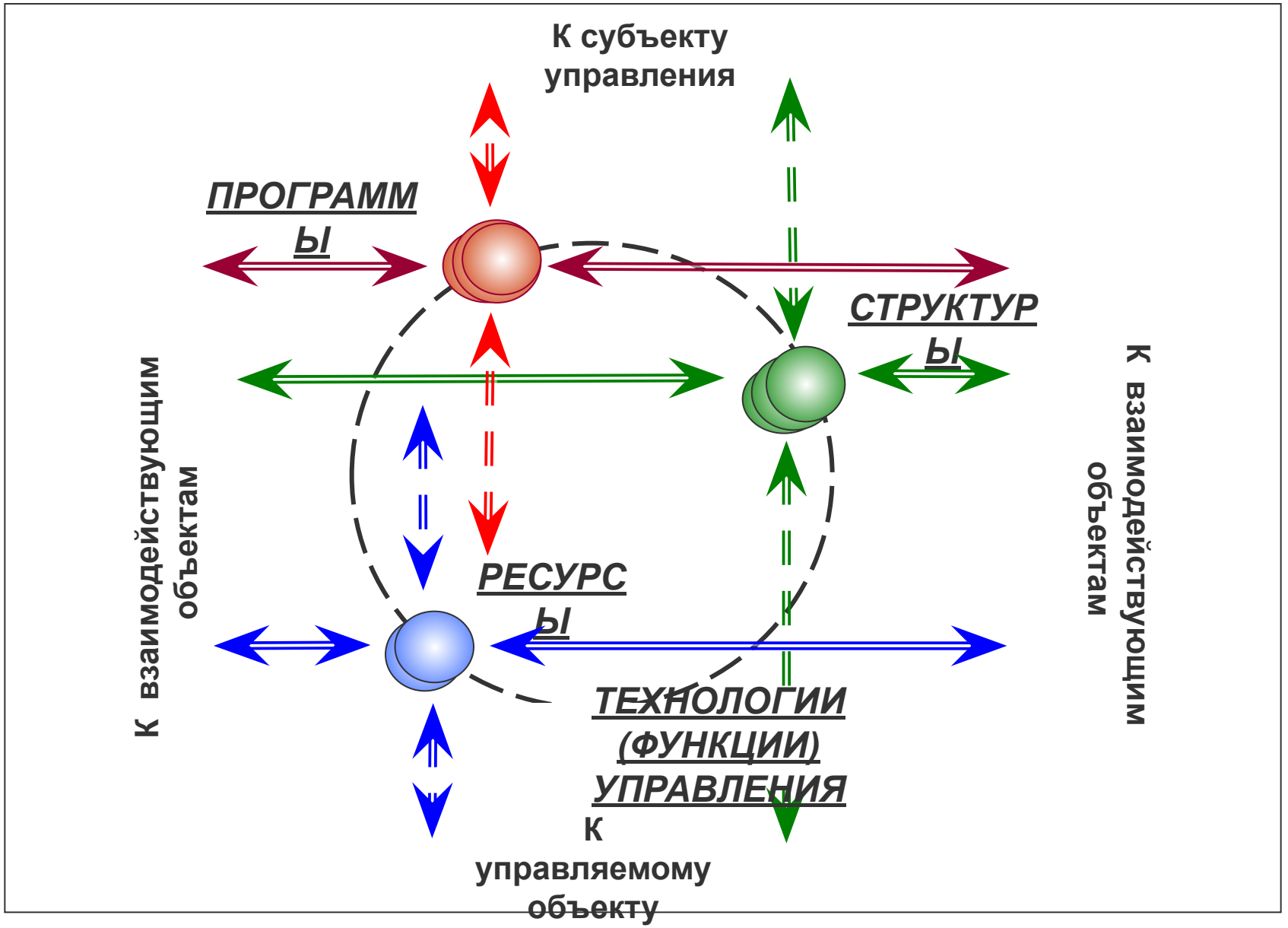
Угрозы безопасности информации — состояния и действия субъектов и материальных объектов, которые могут привести к изменению, уничтожению и хищению информации.

Изменение, уничтожение, хищение и блокирование информации — это результаты реализации угроз или свершившиеся угрозы.

Раздел 1.2. Защищаемые информация и информационные ресурсы. Объекты защиты.

ИНФОРМАЦИЯ КАК ИНФОРМАЦИОННЫЙ ОБЪЕКТ

ТОПОЛОГИЯ ИНФОРМАЦИОННОГО ОБЪЕКТА



В качестве стандартной модели безопасности часто приводят модель CIA:

- конфиденциальность (англ. confidentiality);
- целостность (integrity);
- доступность (availability).

Под конфиденциальностью понимается доступность информации только определённому кругу лиц,

под целостностью – гарантия существования информации в исходном виде,

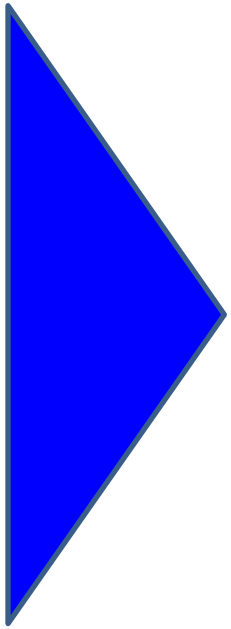
под доступностью – возможность получение информации авторизованным пользователем в нужное для него время.

Категории информации

Ограниченного доступа, содержащая сведения, составляющие государственную тайну

Ограниченного доступа, не содержащая сведения, составляющие государственную тайну

Общедоступная информации



Виды информационных и автоматизированных систем

- АРМ
- ГИС
- МИС
- АСУ ТП
- АСУ производства
- Сайты
- ИТКС
- ГРИД технологии
- Супер компьютеры
- Облачные технологии

Объект информатизации - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

Источник: ГОСТ Р 51275-2006 - Защита информации. Объект информатизации. Факторы, воздействующие на информацию.

Определение информации

- информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
- информация о гражданах (персональные данные) – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;
- конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

В более общем смысле информация – это сведения об окружающем мире, которые являются объектом хранения, преобразования, передачи и использования для определенных целей.

Носители информации

Для хранения как секретной, так и несекретной информации применяются одни и те же носители, которые охраняются ее собственником. Носители защищаемой информации классифицируются как документы; изделия (предметы); вещества и материалы; электромагнитные, тепловые, радиационные и другие излучения; гидроакустические, сейсмические и другие физические поля, представляющие особые виды материи; сам объект с его видовыми характеристиками и т.п.

В качестве носителя защищаемой информации может быть также человек.

Формы представления информации зависят от ее характера и физических носителей, на которых она представлена.

Основными формами информации являются:

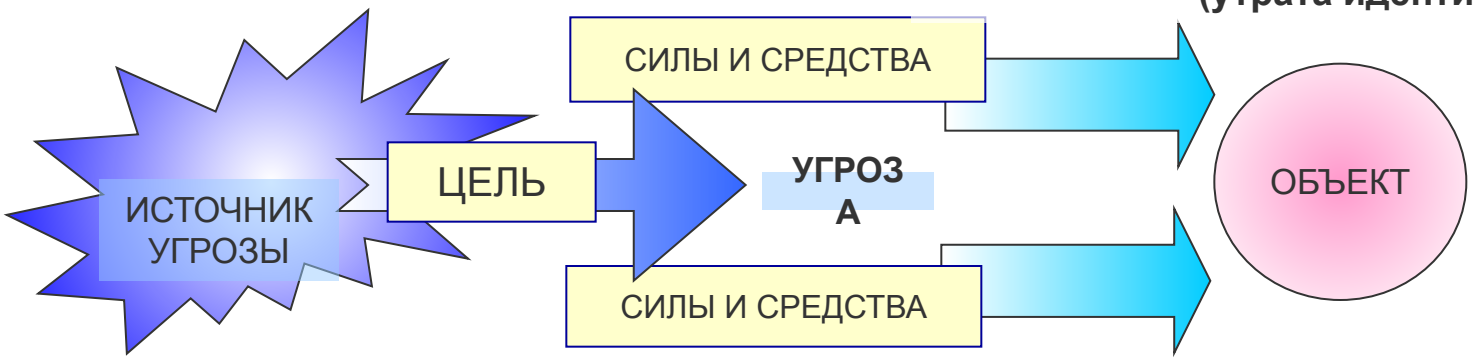
- документальные;
- акустические;
- телекоммуникационные;
- видовые.

Раздел 1.3. Угрозы безопасности информации, связанные с НСД.

СУЩНОСТЬ ПОНЯТИЙ «ОПАСНОСТЬ» И «БЕЗОПАСНОСТЬ»

ИНФОРМАЦИОННАЯ ОПАСНОСТЬ – состояние информационной обстановки, характеризуемое обострением рисков объекта (вызовов, угроз объекту), реализация которых сделает его менее соответствующим своему предназначению

ВЫЗОВЫ (УГРОЗЫ):
- утрата элементов структуры;
- нарушение системных связей;
- нарушение программ и функций;
- потеря способности к развитию;
- прекращение существования (утрата идентичности).



БЕЗОПАСНОСТЬ ПРЕДПОЛАГАЕТ

отсутствие опасности для функционирования (безопасность как состояние)

надежную **защищенность** от воздействия угроз (безопасность как свойство)

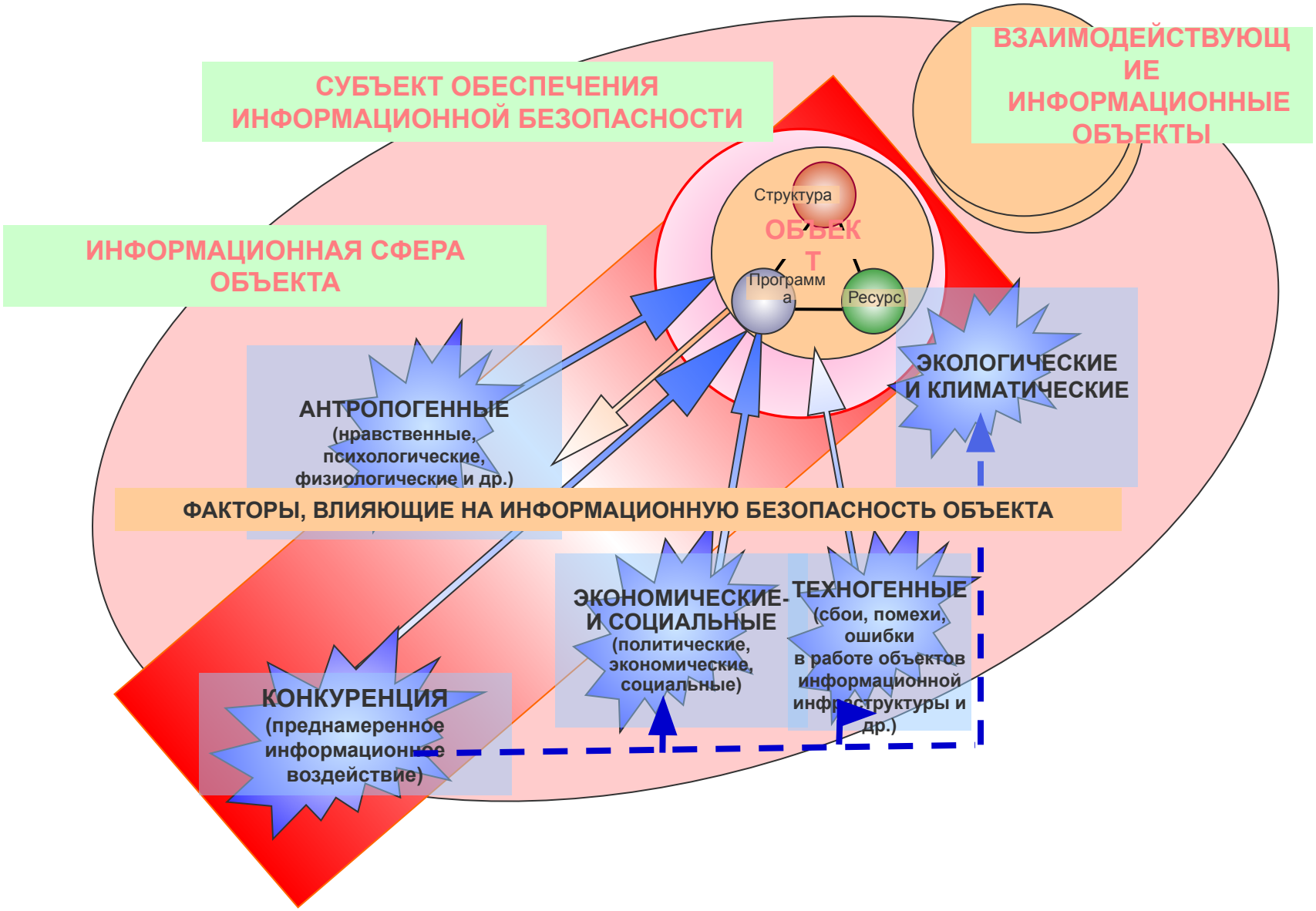
способность преодолевать угрозы, избегать опасность (безопасность как система)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – состояние информационной обстановки, характеризуемое отсутствием опасности, надежной защищенностью от угроз и способностью их нейтрализовывать

ЦЕЛИ ДОСТИЖЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Конфиденциальность, целостность и доступность: «модель CIA (Confidentiality-Integrity-Availability)»
Стандарты ISO 27001, ISO 27002

ФАКТОРЫ, ОКАЗЫВАЮЩИЕ ВЛИЯНИЕ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ



ИНТЕРЕСЫ КОРПОРАТИВНОГО ВЕДОМСТВА В ИНФОРМАЦИОННОЙ СФЕРЕ

Личности

- доступ к информации для удовлетворения потребностей;
- защита информации, обеспечивающей личную безопасность

Общества (коллектива)

- обеспечение интересов акционеров в информационной сфере;
- укрепление правовых основ информационной деятельности;
- поддержание согласия;
- защита духовных ценностей

Ведомства

- реализация интересов ведомства в информационной сфере;
- информационная поддержка деловой политики;
- регулирование и укрепление позиций на рынке;
- развитие информационной инфраструктуры

Угроза

Угроза – совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию ИТ или его владельцу.

РД Руководство по разработке профилей защиты и заданий по безопасности Гостехкомиссия России, 2003

Угроза – потенциальная причина нежелательного инцидента, который может причинить вред системе или организации.

ISO/IEC 13335-1-2004
ISO/IEC 17799:2005
ГОСТ Р ИСО/МЭК ТО 13335-1-2006

Угроза – опасность, предполагающая возможность потерь (ущерба)

СТО БР ИББС-1.0-2008

Уязвимость

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Базовая модель угроз безопасности персональных данных при их обработке в ИСПДн

Уязвимость – слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами.

ISO/IEC 13335-1-2004
ISO/IEC 17799:2005
ГОСТ Р ИСО/МЭК ТО 13335-1-2006

Уязвимость информационной безопасности – слабое место в инфраструктуре организации банковской системы РФ, включая СОИБ, которое может быть использовано для реализации или способствовать реализации угрозы ИБ.

СТО БР ИББС-1.0-2008

ОПАСНОСТЬ И БЕЗОПАСНОСТЬ ОБЪЕКТА КАК ХАРАКТЕРИСТИКИ СОСТОЯНИЯ ОБСТАНОВКИ

БЕЗОПАСНОСТЬ

ПОЛИТИКА

Компетенция политики – применение технологий перевода угроз в вызовы и вызовов в риски

ОПАСНОСТЬ

Степени	Компоненты		Готовность к нанесению ущерба
	намерения	возможность	
РИСК	нет	нет	мнимая
ВЫЗОВ	нет	есть	гипотетическая (возможная)
	есть	нет	
УГРОЗА	есть	есть	реальная (явная)

СТЕПЕНИ (УРОВНИ) ОПАСНОСТИ

- степени готовности противника к конфликтным действиям;
- степени зарождения (насыщения, обострения) противоречий между сторонами;
- уровни предконфликтного состояния сторон;
- персонификация (наличие или отсутствие явных субъектов и объектов противоречий)

РИСК → *ВЫЗОВ* → *УГРОЗА*

- наличие условий и факторов (интересов, ограниченных ресурсов, противоречий) для реализации;
- наличие возможности у объекта воздействия помешать достижению цели субъектом (US National Security Strategy)

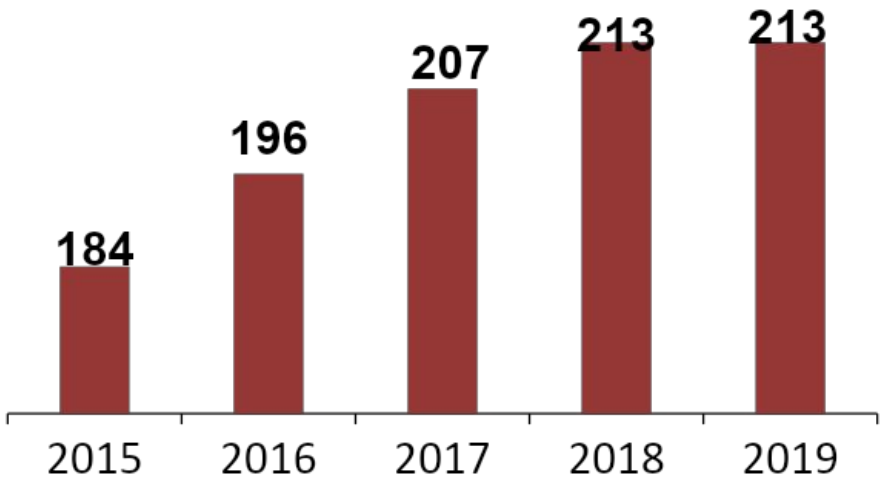
- стремление сторон начать спорить (бороться, конфликтные отношения);
- проявление (усиление) факторов обострения обстановки (противоречий);
- возможность противодействия со стороны объекта в ответ на воздействие субъекта (US National Security Strategy)

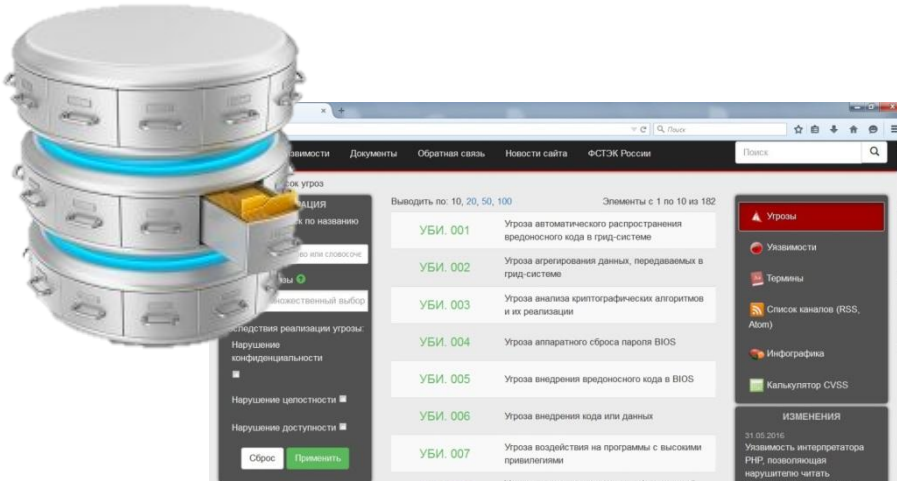
- обещание (намерение) сторон причинить вред, ущерб (потерю, убыток, урон);
- подготовительные (демонстративные) действия сторон, которые могут привести к конфликту

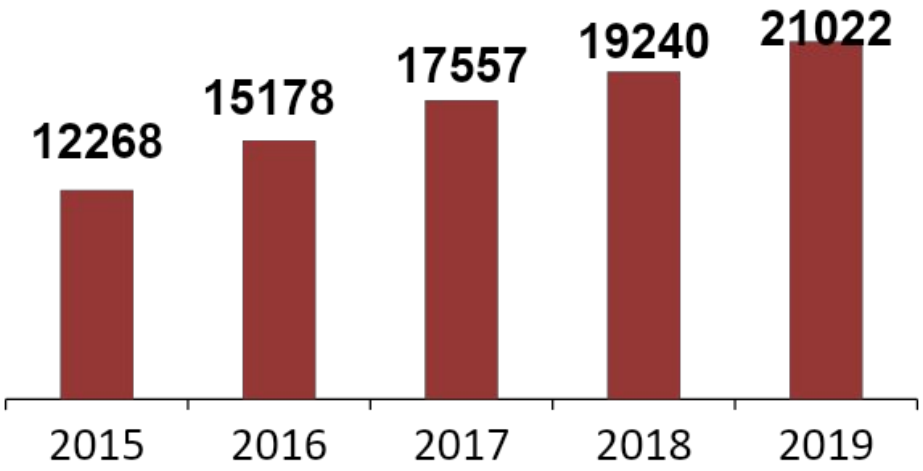
а) Субъективные намерения (замыслы, желания) противника

б) Объективные возможности у противника (наличие сил и средств) для реализации своих замыслов

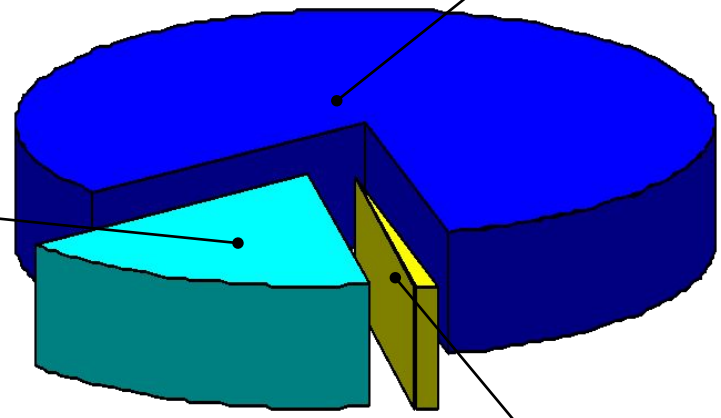
Банк данных угроз безопасности информации







Примерная структура возможных источников угроз конфиденциальной информации



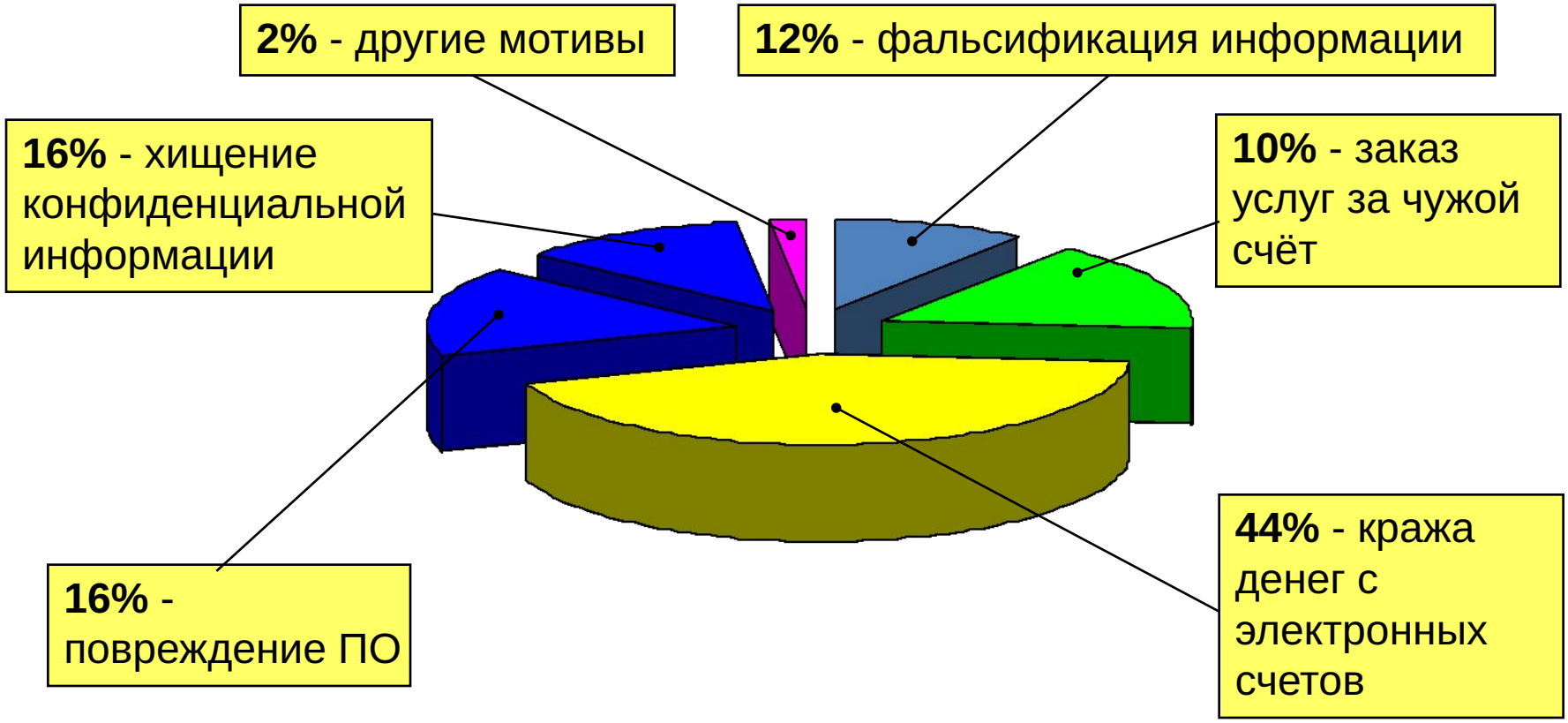
82% - собственные сотрудники организаций

17% - технические средства разведки; конкурирующие фирмы, клиенты, контрагенты; криминальные структуры, террористы

1% - случайные люди

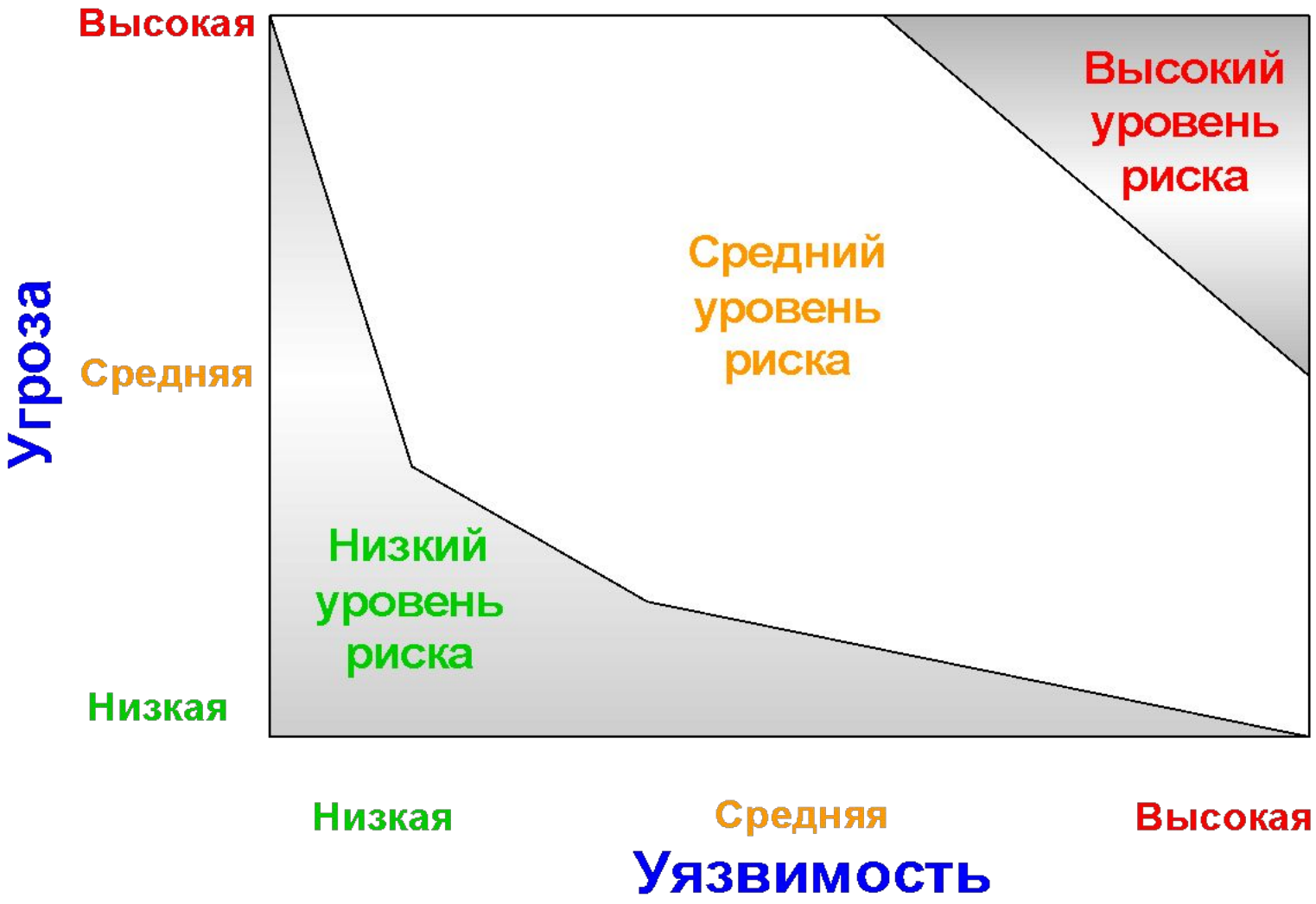
Структура основных целей (мотивов) умышленных действий персонала, приведших к утрате и модификации информации

По данным исследовательского центра DataPro Research (США)



Составляющие угрозы

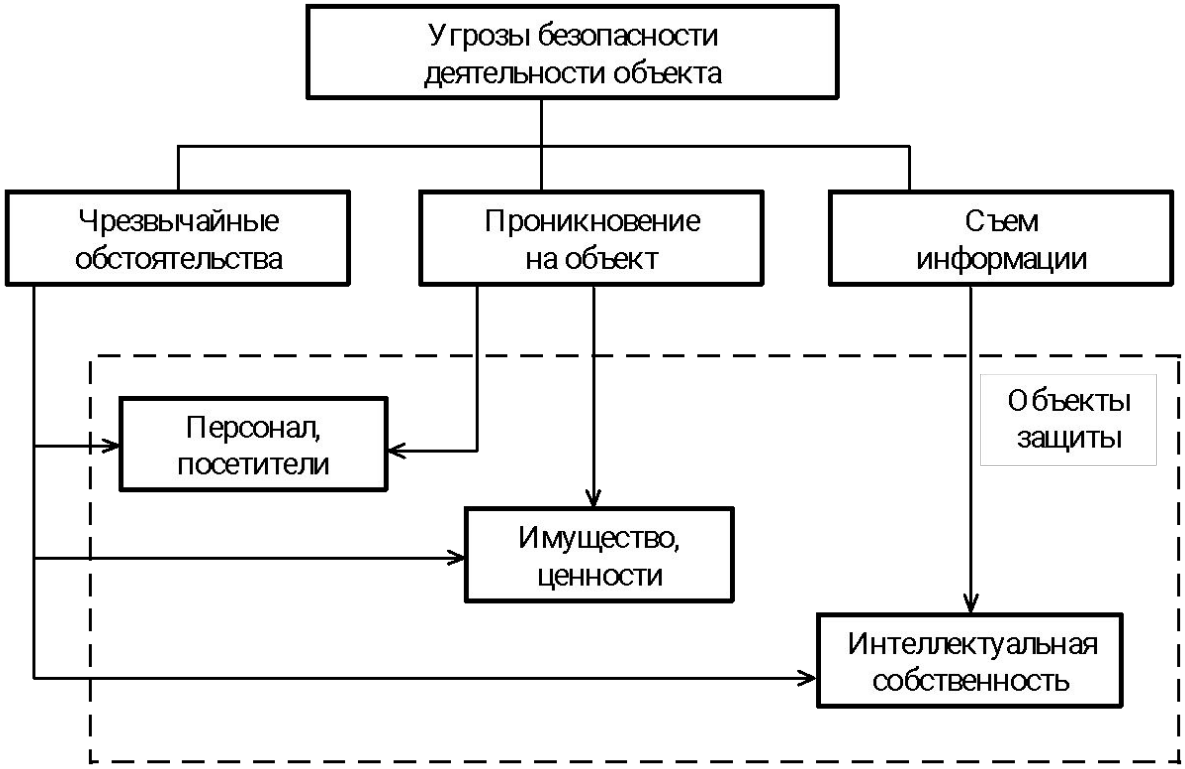
Уровень риска



Обобщенная модель способов овладения конфиденциальной информацией

№ п/п	Источники	СПОСОБЫ													Общее количество по источнику
		инициативное сотрудничество	склонение к сотрудничеству	выпытывание	подслушивание	наблюдение	хищение	копирование	подделка (модификация)	уничтожением (порча, разрушение)	незаконное подключение	перехват	незаконное ознакомление	фотографирование	сбор и аналитическая обработка	
1.	Люди	■	■	■	■	■	■		■	■			■	■		10
2.	Документы					■	■	■	■	■		■	■	■	■	9
3.	Публикации								■				■		■	3
4.	Технические носители						■	■	■	■					■	5
5.	ТСПИ				■	■	■	■	■	■	■	■	■	■		10
6.	Продукция					■	■	■	■	■			■	■		7
7.	Отходы						■								■	2
Итого		1	1	1	2	4	6	4	6	5	1	2	5	4	4	46

Воздействие различных типов угроз на объекты защиты



Раздел 1.4. Формирование требований по защите информации и создание системы защиты информации от НСД.

МЕТОДИЧЕСКИЙ АППАРАТ ФОРМИРОВАНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЦЕЛЬ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Формирование эффективной системы управления
- Формирование национального патриотического, корпоративного мировоззрения, ценностей, смыслов, целей
- Развитие современных технико-технологических основ управления
- Совершенствование образованности и профессиональной компетентности
- Обеспечение целостности, доступности и конфиденциальности информации
- Нейтрализация угроз в информационной сфере и их источников

МЕТОДЫ: Организационные | Экономические | Технические | Специальные

- ПОДДЕРЖАНИЕ УСЛОВИЙ ЭФФЕКТИВНОГО УПРАВЛЕНИЯ
- СОХРАНЕНИЕ ПОЗИТИВНЫХ ТЕНДЕНЦИЙ РАЗВИТИЯ
- СОХРАНЕНИЕ ОСНОВ КУЛЬТУРЫ, РАЗВИТИЕ БИЗНЕСА И ПОДДЕРЖАНИЕ СПЛОЧЕННОСТИ КОЛЛЕКТИВА

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Организационная структурно-функциональная подсистема
- Подсистема правового обеспечения
- Подсистема подготовки кадров и образования
- Подсистема морально-психологического обеспечения
- Подсистема анализа, прогнозирования и контроля
- Подсистема лингвистического, семантико-логического обеспечения
- Подсистема научных исследований
- Подсистема работы со СМИ и общественностью
- Подсистема мер обеспечения безопасности информации
- Подсистема технического обеспечения
- Подсистема взаимодействия с другими предприятиями и конкурентами

ВИДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

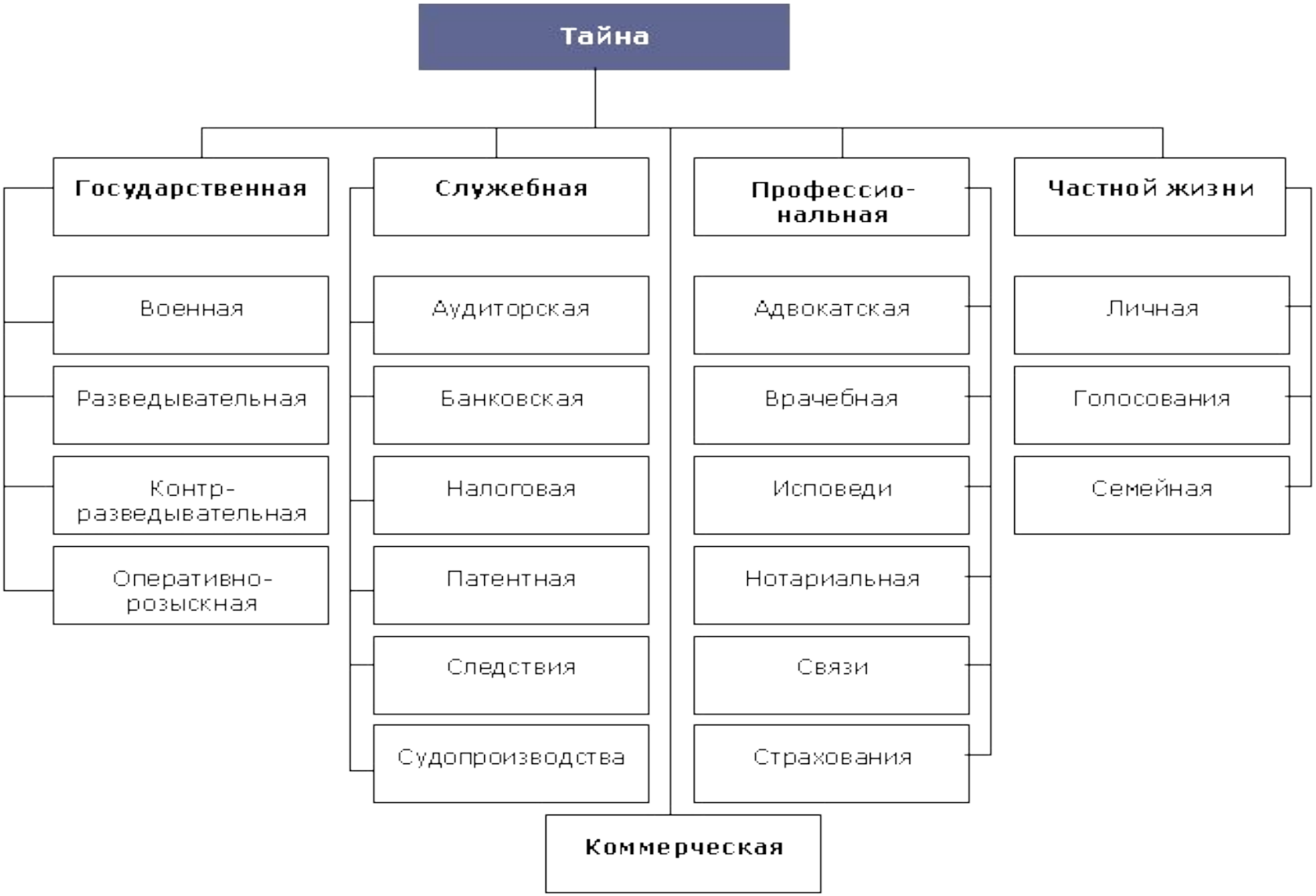
- Методическое
- Правовое
- Психологическое
- Информационное
- Научно-технологическое
- Лингвистическое
- Математическое (алгоритмическое)
- Защиты информации и др.
- Программное
- Аппаратно-техническое

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Понятия тайны

- **Тайной** называется информация о ком-либо, чём-либо, которая известна узкому кругу лиц и не предназначена для посторонних людей.
- **Коммерческая тайна** — это финансовая, деловая и т. п. информация, которая охраняется предпринимателем от посторонних лиц.
- **Государственная тайна** — это защищаемые государством сведения, распространение которых может нанести ущерб национальной безопасности.
- **Военная тайна** — это секретные сведения о расположении и функционировании военных объектов, воинских подразделений и т. п.
- **Тайной** называются сведения личного характера, которые не должны стать известными тому, для кого они не предназначены.
- **Тайной** называют профессиональные, специализированные сведения, знания, приёмы, которые неизвестны непосвящённым, новичкам в каком-то деле.

Некоторые виды тайн



Государственная тайна

Гри́ф секре́тности — реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемый на самом носителе и/или в сопроводительной документации на него.

В Российской Федерации сведения, отнесённые к государственной тайне, по степени секретности подразделяются на сведения:

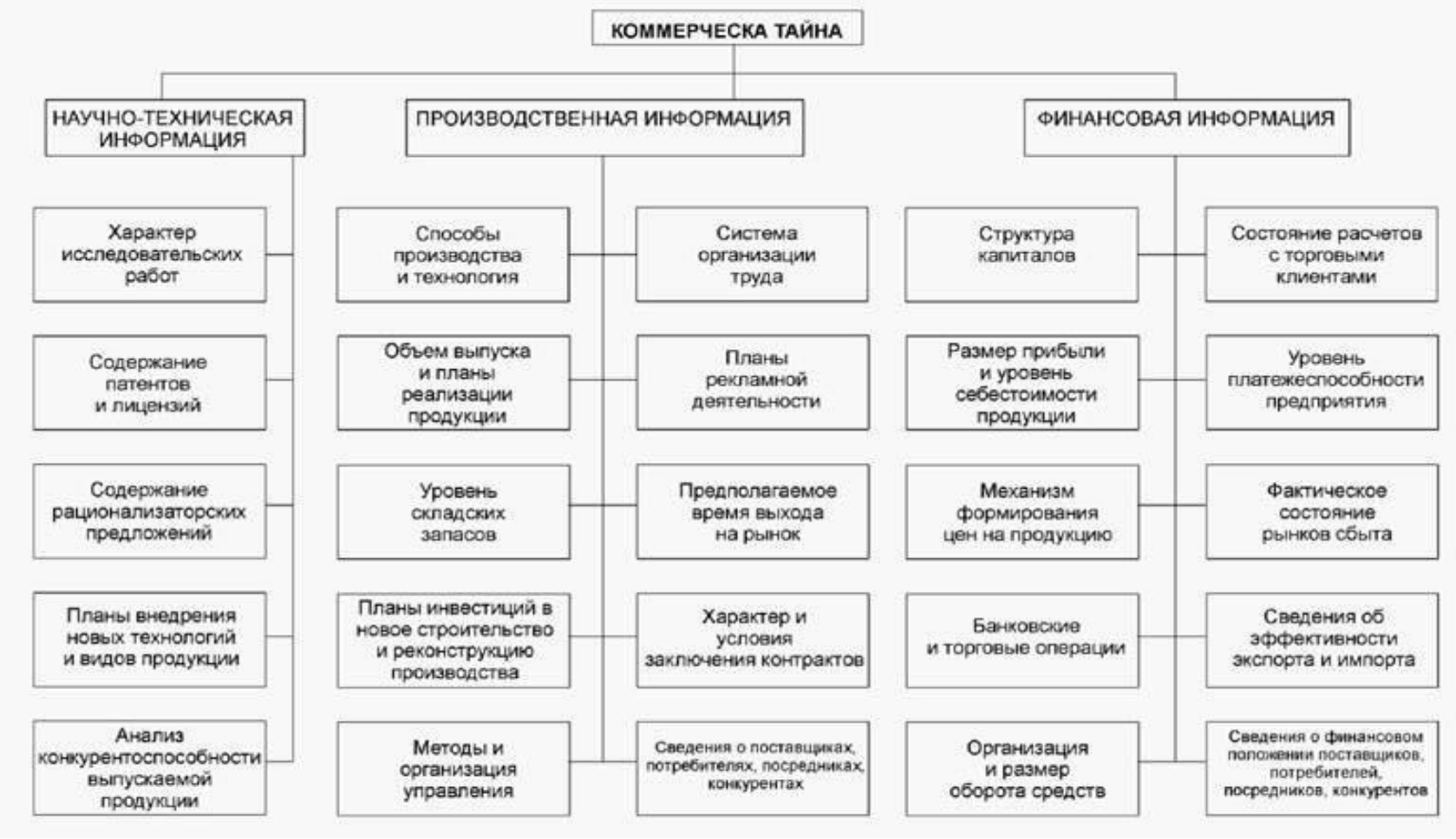
- **особой важности**: К сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей.
- **совершенно секретные**: К совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.
- **секретные**: К секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесённый интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности.

Не допускается использование грифов секретности для засекречивания сведений, не отнесённых к государственной тайне.

В Российской Федерации (как и в СССР до этого) также существует ограничительная пометка «*для служебного пользования*», которая ставится на несекретные документы органов государственной власти, ограничение на распространение которых диктуется служебной необходимостью.

Коммерческая тайна

Коммерческая тайна — режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. Под режимом конфиденциальности информации понимается введение и поддержание особых мер по защите информации.



Служебная тайна

Служебная тайна – это защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах государственного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Профессиональная тайна

Профессиональная тайна, обязанность не разглашать того, что стало известно лицу в силу его профессии; сюда принадлежит тайна исповеди, врачебная, адвокатская, нотариальная, служебная (канцелярская), тайна совещаний присяжных заседателей.

Обязанность П. тайны отчасти нравственного характера и охраняется обычаем, отчасти установлена законом, и нарушение ее карается (у нас лишь служебная или канцелярская тайна).

Лица, обязанные к П. тайне, освобождаются от показания на суде сведений, которые стали им известны в силу их профессий.

Профессиональная тайна

Личная тайна

Личную или семейную тайну составляют все сведения и факты, которые не относятся к общественной жизни гражданина, его работе или учебе. Понятие такой тайны для каждого человека индивидуально и зависит от его собственных представлений.

Например, к личной тайне относится факт обращения к адвокату по уголовному или гражданскому делу, наличие банковских вкладов, состояние здоровья человека, личные отношения, партийная принадлежность, отношение к религии и т.д.

К личной тайне относится и врачебная тайна, которая также не подлежит распространению без согласия гражданина.

Угрозы безопасности информации. Основной интерес зарубежной разведки:

- О состоянии и прогнозах развития военного, научно-технического и экономического потенциалов государств;
- О достижениях науки и техники, содержании научно-исследовательских, опытно-конструкторских, проектных работ и технологий, имеющих важное оборонное и экономическое значение;
- О тактико-технических характеристиках и возможностях боевого применения образцов вооружения и боевой техники;
- О дислокации, составе, вооружении войск и состоянии их боевого обеспечения;
- Об объемах запасов, добычи, поставки и потребления стратегических видов сырья, материалов и полезных ископаемых;
- О выполнении условий международных договоров, прежде всего, об ограничении вооружений и др.

Область интересов для коммерческой разведки:

- Коммерческая философия и деловая стратегия руководителей фирм-конкурентов, их личные и деловые качества
- Научно-исследовательские и конструкторские работы
- Финансовые операции фирм
- Организация производства, в том числе данные о вводе в строй новых, расширении и модернизации существующих производственных мощностей, объединение с другими фирмами
- Технологические процессы при производстве новой продукции, результаты ее испытаний
- Маркетинг фирмы, в том числе режимы поставок, сведения о заказчиках и заключаемых сделках, показатели реализации продукции
- Сведения об организациях, потенциально являющихся союзниками или конкурентами
- Сведения о деятельности потенциальных и реальных конкурентов
- Учет и анализ попыток несанкционированного получения коммерческих секретов конкурентами
- Оценка реальных отношений между сотрудничающими и конкурирующими организациями;
- Анализ возможных каналов утечки конфиденциальной информации.

Методы коммерческой разведки:

- промышленный шпионаж

Цель – добывание данных о разрабатываемой продукции

- **бизнес-разведка** (деловая, конкурентная, экономическая)

Цель – получение информации для руководства, необходимой для принятия им обоснованных управленческих решений, т.е. сведения о глобальных процессах в экономике, политике, технологии производства, партнерах и конкурентах, тенденциях рынка и других вопросах

Основу конкурентной разведки составляют процессы поиска информации в открытых источниках и ее анализ с целью получения необходимых сведений

Наращивание зарубежными странами возможностей воздействия на информационную инфраструктуру в военных целях

Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия

Использование террористическими и экстремистскими организациями механизмов информационного воздействия на сознание

Возрастание масштабов компьютерной преступности

Увеличение масштабов применения информационных технологий в военно-политических целях

Увеличение масштабов и рост скоординированности компьютерных атак на объекты критической информационной инфраструктуры

Недостаточный уровень развития конкурентоспособных информационных технологий

Недостаточная эффективность научных исследований

Стремление отдельных государств использовать технологическое превосходство

ОРГАНЫ, ОБЕСПЕЧИВАЮЩИЕ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ РОССИЙСКОЙ ФЕДЕРАЦИИ

Комитет Государственной думы по безопасности

Совет Безопасности России

Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

Федеральная служба безопасности Российской Федерации (ФСБ России)

Служба внешней разведки Российской Федерации (СВР России);

Министерство обороны Российской Федерации (Минобороны России)

Министерство внутренних дел Российской Федерации (МВД России)

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

Закон
«О государственной тайне»

№5485-1
от 21.07.1993

Федеральный закон
«Об информации, информационных технологиях и о защите информации»

№ 149-ФЗ
от 27.07.2006

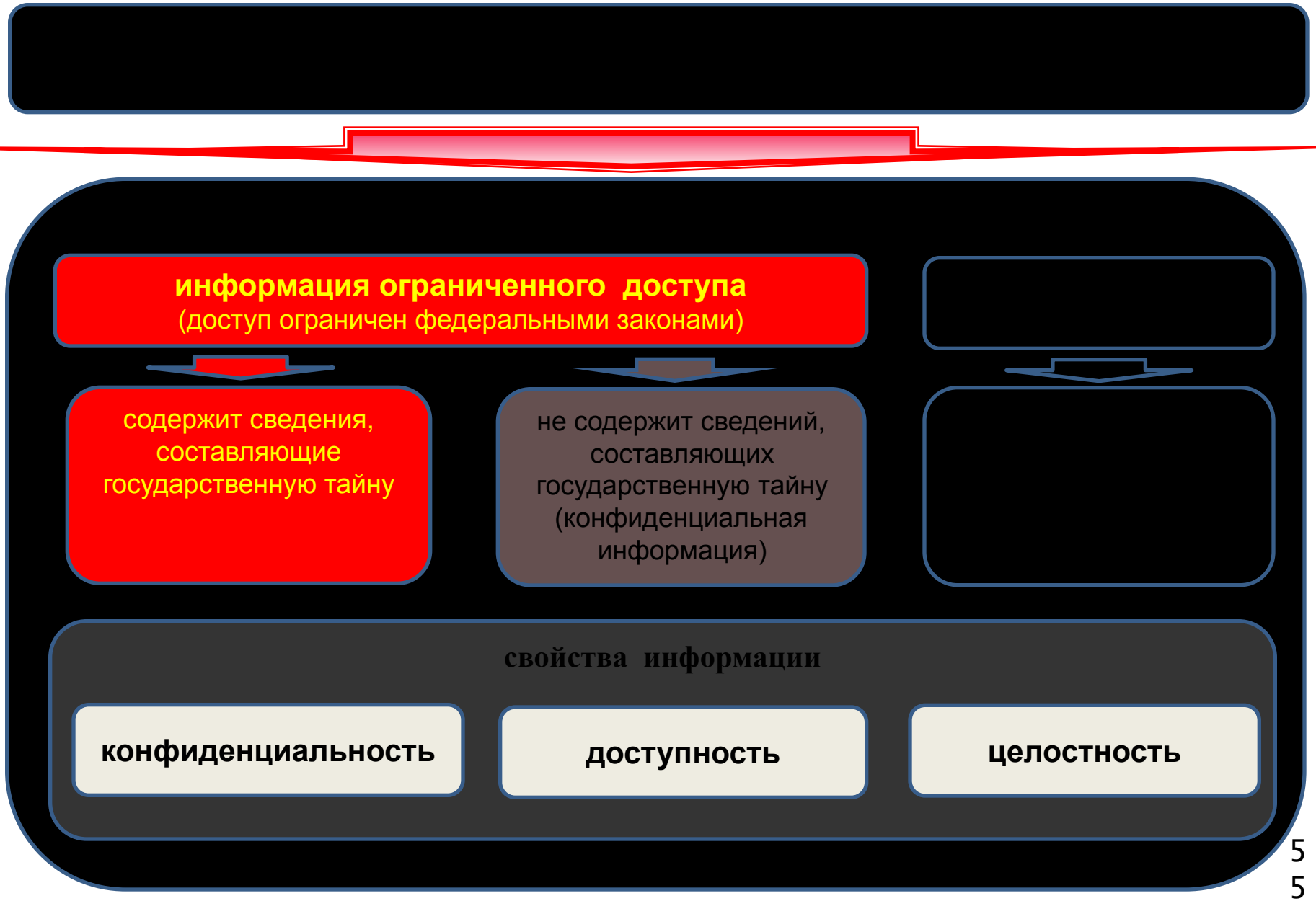
Федеральный закон
«О персональных данных»

№ 152-ФЗ
от 27.07.2006

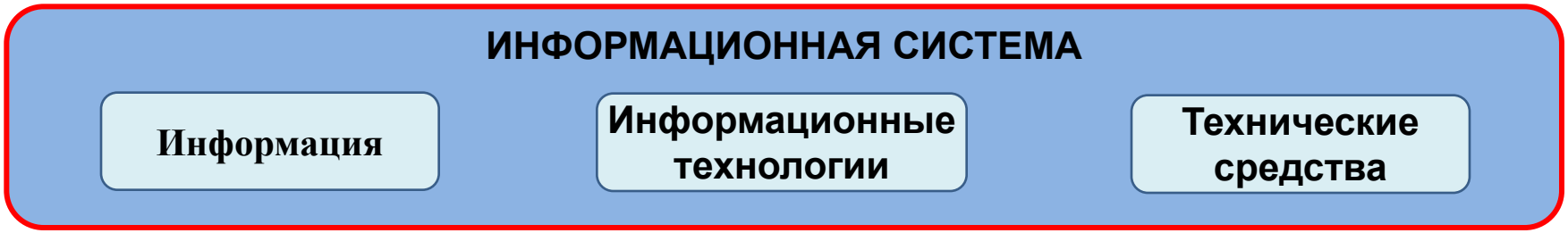
Федеральный закон
«О безопасности критической информационной инфраструктуры Российской Федерации»

№ 187-ФЗ
от 26.07.2017

149-ФЗ
«Об информации, информационных технологиях и о защите информации»



149-ФЗ
«Об информации, информационных технологиях и о защите информации»



Государственные информационные системы

Муниципальные информационные системы

Иные информационные системы

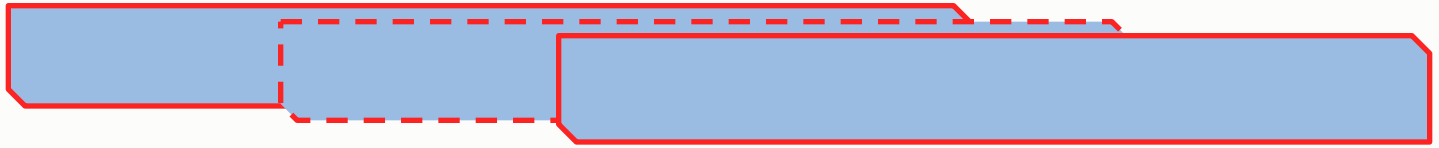
- **Федеральные**
- **Региональные**

Правительство Российской Федерации утверждает **требования**
к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем

Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области ПД ИТР и ТЗИ, в пределах их полномочий

«Закон о государственной тайне»

Решения Межведомственной комиссии по защите государственной тайны



Постановления Правительства Российской Федерации

Положение о государственной системе защиты информации в РФ от ИТР и от ее утечки по техническим каналам

Инструкция по обеспечению режима секретности в Российской Федерации

Нормативные правовые и методические документы ФСТЭК России

Документы, регулирующие вопросы организации работ по ТЗИ

Документы, регулирующие вопросы выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам

Документы, регулирующие вопросы выполнения комплекса мероприятий по предотвращению несанкционированного доступа к информации

152-ФЗ «О персональных данных»

НПА Правительства Российской Федерации

Постановление Правительства Российской Федерации

№ 1119

«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Постановление Правительства Российской Федерации

№ 211

«Об утверждении перечня мер, направленных на выполнения обязанностей, предусмотренных 152-ФЗ «О персональных данных» и принятыми в соответствие с ними нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»

НПА и методические документы ФСТЭК России

«Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

(утверждены приказом ФСТЭК России **от 18.02.2013 № 21**)

Документы, регулирующие вопросы защиты информации от ее утечки по техническим каналам и предотвращения НСД к информации

Методические документы, регулирующие вопросы актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Критическая информационная инфраструктура Российской Федерации

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

№ 187-ФЗ

О безопасности критической информационной инфраструктуры Российской Федерации

Москва, Кремль
26 июля 2017 года
N 187-ФЗ

Президент
Российской Федерации
В.ПУТИН

Безопасность критической информационной инфраструктуры - состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак

Компьютерная атака - целенаправленное воздействие на объекты КИИ, сети электросвязи, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации

Изменения законодательной базы Российской Федерации

Федеральный закон от 26 июля 2017 г. № 193-ФЗ
«О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»

Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»

Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»

Федеральный закон от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»

Федеральный закон от 26 июля 2017 г. № 194-ФЗ
«О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»

Глава 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной информации» дополнена статьей 274.1

Статья 151 Уголовно-процессуального кодекса Российской Федерации относит составы преступлений к подследственности правоохранительных органов, выявивших эти преступления

Документы ФСТЭК России, регулирующие вопросы предотвращения утечки информации по техническим каналам:

- «**Сборник** временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам» (утвержден Гостехкомиссией в 2002 г.)**:**
  - Временная методика оценки защищенности помещений от утечки речевой КИ по акустическому и виброакустическому каналам;
  - Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований в ВТСС;
  - Временная методика оценки защищенности ВТСС, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации;
  - Временная методика оценки защищенности конфиденциальной информации, обрабатываемой ОТСС, от утечки за счет наводок на ВТСС и их коммуникации;
- **Требования** к средствам активной защиты информации от утечки за счет ПЭМИН» (утверждены приказом ФСТЭК России от 3.10.2014 № 033, зарегистрированы Минюстом России, р/н № 35057 в 2014г., применяются с 1.04.2015)

Документы ФСТЭК России, регулирующие вопросы

предотвращения НСД к информации:

- «**Сборник руководящих документов по защите информации от несанкционированного доступа**» (издан Гостехкомиссией России в 1998 г.);
- «**Руководящий документ.** Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (утвержден приказом Гостехкомиссии России от 04.06.1999 № 114);
- «**Сборник методических документов** по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи (МД по ТЗИ ВРСП-К) (утвержден приказом ФСТЭК России от 15.03.2012 г. № 27);
- **Документы по техническому регулированию, устанавливающие требования к средствам защиты информации**

Документы по стандартизации

в области технической защиты информации

Документы (данные), используемые при решение вопросов технической защиты информации в ИС (АС):

- **Проектная документация**;
- **Банк данных угроз безопасности информации ФСТЭК России;**
- **Методические документы по моделированию угроз безопасности информации;**
- **Модель угроз безопасности информации;**
- **Документация на используемые средства защиты информации;**
- **Эксплуатационная документация;**
- **Локальные нормативные акты (организационно-распорядительные документы)**

Нормативные правовые акты по защите информации в ИС общего пользования

ИНФОРМАЦИЯ в информационных системах общего пользования

(Перечни сведений для обязательного размещения в сети Интернет в форме открытых данных (постановление Правительства РФ **24.11.2009 г. N 953,** распоряжение Правительства РФ **от 10 июля 2013 г. N 1187-р**)

Целостность

Доступность

149-ФЗ

Постановление Правительства РФ
от 18.05.2009 г. **№ 424**

«Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям»

ПРИКАЗ Минкомсвязи России
от 25.08.2009 г. № 104

«Об утверждении требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования»

ПРИКАЗ ФСБ России и ФСТЭК России
от 31.08.2010 г. № 416/489

«Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»

Совместный приказ ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489

Классы ИС общего пользования:

1 класс – системы Правительства Российской Федерации, федеральных министерств, федеральных служб и федеральных агентств, руководство деятельностью которых осуществляет Президент Российской федерации,
ИС федеральных служб и федеральных агентств, подведомственных этим федеральным министерствам;

2 класс – все остальные информационные системы общего пользования

В системах:

1 класса - используются СЗИ сертифицированные ФСБ России;

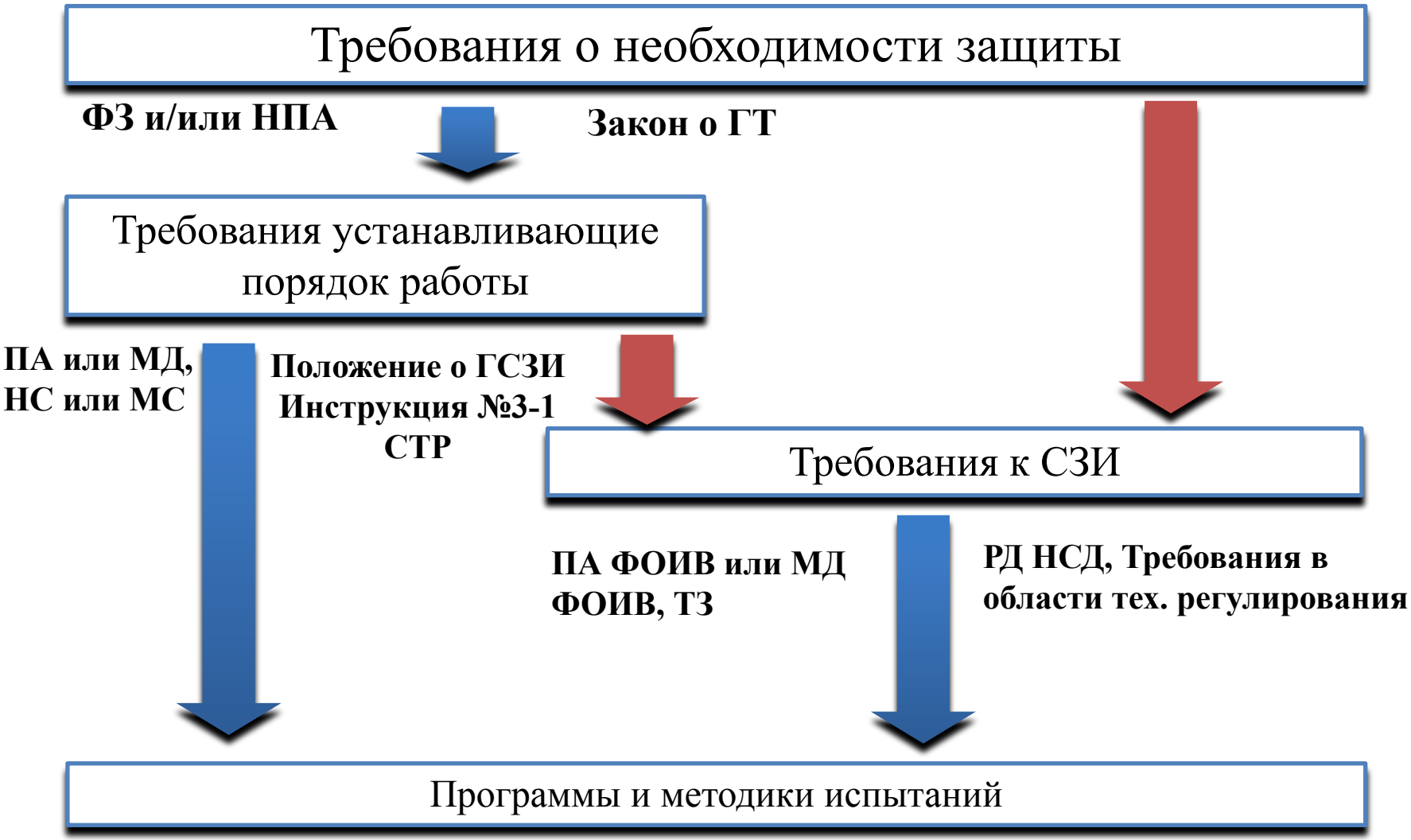
2 класса – используются СЗИ, сертифицированные ФСБ России и (или) ФСТЭК России

Основные мероприятия по обеспечению защиты информации в ИС:

- формирование модели угроз;
- разработка на основе модели угроз системы защиты информации (СЗИ);
- проверка готовности СЗИ к использованию с составлением заключений о возможности эксплуатации;
- установка и ввод в эксплуатацию СЗИ;
- обучение лиц, использующих средства защиты информации;
- учет применяемых СЗИ, эксплуатационной и технической документации к ним;
- контроль за соблюдением условий использования СЗИ;
- проведение разбирательств и составление заключений по фактам несоблюдения условий использования СЗИ, которые могут привести к нарушению безопасности информации;
- описание системы защиты информации

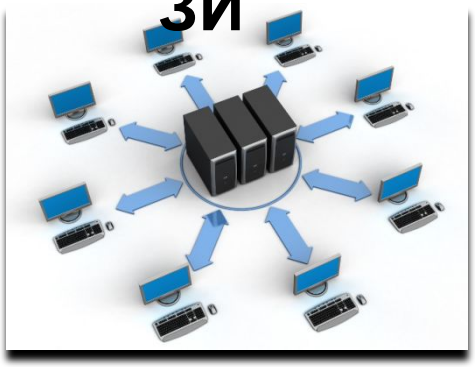
МОДУЛЬ 2. Защита информации от НСД
Раздел 2.1. Организационно-технические основы выполнения мероприятий по ТЗИ от НСД.

СИСТЕМА ТРЕБОВАНИЙ В ОБЛАСТИ ТЗИ



ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Система ЗИ



≠

Выполнение требований Аттестация

Нейтрализация актуальных

=

Выполнение необходимых процедур (в том числе аттестация)

Поддержка жизненного цикла системы ЗИ

Уверенность оператора в отсутствии последствий в случае инцидента

ТРЕБОВАНИЯ УСТАНАВЛИВАЮЩИЕ ПОРЯДОК РАБОТЫ

Система требований к оценке эффективности

ТЗ и ТП

- Нейтрализация актуальных угроз
- Выполнение требований к СЗИ

Программа и методика испытаний

Испытания

1. Формирование требований к системе ЗИ АСЗИ

- Формирование требований к АС
- Разработка концепции АС
- Техническое задание

2. Разработка системы ЗИ АСЗИ

- Эскизный проект
- Технический проект
- Рабочая документация

3. Внедрение системы ЗИ АСЗИ

- Ввод в действие
- Аттестация АСЗИ

4. Сопровождение системы ЗИ в ходе эксплуатации АСЗИ

- Сопровождение АС

ТРЕБОВАНИЯ УСТАНАВЛИВАЮЩИЕ ПОРЯДОК РАБОТЫ

Государственная тайна	КСИИ	Информация ограниченного доступа, не содержащая сведения составляющие ГТ		Информация, которая в соответствии с ФЗ подлежит предоставлению или распространению (Сайты гос. органов)
СТР	**МД КСИИ**	**Приказ ФСТЭК России №31**	**Приказ ФСТЭК России №17, 21**	**СТР-К**
			МД. Меры ЗИ в ГИС	Приказ ФСБ России и ФСТЭК России №416/489

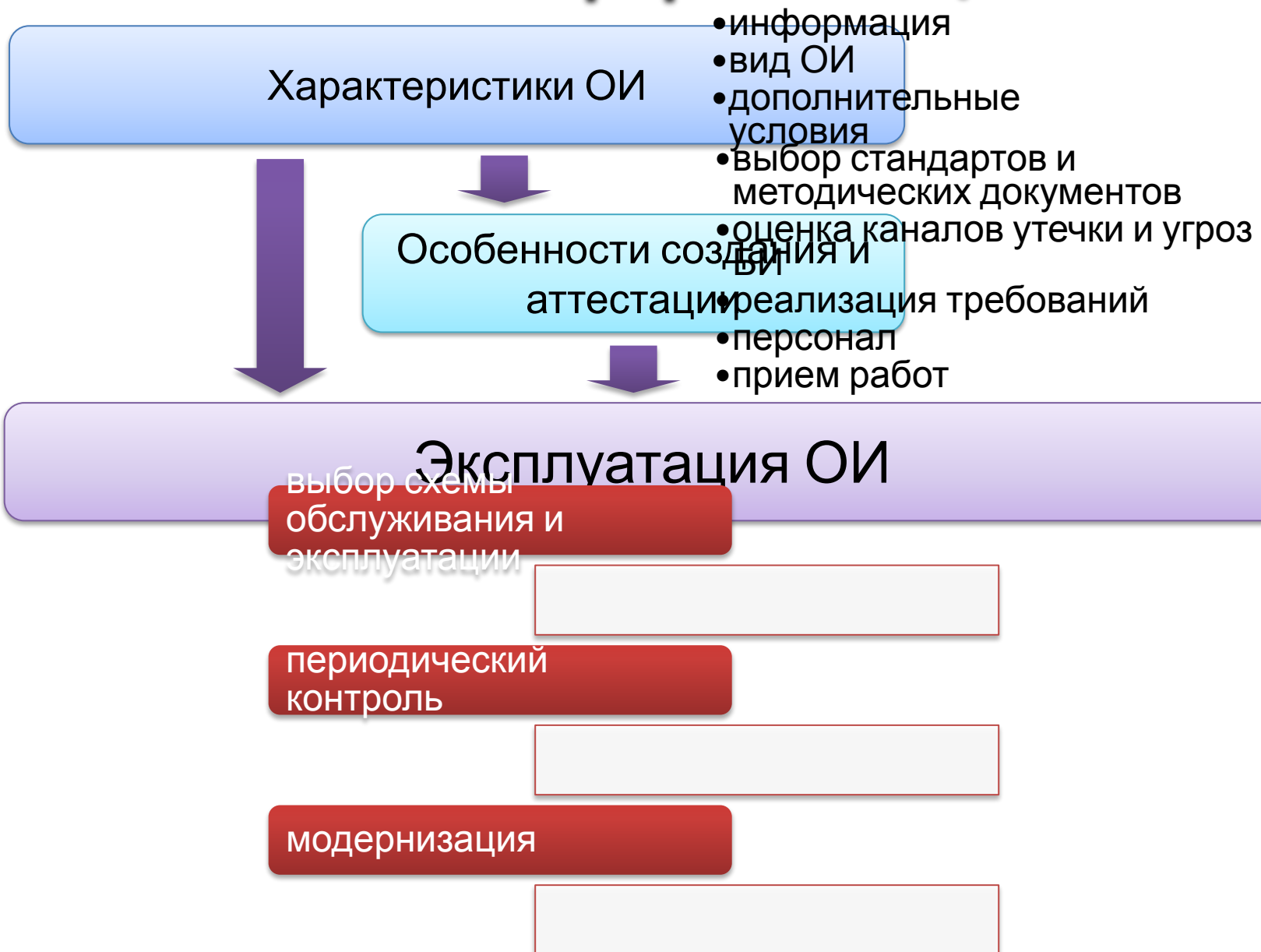
РД. СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации.

.РД. АС. Защита от НСД к информации. Классификация АС и требования по ЗИ

РД. Защита от НСД к информации. Часть1. Программное обеспечение СЗИ. Классификация по уровню контроля отсутствия НДВ.

РД. СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации.

Эксплуатация объектов информатизации



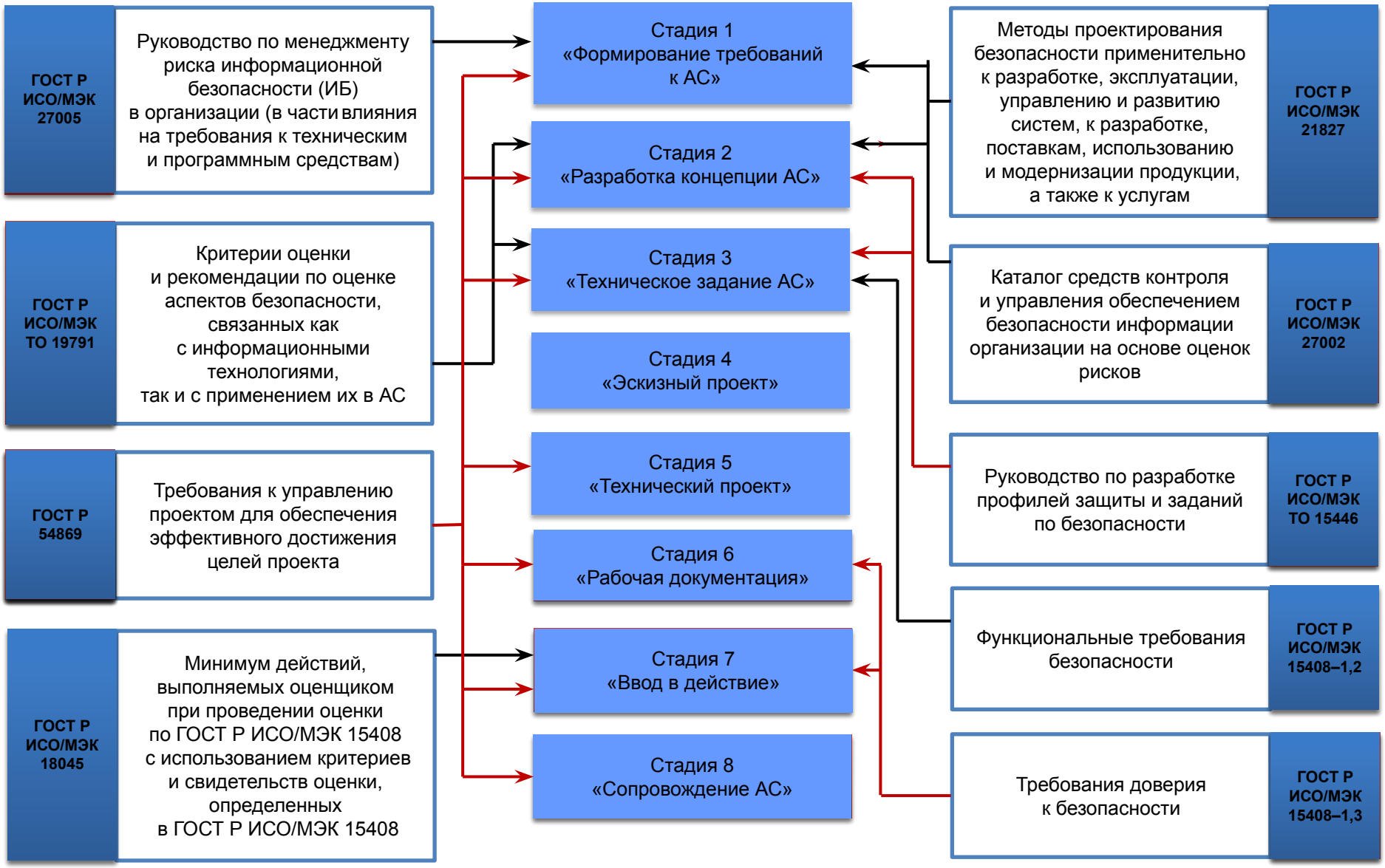
НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ АВТОМАТИЗИРОВАННННЫМИ СИТЕМАМИ

ПРИКАЗ ФСТЭК РОССИИ № 17

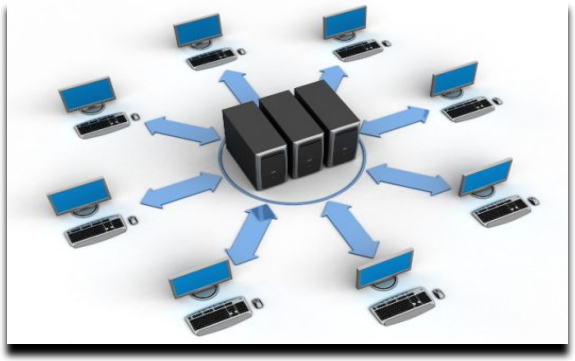
ПУНКТ 18. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ХОДЕ ЭКСПЛУАТАЦИИ

- управление (администрирование) системой защиты информации ИС
- выявление инцидентов и реагирование на них
- управление конфигурацией аттестованной ИС и ее системы ЗИ
- контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе

Эксплуатация объектов информатизации



ОЦЕНКА СООТВЕТСТВИЯ СЗИ



оператор ИС

Доверие к качеству разработки и производства

Доверие к функционалу

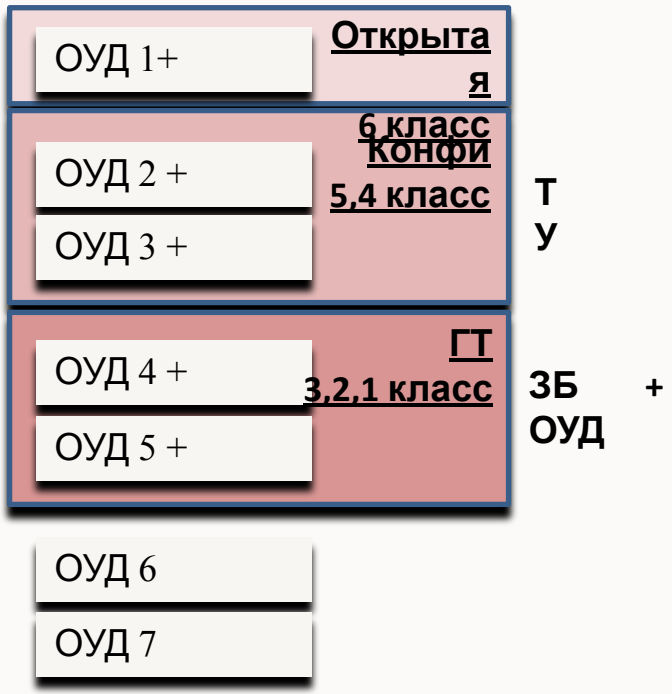
Отсутствие НДВ

Отсутствие уязвимостей

Своевременное и доверенное обновление

Система требований нового поколения

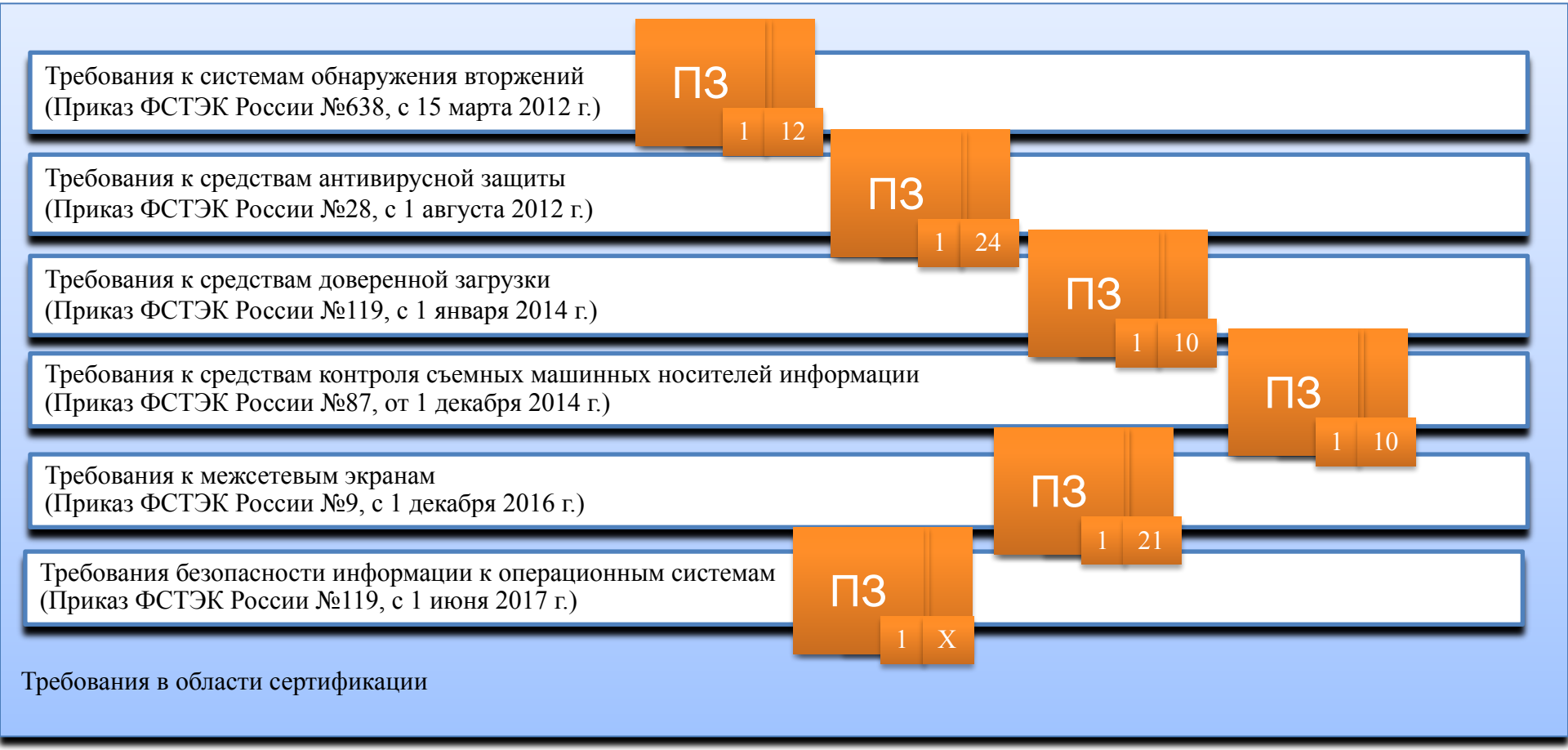
ПОЛУЧЕНИЕ ДОКАЗАТЕЛЬСТВ СООТВЕТСТВИЯ КЛАССУ СЗИ



Действия по ОУД 3 оценочный уровень доверия **(4 класс СЗИ)**

1. Оценка ЗБ
2. Оценка управления конфигурацией
3. Оценка документов поставки и эксплуатации
4. Оценка документов разработки
5. Оценка руководств
6. Оценка поддержки жизненного цикла
7. Оценка тестов
8. Тестирование
9. Оценка уязвимостей

СИСТЕМА ТРЕБОВАНИЙ К СЗИ ОТ НСД



ЭВОЛЮЦИЯ СИСТЕМЫ ТРЕБОВАНИЙ К СЗИ

Система РД

- РД СВТ
- РД АС
- РД МЭ
- РД НДВ

- Управление доступом
- Регистрация и учет
- Обеспечение целостности
- Межсетевое экранирование

Система требований к СЗИ от НСД нового

- Требования безопасности информации к ОС
- Требования к средствам идентификации и
- Требования к средствам управления доступом
- Требования к средствам разграничения доступа
- Требования к средствам контроля целостности
- Требования к средствам очистки памяти
- Требования к средствам межсетевого экранирования
- Требования к системам управления базами данных
- Требования к средствам управления потоками информации
- Требования к средствам защиты от несанкционированного вывода (ввода) информации (DLP –
- Требования к средствам контроля и анализа защищенности
- Требования к средствам ограничения программной среды
- Требования к средствам защиты среды виртуализации
- Требования к базовым системам ввода-вывода

ТРЕБОВАНИЯ К МЕЖСЕТЕВЫМ ЭКРАНАМ

Приказ ФСТЭК России №9, с 1 декабря 2016 г.

Типы	
А	- уровня сети
Б	- уровня логических границ сети
В	- уровня узла
Г	- уровня приложения
Д	- уровня промышленной сети

Классы		
1	2	3
Гос. тайна		
4		
1 ГИС (ИСПДн), 1 АСУ ТП		
5		
2 ГИС (ИСПДн), 2 АСУ ТП		
6		
3,4 ГИС (ИСПДн), 3 АСУ ТП		

ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ К ОПЕРАЦИОННЫМ СИСТЕМАМ

Приказ ФСТЭК России № 119, с 1 июня 2017 г.

Типы

- **А** - общего назначения
- **Б** - встраиваемая
- **В** - реального времени

Классы

- **1**
- **2**
- **3**

Гос. тайна

- **4**

1 ГИС (ИСПДн), 1 АСУ ТП

- **5**

2 ГИС (ИСПДн), 2 АСУ ТП

- **6**

3,4 ГИС (ИСПДн), 3 АСУ ТП

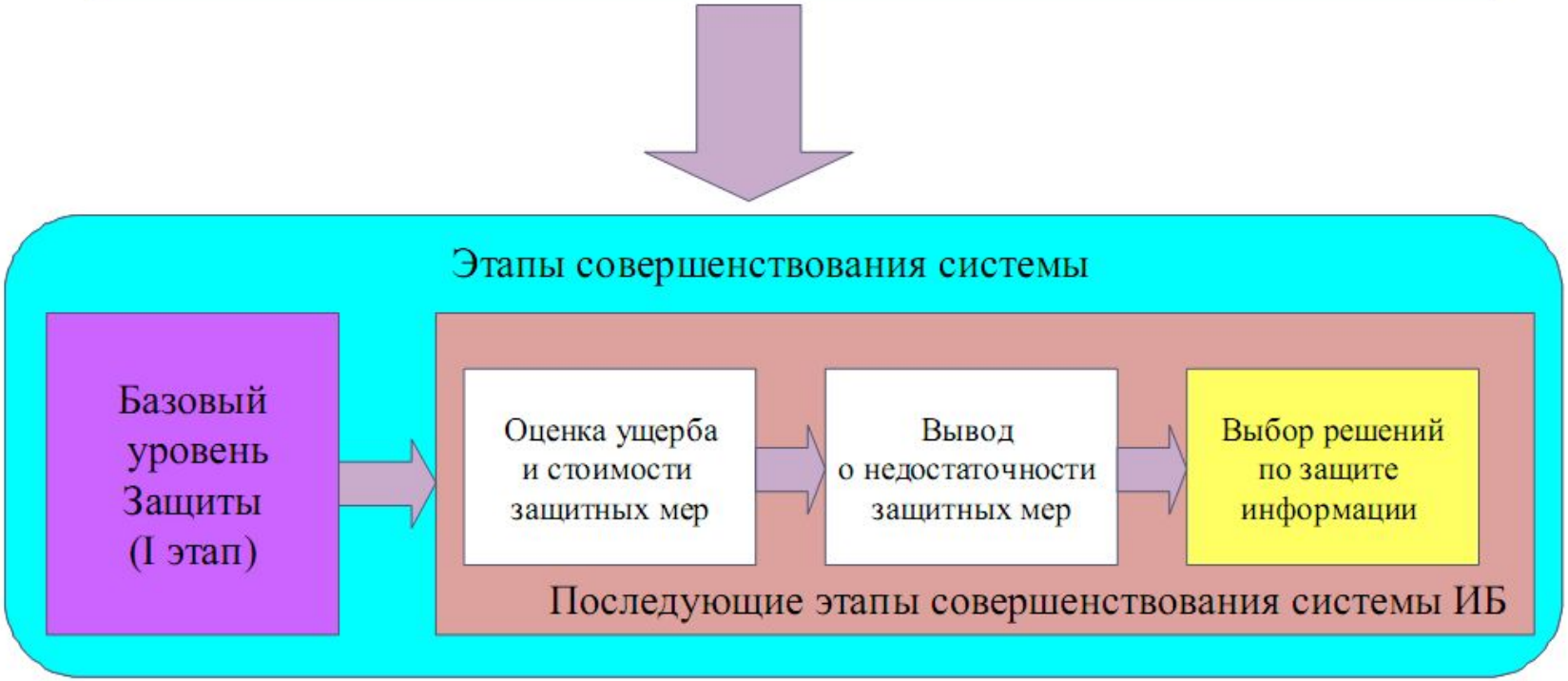
Раздел 2.2. Меры и средства защиты информации от НСД.

Требования к системе информационной безопасности и этапы ее развития

Требования к системе информационной безопасности:

централизация, плановость, конкретность и целенаправленность, активность,

надежность и универсальность, нестандартность, открытость, экономическая эффективность



МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРАВОВЫЕ

1. Изменения в законодательстве в интересах системы обеспечения инф. безопасности
2. Законодательное разграничение полномочий между органами власти
3. Уточнение статуса иностранных информационных агентств
4. Законодательное закрепление приоритета развития национальных сетей связи

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ

1. Создание и совершенствование системы обеспечения информационной безопасности
2. Предупреждение и пресечение правонарушений в информационной сфере, привлечение к ответственности лиц, совершивших преступления
3. Совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности СПО
4. Создание систем и средств предотвращения НСД к обрабатываемой информации
5 Выявление технических устройств и программ, представляющих опасность
6. Предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты
7. Сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации
8. Совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации

ЭКОНОМИЧЕСКИЕ

1. Разработка программ обеспечения информационной безопасности и определение порядка их финансирования
2. Совершенствование системы финансирования работ, по реализации правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков

СОДЕРЖАНИЕ И СРЕДСТВА НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

УДАЛЕННЫЙ ДОСТУП К ИНФОРМАЦИОННЫМСИСТЕМАМ

- через каналы связи
- через аппаратные и программные средства абонентов
- через технические и программные средства других сетей

НЕПОСРЕДСТВЕННОЕ ПРОНИКНОВЕНИЕ В АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА

- АРМ должностных лиц
- средства контроля и управления
- технологические средства регламентных и ремонтных работ

СРЕДСТВА

Средства компьютерной разведки и дешифрования

- Средства исследования параметров
- Средства подключения
- Средства преодоления систем защиты ИТКС
- Средства добывания информации
- Средства подбора паролей, ключей и вскрытия алгоритмов
- Средства сбора, передачи, обработки и хранения

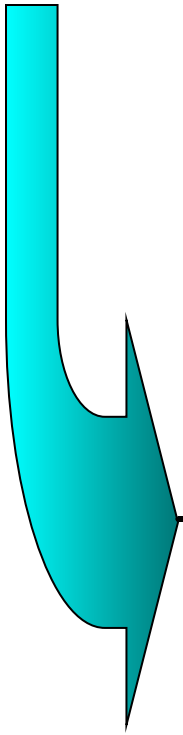
Средства нарушения конфиденциальности и целостности информации

- Средства реализации компьютерных атак
- Средства применения компьютерных вирусов
- Закладки, вызывающие ошибки в общем и специальном программном обеспечении
- Средства реализации несанкционированного доступа к информации

Средства нарушения доступности информации

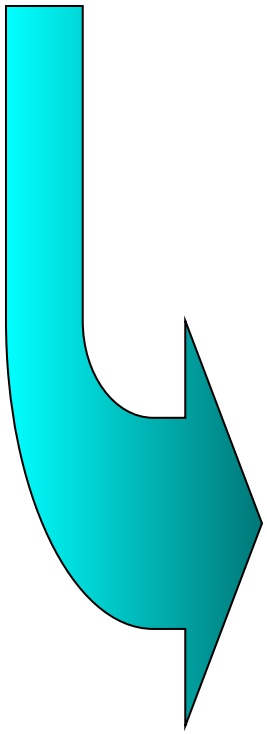
- Программно-аппаратные закладные устройства
- Спам-программы
- Закладки, вызывающие повышенный износ оборудования
- Закладки, вызывающие имитацию сбоев и нарушения в технических средствах
- Средства подавления информационного обмена в телекоммуникационных сетях

Основные направления деятельности государственной системы ТЗИ



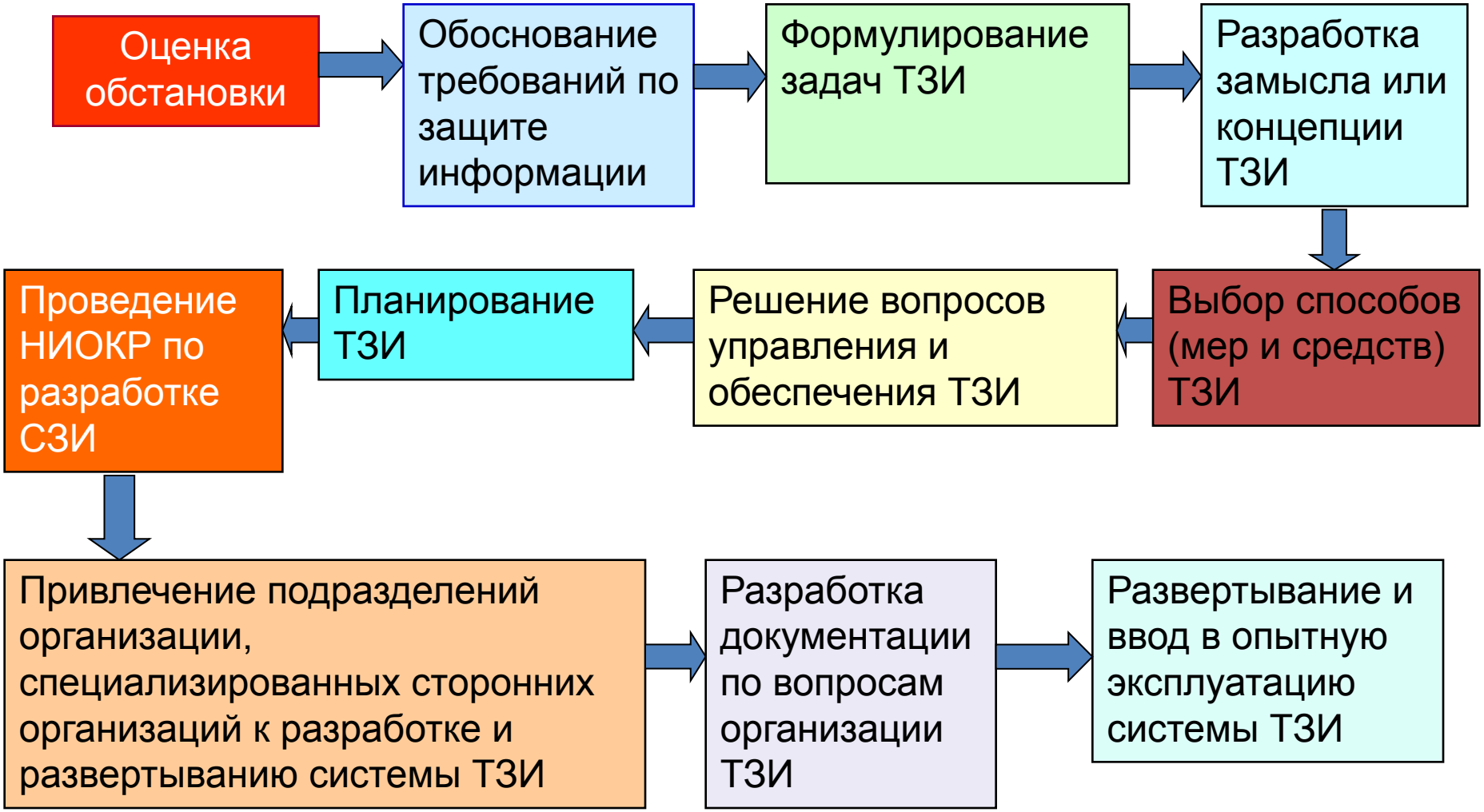
- Формирование системы документов и исходных данных по вопросам ТЗИ
- Разработка и обеспечение выполнения комплекса мер по ТЗИ
- Разработка и внедрение технических решений по ТЗИ
- Разработка средств ТЗИ и контроля
- Создание и применение информационных и автоматизированных систем управления в защищенном исполнении
- Лицензирование деятельности организаций
- Сертификация средств защиты информации
- Аттестация объектов информатизации на соответствие требованиям по безопасности
- Контроль состояния ТЗИ

Основные объекты защиты



- Вооружение и военная техника
- Военные объекты
- Объекты оборонно-промышленного комплекса
- Объекты органов государственного и военного управления
- Технологии оборонного назначения
- Объекты информационных систем
- Информационные ресурсы
- Органы государственной власти, органы местного самоуправления, организации, их деятельность, производимая в них продукция (работы и услуги) и возникающие при этом физические поля

Общий алгоритм организации ТЗИ на объекте информатизации

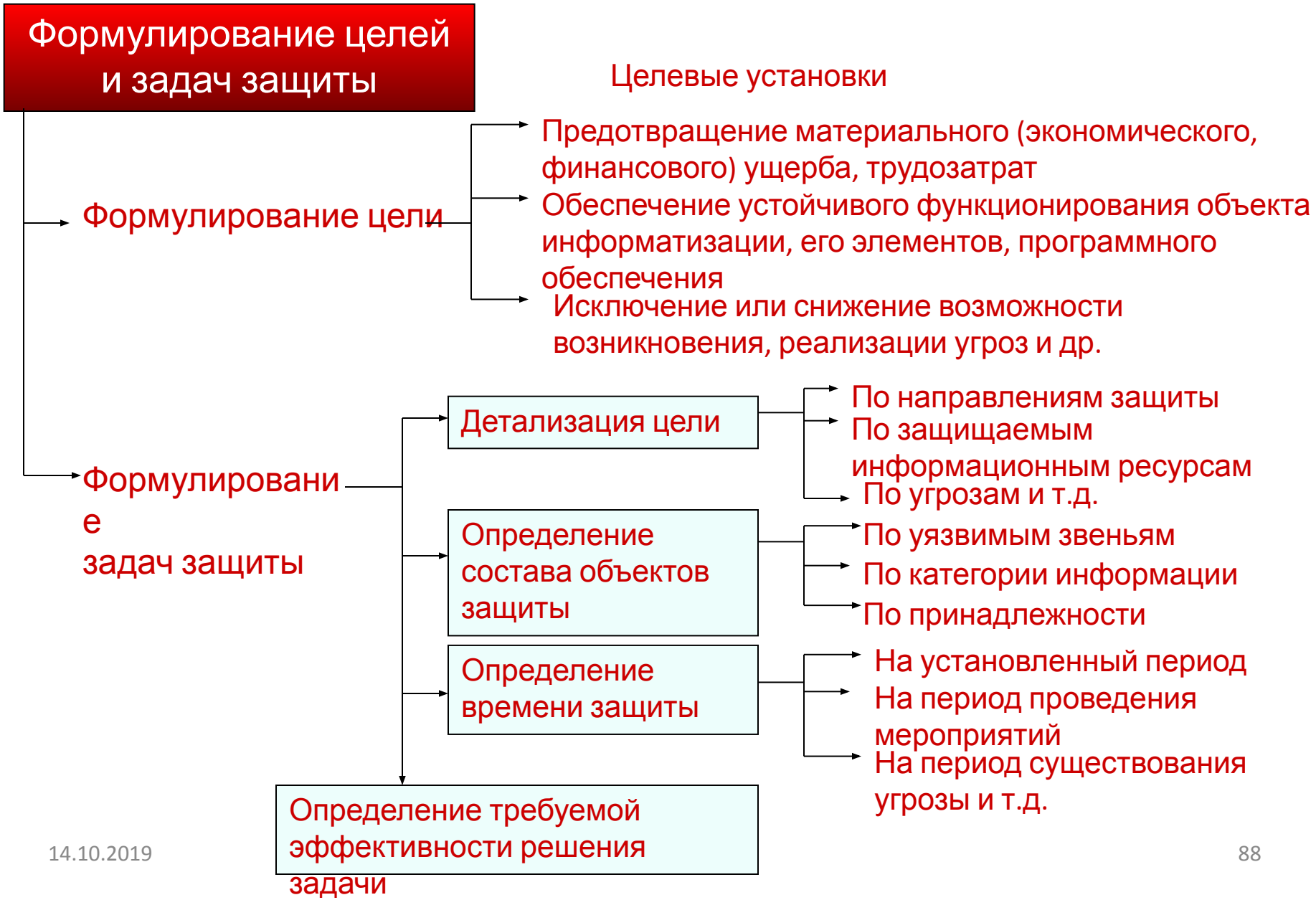


Порядок организации ТЗИ на этапе оценки обстановки

Оценка обстановки

- Анализ информационных ресурсов
  - Инвентаризация информационных и технических ресурсов
  - Категорирование информации по видам тайн и уровням конфиденциальности
  - Оценка времени устаревания информации
  - Определение условий допуска должностных лиц к информационным ресурсам и фактической их реализации
- Анализ уязвимых звеньев и возможных угроз безопасности информации
  - Оценка возможности физического доступа в помещения и к СВТ
  - Выявление возможных технических каналов утечки информации
  - Оценка возможности несанкционированного доступа к информации (непосредственного и удаленного)
  - Анализ возможностей программно-математического воздействия
  - Анализ возможностей непреднамеренного электромагнитного воздействия на информационные
  - Анализ возможности реализации угроз техногенного характера
  - Анализ рисков от реализации угроз
- Анализ имеющихся в распоряжении мер и средств защиты информации
  - По направлениям защиты: от физического доступа, от утечки по ТКУИ, от НСД, от ЭМИ, от техногенных угроз и др.

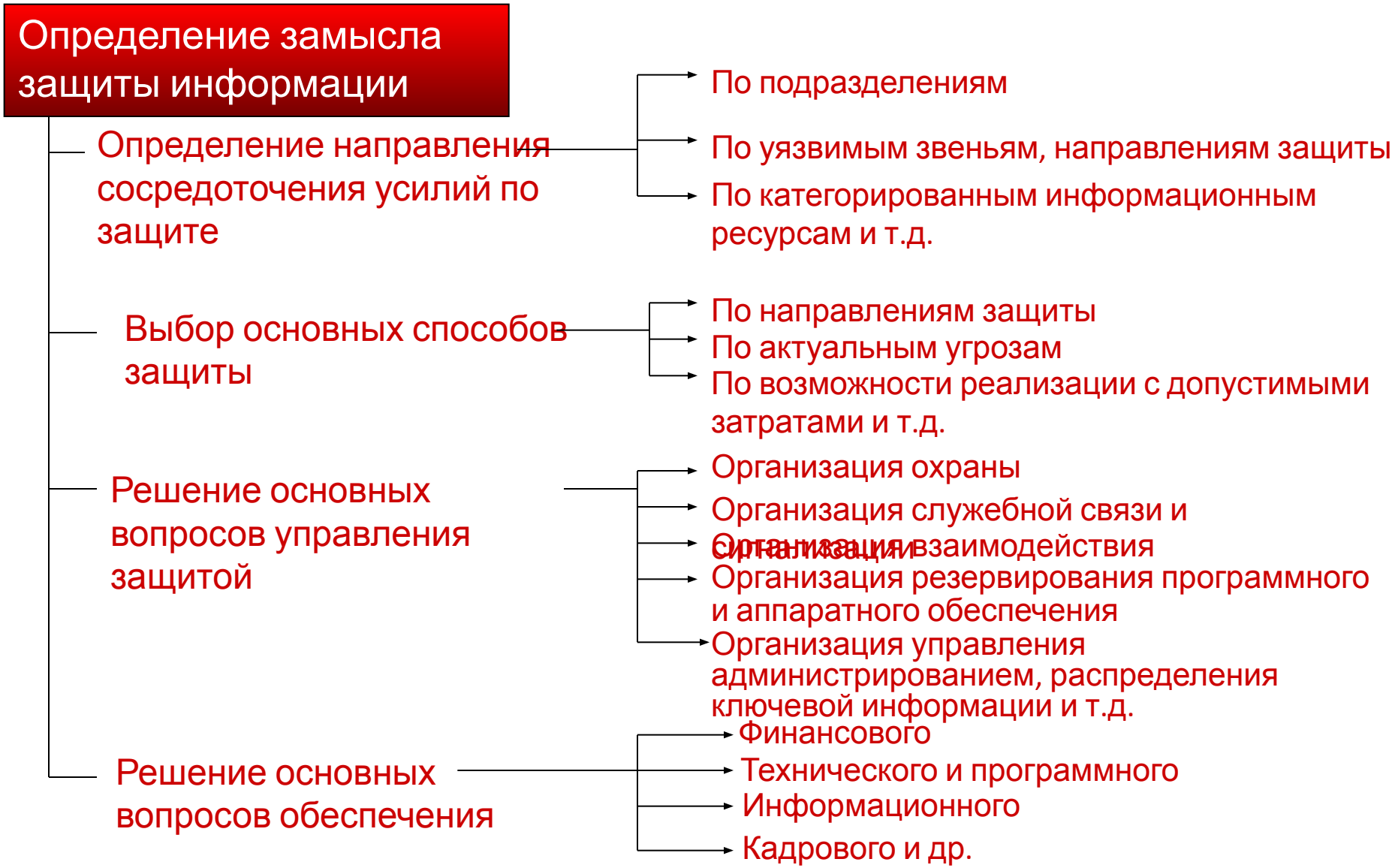
Порядок организации ТЗИ на этапе определения задач защиты



Содержание замысла защиты информации

- Цель защиты;
- Основные требования по ТЗИ, которые необходимо выполнить;
- Направления, на которых должны быть сосредоточены усилия по ТЗИ (элементы объекта информатизации, блоки защищаемой информации, угрозы, которые должны быть парированы в первую очередь);
- Целесообразные стратегии, основные способы защиты информации на объекте информатизации и контроля ее эффективности;
- Предложения по распределению задач ТЗИ между подразделениями организации, должностными лицами;
- Перечень программных и программно-аппаратных средств защиты и контроля, подлежащих применению, разработке (закупке);
- Основные вопросы управления, взаимодействия и обеспечения решения задач ТЗИ.

Порядок организации ТЗИ на этапе определения замысла защиты



Документы по организации ТЗИ на объекте информатизации

Утвержденный перечень сведений конфиденциального характера по каждому виду тайны

Акт и журнал инвентаризации информационных ресурсов

Акт категорирования защищаемой информации

Концепция ТЗИ на предприятии

Положение о порядке организации и проведения работ по защите конфиденциальной информации

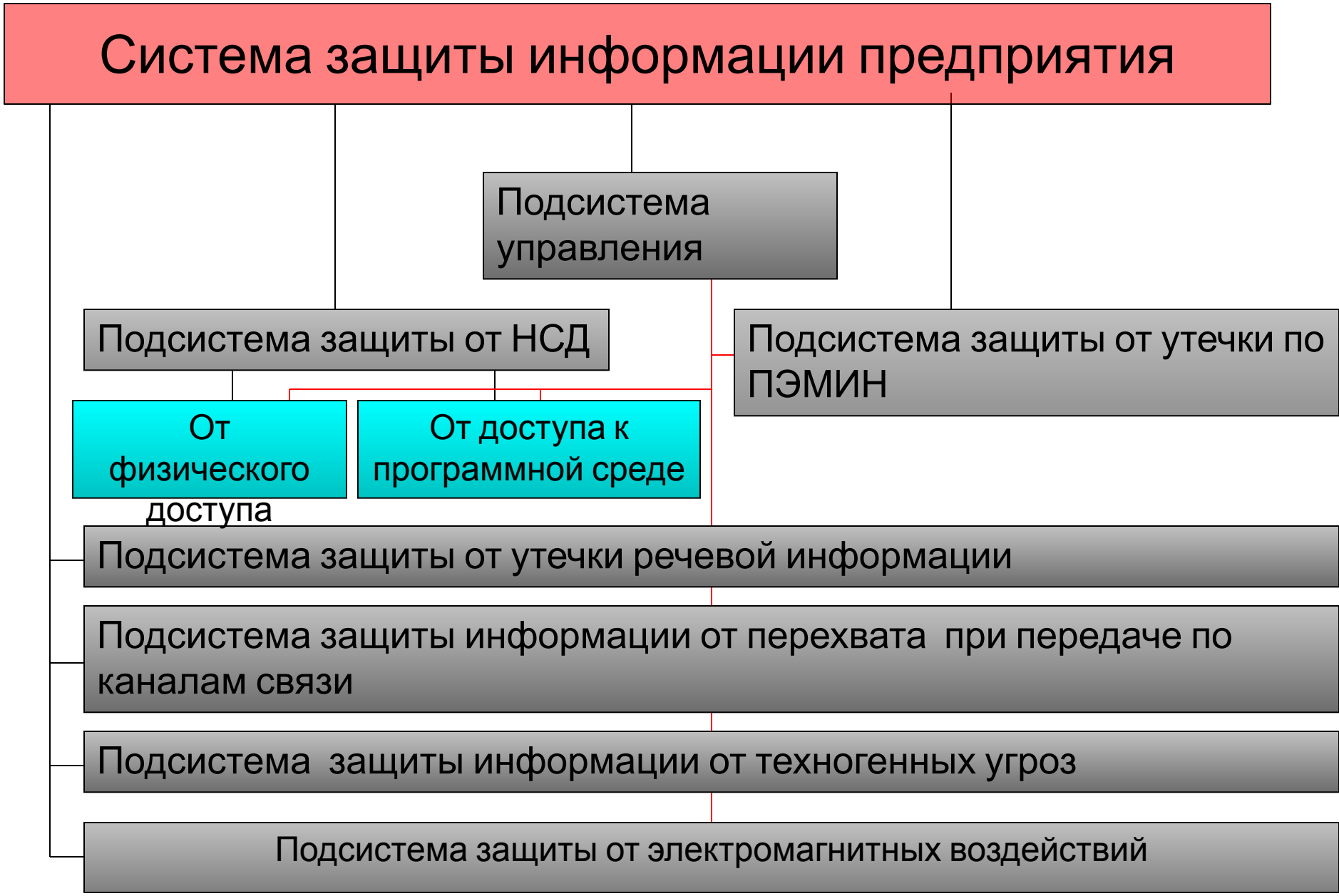
Модель угроз безопасности информации на объекте информатизации

План проведения мероприятий по ТЗИ на объекте информатизации

План обеспечения ТЗИ и взаимодействия

План или график проведения контрольных мероприятий

Система защиты информации предприятия



Подсистема защиты информации от НСД

Подсистема защиты от угроз физического доступа (контроля физического доступа)

Подсистема контроля доступа на территорию объекта и в помещения

- Подсистема охранной сигнализа-ции и наблюдения
- Автоматизи-рованные контрольно - пропускные пункты

Комплекс средств контроля и защиты от физического доступа к аппаратуре

- Комплекс средств контроля вскрытия аппаратуры
- Комплекс средств блокирования аппаратуры
- Средства учета и уничтожения носителей
- Комплекс средств физической аутентификации пользователей

Подсистема защиты от НСД к программной среде

- Комплекс программных и программно-аппаратных средств разграничения доступа (в том числе криптозащиты, межсетевого экранирования, построения VPN-сетей и др.)
- Программные средства блокирования несанкционированных действий, сигнализации и регистрации
- Подсистема защиты от программно-математического воздействия
- Средства повышения достоверности данных и надежности транзакций
- Средства архивирования, резервного копирования
- Программные средства обнаружения вторжений и сетевых атак

Подсистема защиты информации от утечки по ПЭМИН

- Комплекс пассивных средств
  - Средства локализации
    - Экранирование ТСПИ и соединительных линий
    - Заземление ТСПИ и экранов соединительных
  - Меры и средства развязывания информационных сигналов
    - Спецсредства защиты от микрофонного эффекта типа
    - Диэлектрические вставки
    - Автономные или стабилизированные источники электропитания, устройства гарантированного
    - Помехоподавляющие фильтры
- Комплекс активных средств
  - Пространственные средства
    - Генераторы шума и средства создания прицельных по частоте помех
    - Генераторы акустического шума (акустических и вибрационных помех)
    - Подавители диктофонов в режиме
  - Средства линейного
    - Для линий электропитания
    - Для посторонних проводников и линий ВТСС за пределами зоны
  - Специальные генераторы импульсов для уничтожения закладных устройств («выжигатели

Подсистема управления защитой информации

Организационная подсистема

- Подсистема управления физическим доступом
- Служба безопасности и система администраторов
- Подсистема организационного контроля

Техническая подсистема

- Программные средства администрирования
- АРМ администратора
- Технические средства регистрации и учета
- Подсистемы обнаружения атак, вторжений и ликвидации их последствий

Подсистема технического контроля

Стадии создания системы ТЗИ с проведением НИОКР

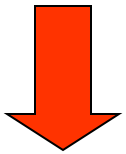
- **предпроектная стадия, включающую предпроектное обследование объекта информатизации, разработку аналитического обоснования необходимости создания СЗИ и технического (частного технического) задания на ее создание;**
- **стадия проектирования (разработки проектов), включающая разработку СЗИ в составе объекта информатизации;**
- **стадия ввода в действие СЗИ, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также аттестацию объекта информатизации на соответствие требованиям безопасности информации**

Предпроектная стадия - обследование объекта информатизации

- **устанавливается необходимость обработки (обсуждения) конфиденциальной информации на данном объекте информатизации;**
- **определяется перечень сведений конфиденциального характера, подлежащих защите;**
- **определяются (уточняются) угрозы безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования объекта;**
- **определяются условия расположения объекта информатизации относительно границ КЗ;**

Предпроектная стадия - обследование объекта информатизации (продолжение)

- определяются конфигурация и топология АС и систем связи в целом и их отдельных компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
- определяются технические средства и системы, предполагаемые к использованию в разрабатываемой АС и системах связи, условия их расположения, общесистемные и прикладные программные средства, имеющиеся на рынке и предлагаемые к разработке;
- определяются режимы обработки информации в АС в целом и в отдельных компонентах;



Предпроектная стадия - обследование объекта информатизации (продолжение)

- определяется класс защищенности АС;
- определяется степень участия персонала в обработке (обсуждении, передаче, хранении) информации, характер их взаимодействия между собой и со службой безопасности;
- определяются мероприятия по обеспечению конфиденциальности информации на этапе проектирования объекта информатизации.

Содержание аналитического обоснования необходимости создания СЗИ

- информационная характеристика и организационная структура объекта информатизации;
- характеристика комплекса основных и вспомогательных технических средств, программного обеспечения, режимов работы, технологического процесса обработки информации;
- возможные каналы утечки информации и перечень мероприятий по их устранению и ограничению;
- перечень предлагаемых к использованию сертифицированных средств защиты информации;
- обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации;
- оценка материальных, трудовых и финансовых затрат на разработку и внедрение СЗИ;
- ориентировочные сроки разработки и внедрения СЗИ;
- перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования объекта информатизации.

Содержание ТЗ на разработку СЗИ

- обоснование разработки;
- исходные данные создаваемого (модернизируемого) объекта информатизации в техническом, программном, информационном и организационном аспектах;
- класс защищенности АС;
- ссылка на нормативно-методические документы, с учетом которых будет разрабатываться СЗИ и приниматься в эксплуатацию объект информатизации;
- требования к СЗИ на основе нормативно-методических документов и установленного класса защищенности АС;
- перечень предполагаемых к использованию сертифицированных средств защиты информации;
- обоснование проведения разработок собственных средств защиты информации, невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения;

Состав оформляемых документов

На стадии ввода в действие объекта информатизации и СЗИ

- акты внедрения средств защиты информации по результатам их приемо-сдаточных испытаний;
- протоколы аттестационных испытаний и заключение по их результатам;
- аттестат соответствия объекта информатизации требованиям по безопасности информации.

Приказы, указания и решения:

- на проектирование СЗИ и назначение ответственных исполнителей;
- на проведение работ по защите информации;
- о назначении лиц, ответственных за эксплуатацию объекта информатизации;
- на обработку в АС (обсуждение в защищаемом помещении) конфиденциальной информации.

Содержание “Положения о порядке организации и проведения работ по защите конфиденциальной информации”

- порядок определения защищаемой информации;
- порядок привлечения подразделений организации, специализированных сторонних организаций к разработке и эксплуатации объектов информатизации и СЗИ, их задачи и функции на различных стадиях создания и эксплуатации объекта информатизации;
- порядок взаимодействия всех занятых в этой работе организаций, подразделений и специалистов;
- порядок разработки, ввода в действие и эксплуатацию объектов информатизации;
- ответственность должностных лиц за своевременность и качество формирования требований по защите информации, за качество и научно-технический уровень разработки СЗИ

Задание

1. Задаться гипотетическим или реально существующим объектом защиты. Построить для него пространственную модель объекта защиты.
2. Сформировать перечень защищаемой информации.
3. Оценить важность и ценность защищаемой информации информации.
4. Определить информационные процессы на предприятии.
5. Построить субъект-объектную и субъект-субъектную модели для определенного информационного процесса.
6. Определить защищаемый объект информатизации.
7. Определить контролируемую зону.
8. Проанализировать обстановку в сфере защиты информации, спланировать необходимые защитные меры и подготовить соответствующие документы.
9. Разработать и ввести в действие документы, регламентирующие организационно-правовые вопросы защиты информации. Как минимум, отразить обязанности о соблюдении конфиденциальности информации в трудовых и гражданско-правовых договорах, ввести за правило подписание соглашений о конфиденциальности при начале переговоров с партнерами.
10. Оформить обязательственные отношения по конфиденциальной информации с лицами, работающими по совместительству на других предприятиях, и с лицами, увольняющимися с предприятия.