Тема №1:
Общие положения по организации связи в СВ

Занятие №10:
Безопасность связи в условиях информационной войны

Учебные вопросы:

1. **Информационные войны**

2. **Безопасность связи в условиях информационных войн**

3. **Мероприятия по защите системы связи от ИТР**

Литература:

1. Наставление по связи в соединениях и воинских частях СВ. – М.: ВИ. 2013, с. 168-170, 177-179.

2. Основы организации связи в СВ. Часть 3. Основы организации связи в частях и подразделениях общевойсковых соединений. – С-Пб.: ВУС. 2003, с. 270-273.

Учебный вопрос №1

Информационные войны

Информационная война –

всеобъемлющая, целостная стратегия реализации информационно-психологического воздействия на противника, обусловленная все возрастающей значимостью и ценностью информации в вопросах командования, управления и политики

Цель ИВ – **обеспечение национальной безопасности за счет информационно-психологического воздействия на противостоящую сторону и защиты собственного информационного ресурса.**

На военном уровне:

Психологическая борьба

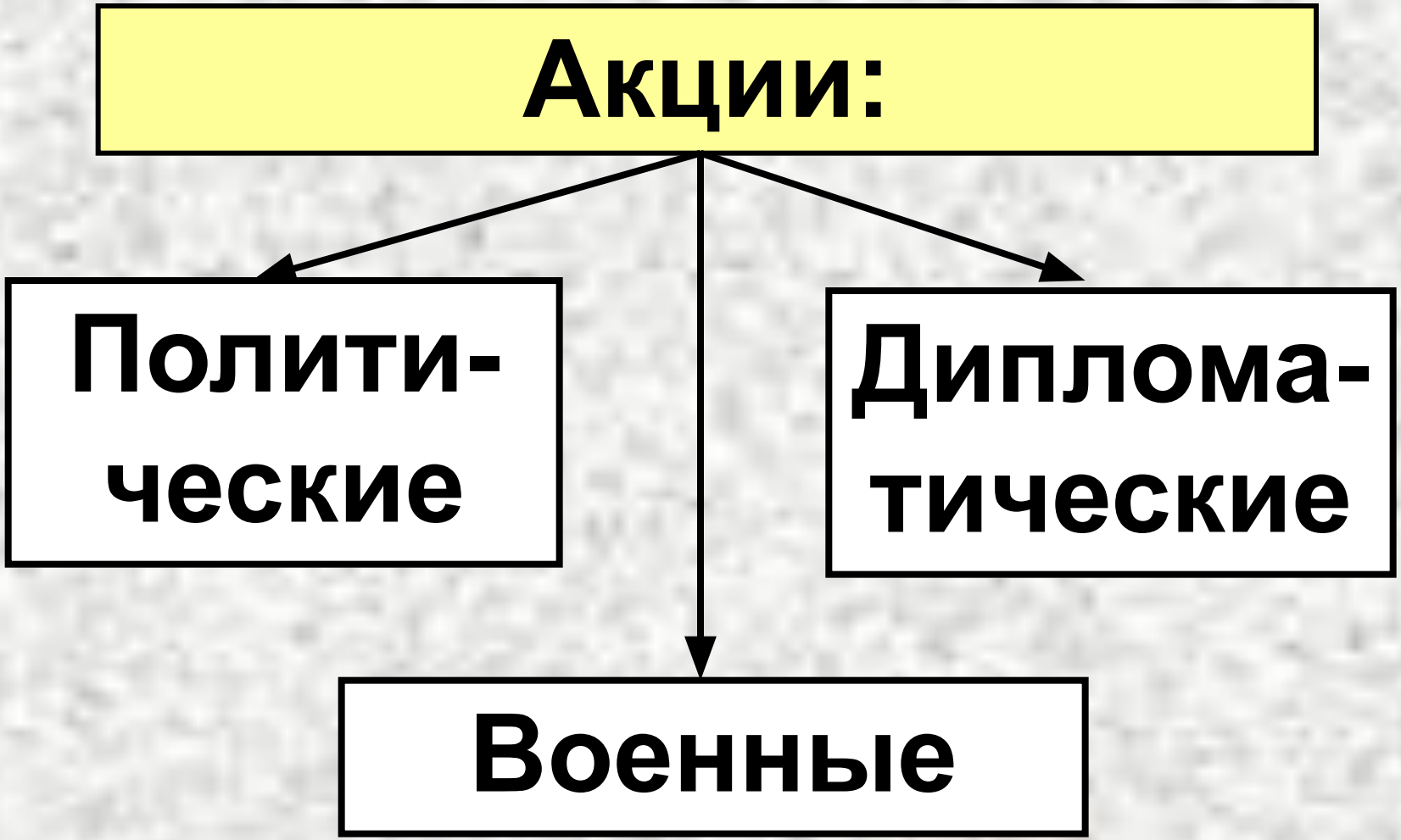
Введение противника в заблуждение

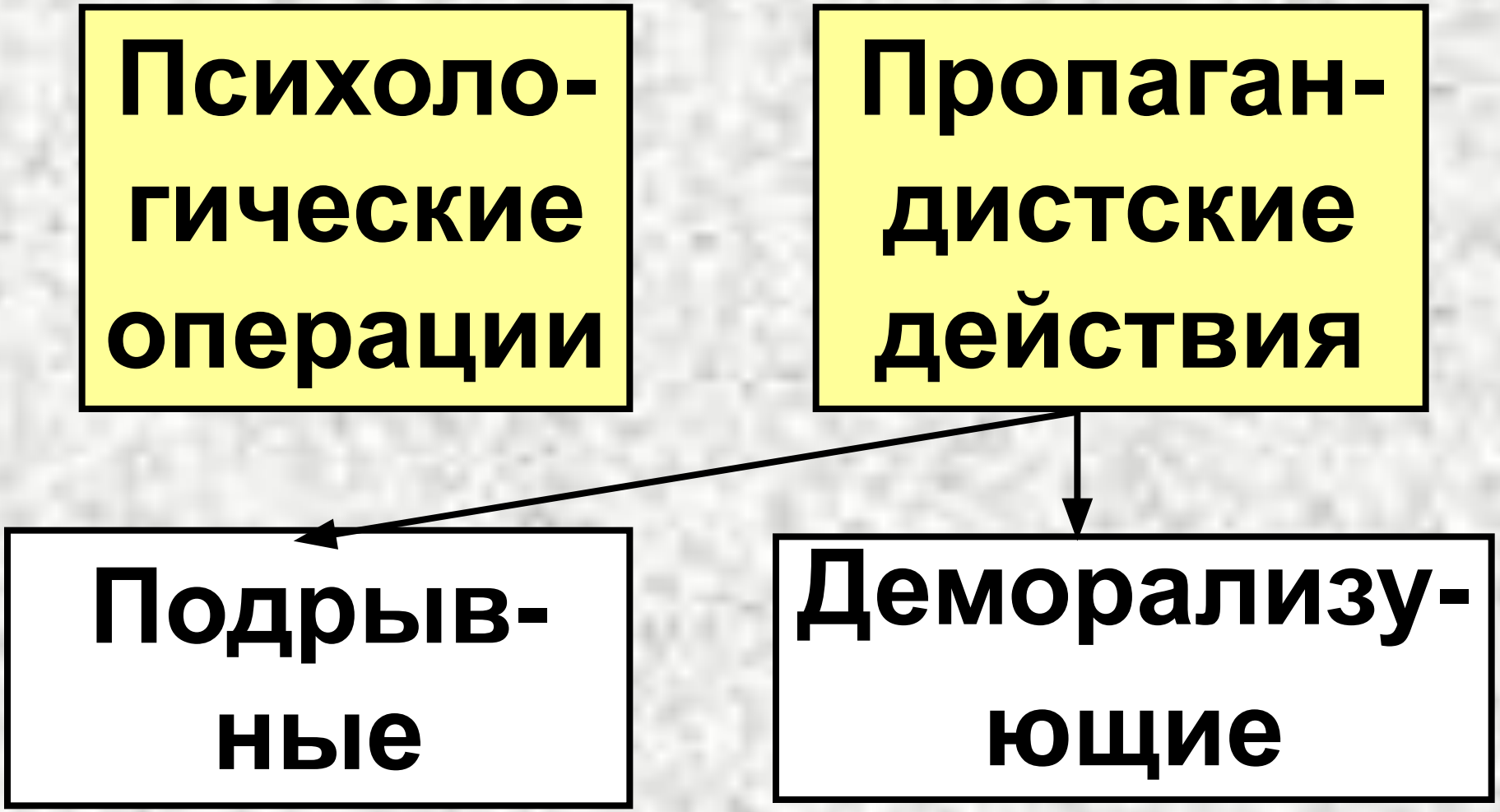
Противодействие разведке противника

РЭБ

Уничтожение ПУ и систем связи

Государственный уровень:




Психолого-гические операции
Пропаган-дистские действия
Подрыв-ные
Деморализу-ющие

Содействие

- Оппозицион-ным вижениям
- Диссидентским движениям

Оказание влияния

- На полити-ческую жизнь
- На культурную жизнь

Оборонительные средства ведения ИВ

Средства новой информационной инфраструктуры

Средства обеспечения безопасности информационной инфраструктуры

Средства информационного обеспечения

Средства информационно–психологического воздействия

Наступательные средства ведения ИВ

Средства информационно-психологического воздействия

Средства информационного воздействия

Средства активного воздействия

Средства ударно-огневого поражения

Учебный вопрос №2

Безопасность связи в условиях информационных войн

Безопасность связи - способность связи противостоять несанкционированному получению, уничтожению и (или) изменению информации, передаваемой (принимаемой, хранимой, обрабатываемой, отображаемой) с использованием технических средств связи и средств автоматизации управления, а также нарушению обмена информацией вследствие всех видов воздействий на систему связи и ее элементы.

Безопасность связи

Безопасность информации

Безопасность процесса передачи, обработки и хранения информации

Цель обеспечения БС:

предотвращение доступа разведки к информации, передаваемой по каналам связи, диверсионного ввода в СУ через систему связи ложной информации или уничтожения информации;

своевременное выявление и исключение каналов утечки информации, доступных разведке, поиск и ликвидация разведаппаратуры перехвата информации, устанавливаемой на линиях связи;

защиты связи, систем связи и АСУ от радиоэлектронной разведки всех видов и противодействия ей.

Организационные и технические мероприятия по обеспечению БС:

Применение способов ОС, систем паролирования и адресования, назначение радиоданных и установление режимов работы средств связи, обеспечивающих максимальную СУВ

Применение для передачи боевых приказов, распоряжений и другой важной информации наиболее защищенных от ИТР каналов связи

Ограничение объема информации, передаваемой различными средствами связи

Выполнение установленных контролируемых зон, а также пространственных, территориальных и временных ограничений в использовании средств связи различного назначения

Определение круга ДЛ, допущенных к использованию открытыми каналами связи

Сокращение времени работы средств связи на излучение

Ведение маскирующего радиообмена

Введение дополнительных ограничений на использование технических средств связи при появлении иностранных представителей, пролетах разведывательных космических и воздушных летательных аппаратов, появлении иностранных кораблей у государственных границ

Применение минимально необходимых мощностей, остронаправленных антенн и других мер, повышающих скрытность излучений

Соблюдение установленных режимов работы средств связи, требований СУВ и мер радиомаскировки

Исключение несанкционированного использования технических средств связи

Организация и осуществление контроля за безопасностью использования систем и средств связи

Выявление и устранение ДП в организации и использовании связи

Выявление и пресечение нарушений правил пользования аппаратурой ЗАС, требований СУВ, установленных режимом работы средств связи, мер радиомаскировки и режима секретности.

Учебный вопрос №3

Мероприятия по защите системы связи от ИТР

Защита системы, частей и подразделений связи – комплекс организационных и технических мероприятий, направленных на создание необходимых условий для развертывания, функционирования и наращивания системы связи в условиях огневого, ядерного и радиоэлектронного воздействия противника.

3.1. Классификация демаскирующих признаков линий связи

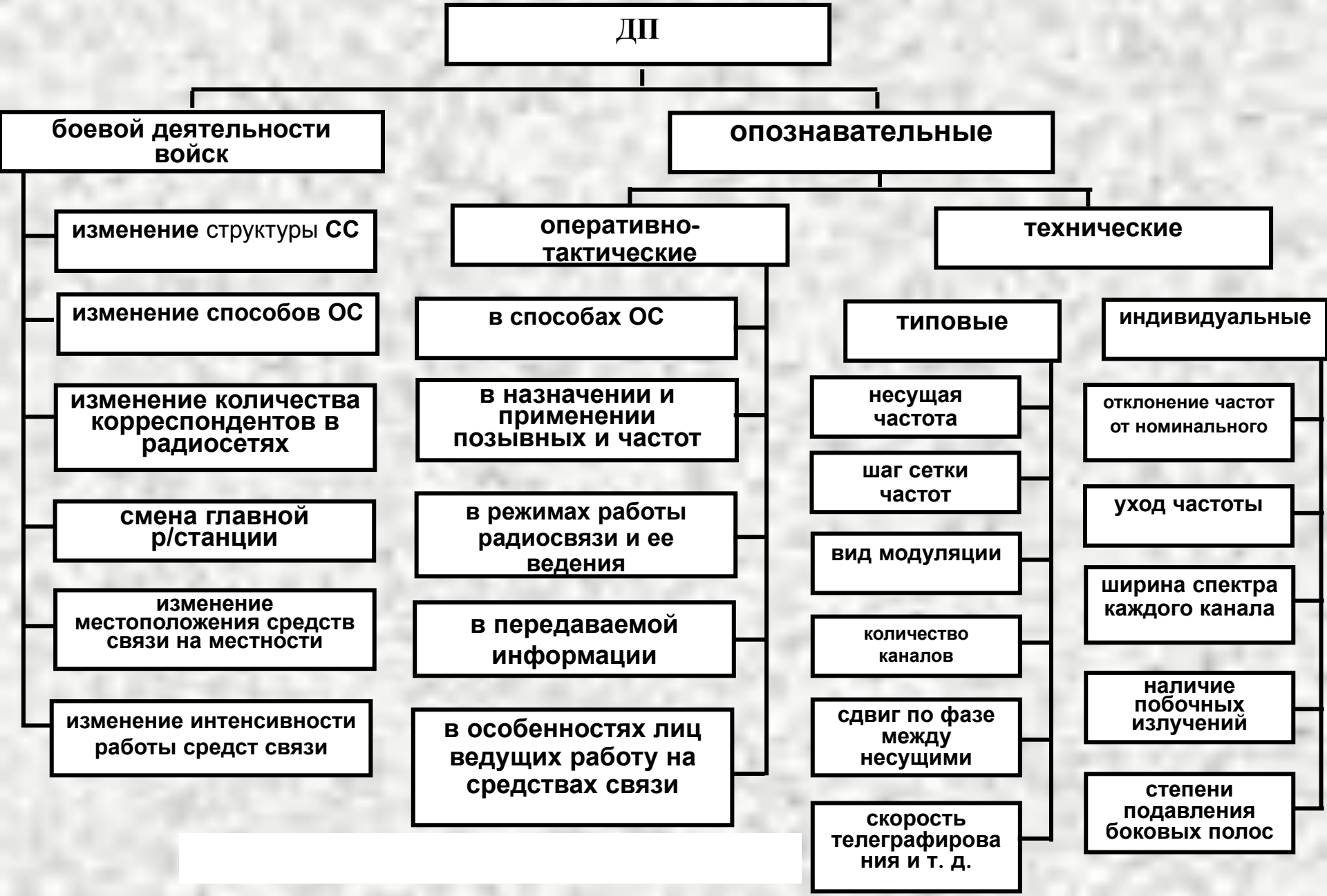
Разведывательный признак-

отличительная особенность объекта РР, которая может быть зафиксирована разведкой, использована для опознания объекта разведки или получения различной информации о нем.

Демаскирующие признаки (ДП) -

радиоразведывательный признак, который может быть использован для опознавания скрываемого объекта разведки или получения скрываемой информации от объекта разведки.

Классификация демаскирующих признаков



ДП боевой деятельности войск

– позволяют вскрыть изменение структуры СУ, изменение состава и размещения группировки войск, определить конкретные действия и намерения этой группировки в данной операционной обстановке.

ДП боевой деятельности войск ***являются***:

- изменение структуры СС
- изменение способов ОС
- изменение количества корреспондентов в радиосетях
- смена главной р/станции
- изменение местоположения средств связи на местности
- изменение интенсивности работы средст связи

Опознавательные ДП

позволяют определить принадлежность к виду ВС, звену управления, конкретному штату.

Оперативно-тактические

Технические

Оперативно-тактические – группа характеристик, средств, комплексов и систем связи, анализ и обработка которых позволяют вскрыть структуру СУ, ее принадлежность, замысел и характер боевой деятельности войск, определить принадлежность к виду ВС, звену управления, конкретному штату.

Они *проявляются*:

в способах ОС

в назначении и применении позывных и частот

в режимах работы радиосвязи и ее ведения

в передаваемой информации

в особенностях лиц ведущих работу на средствах связи.

Технические ДП – позволяют радиоразведке противника определить конкретный тип радиоэлектронных средств (РЭС) связи.

Типовые (групповые) технические ДП – позволяют определить принадлежность источника радиоизлучения к определенному виду РЭС.

К типовым *относятся*:

- номинальное значение несущей частоты;
- шаг сетки частот;
- вид модуляции;
- работа по одному и двум каналам;
- наличие ТФ каналов в частотном стволе;
- сдвиг по фазе между несущими при фазовой модуляции;
- скорость телеграфирования и т. д.

Индивидуальные технические ДП – дают возможность опознать конкретные образцы РЭС.

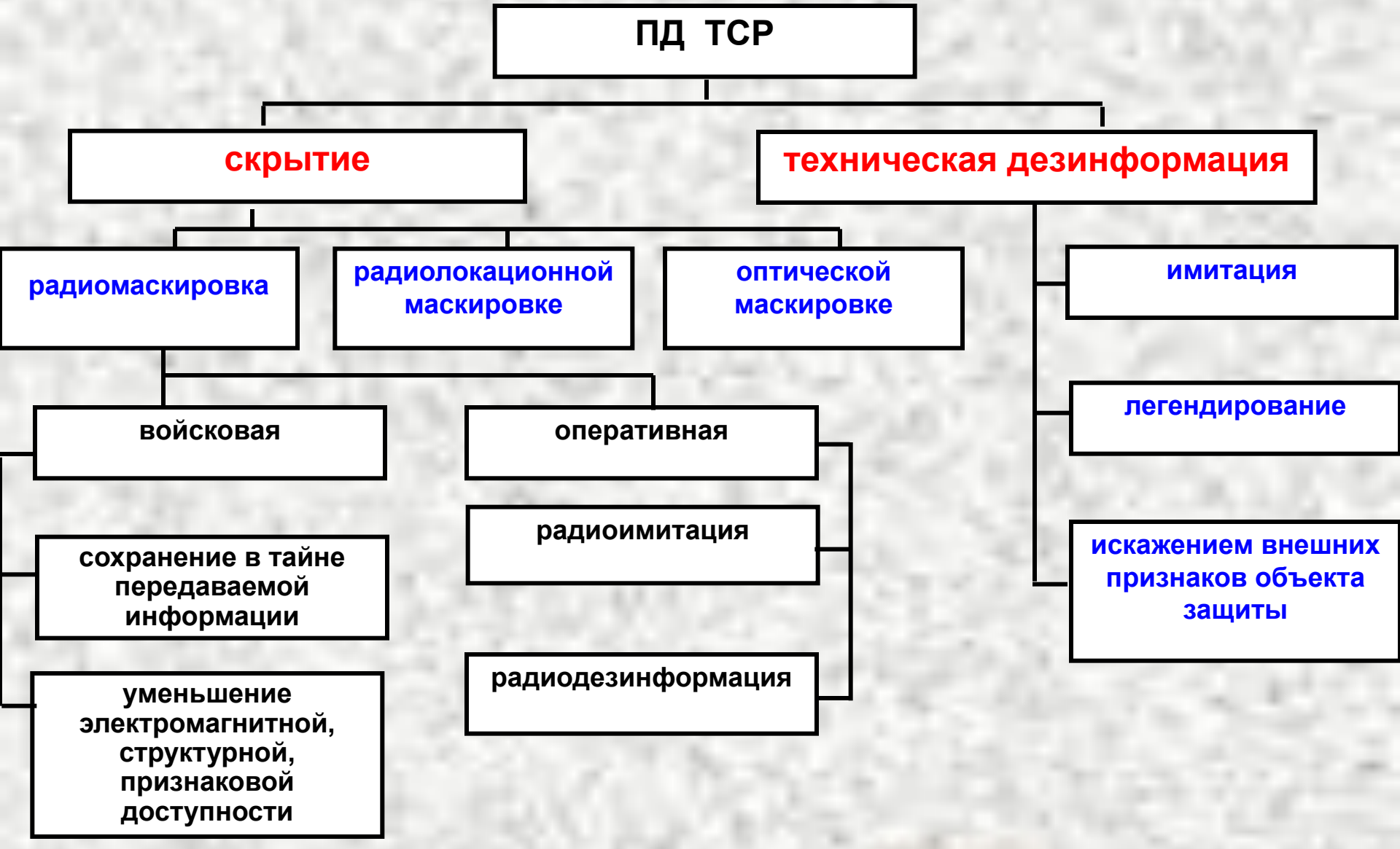
К индивидуальным *относятся*:

- отклонение частот от номинального значения;
- уход частоты (изменение за время сеанса связи);
- ширина спектра каждого канала;
- наличие и уровень побочных излучений;
- наличие и уровень сигнала, степени подавления боковых полос.

3.2. Защита системы связи от ИТР противника

Противодействие техническим средствам разведки (ПД ТСР) – совокупность мероприятий, проводимых с целью исключения или затруднения добывания противником с помощью ТСР сведений, составляющих военную и государственную тайну.

Противодействие техническим средствам разведки



Целью ПД ТСР *является*:

1. Лишение противника необходимой ему информации для поддержания его в полном или частичном неведении.

2. Введение противника в заблуждение путем создания условий для сбора противником ложной информации, получаемой различными видами и средствами разведки.

Скрытие:

это **устранение** или **искажение** ДП, раскрывающих охраняемые сведения, и **закрытие** возможных каналов утечки информации.

Радиомаскировка

Войсковая радиомаскировка – комплекс мероприятий, способствующих достижению **скрытности** связи.

Оперативная радиомаскировка – комплекс мероприятий проводимых с целью **скрытия от РР** противника или **введение его в заблуждение** в отношении истинных намерений, характера, замысла действия войск, их состояния и др. сведений.

Оперативная радиомаскировка

Радиоимитация **– создание ложной радиоэлектронной обстановки, отвечающей замыслам оперативной маскировки путем развертывания ложной системы связи.**

Радиодезинформация **– передача по каналам связи специально разработанной ложной информации с целью введения противника в заблуждение относительно истинных намерений наших войск.**

Радиолокационная маскировка

комплекс мероприятий направленных на снижение радиолокационного контраста объектов СС относительно фона окружающей местности.

Оптическая маскировка

комплекс мероприятий, проводимых для введения противника в заблуждение относительно состава, расположения, местонахождения, назначения и состояния объектов связи.

Техническая дезинформация

создание условий, существенно затрудняющих распознавание действительных объектов по данным разведки.

Имитация:

создание ложной обстановки (ложные УС, и т.д.), а так же демонстрация их действий.

Легендирование:

проведение мероприятий, искажающих представления разведки о характере, предназначения объектов, частей и их деятельности.

Искажение внешних признаков:

проведение мероприятий, искажающих или ликвидируют представления разведки о формах, структуре, расположении, перемещении объектов связи.

Выполнение задач ПД ТСР противника *достигается*:

проведением мероприятий по тактической маскировке;

высоким уровнем подготовки и бдительности л/с;

соблюдением установленных режимов работы средств связи;

организацией и контролем БС;

выбором способов организации связи;

сокращением времени работы средств на передачу;

работой р/средств с минимальной мощностью;

применением узконаправленных антенн;

использованием маскирующих свойств местности;

размещением излучающих средств за пределами УС;

сменой радиоданных;

применением маскирующего обмена;

соблюдением правил ведения связи;

выявлением и устранением демаскирующих признаков средств связи;

пресечением нарушений требований СУВ;

оповещением подразделений связи о появлении ТСР иностранных государств ;

контролем за выполнением мероприятий ПД ТСР противника;

инженерным оборудованием УС;

временными, частотными и др. ограничениями на применение средств связи;

скрытным перемещением подразделений связи;

ограничением всякого движения на УС;

определением угрозы безопасности использования сетевых ресурсов и обмена информацией.

3.3. Защита линий связи от радиоразведки противника

Снижение энергетической доступности *достигается*:

применением эквивалентов антенн, антенных насадок

выбором минимально необходимой мощности излучения

применением антенн с узконаправленными диаграммами направленности

работой в верхнем участке диапазона радиосредства

использованием защитных экранирующих свойств местности.

Уменьшение частотно-временной доступности *достигается*:

настройкой РЭС без выхода в эфир

работой РЭС на излучение только в момент передачи информации

повышением скорости передачи информации по радиолиниям

ограничение количества и ведение переговоров короткими, фразами.

Уменьшение признаковой доступности *достигается*:

обеспечением связи с использованием линейных позывных или без позывных

реализацией безквитанционных способов обмена

назначением общих групп ЗПЧ нескольким р/с, р/н и их поочередным использованием

осуществлением контроля за соблюдением порядка прохождения оперативной и маскирующей нагрузки

организация кабельных вставок на участках РРЛ, которые наиболее доступны радиоразведке противника

развертывание радиорелейных и тропосферных линий зигзагообразным образом

использование способа организа-ции связи через «посредника» или через ретранслятор.