Тема № 1. Информационное обеспечение современной вооруженной борьбы.

ЛЕКЦИЯ №2

Наступательная и оборонительная составные части информационного обеспечения (ИО). РЭБ - основной компонент ИО вооружённой борьбы.

Учебные цели:

1. Рассмотреть и изучить сущность наступательной и оборонительной компонент информационного обеспечения.
2. Дать определение РЭБ и её составным частям.
3. Изучить цели и задачи РЭБ, принципы организации и ведения РЭБ.

План лекции:

Введение.

1. Наступательная и оборонительная составные части ИО.
2. РЭБ – основной компонент ИО вооружённой борьбы. Определение РЭБ и её составные части.
3. Цели, принципы организации и ведения РЭБ.

Литература

1. Наставление по обеспечению боевых действий. Радиоэлектронная борьба. Утверждено Приказом начальника Генерального штаба ВС - первым заместителем Министра обороны РБ 30.11.2015.
2. Гордей В.В., Ляшук Г.Д., Митянов И.В., Ржевусский В.Л. Основы иформационного обеспечения и радиоэлектронной борьбы. Основы радиоподавления радиосвязи. Учебное пособие. - Мн.: ВАРБ, 2006.
3. А.А. Фирсаков, А.Е. Жучковский. Основы информационного обеспечения и радиоэлектронной борьбы. Курс лекций. - Мн.: ВАРБ, 2005.

Введение.

Информационное обеспечение включает в себя:

1. Информационное воздействие.
2. Защиту от аналогичного информационного воздействия противника.
3. Информационно-аналитическое обеспечение воздействия и защиты.

Из них две составные части являются основными:

- наступательная (активная);
- оборонительная (защитная).

1. Наступательная и оборонительная составляющие информационного обеспечения

1.1. Наступательная (активная) составляющая информационного обеспечения

Наступательная (активная) составляющая ИО - информационное воздействие - *согласованный по целям, задачам, месту и времени комплекс мероприятий по:*

- **комплексному воздействию** на **информацию**;
- **программному и электронному воздействию** на **информационно-технические объекты**;
- **информационно психологическому воздействию** на **информационно-психологические объекты**.

Наступательная (активная) составляющая информационного обеспечения – информационное воздействие

Информационное оружие - это устройства и средства, предназначенные для нанесения противоборствующей стороне максимального урона в ходе информационного противоборства путем опасных информационных воздействий

ФОРМЫ ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ

Информационная операция	совокупность согласованных и взаимосвязанных по целям, задачам, месту и времени информационных действий и акций, проводимых по единому замыслу и плану в интересах создания условий для обеспечения военной безопасности государства, подготовки и ведения стратегических действий (операций) Вооруженных Сил
Информационные действия	совокупность согласованных и взаимосвязанных по цели, задачам, месту и времени информационных акций для решения нескольких последовательно возникающих задач
Информационная акция	ограниченное по масштабу и времени информационное воздействие для решения, как правило, одной задачи
Информационный удар	одновременное кратковременное информационно-психологическое, программное, электронное и физическое воздействие на группу информационных объектов
Информационная атака	однократное информационное и физическое воздействие на одиночный информационный объект

Средства наступательной составляющей информационного обеспечения

- **Техника радиоподавления**
  - Радиосвязи
  - Бортовых и наземных РЛС
  - Навигационной аппаратуры
- Оружие, наводящееся на излучение радиоэлектронных средств
- **Средства дезинформации**
  - Электронные средства массовой информации
  - Средства связи для осуществления дезинформации
- Специалисты информационного воздействия в компьютерных сетях
- Компьютерные вирусы

1.2. Оборонительная (защитная) составляющая информационного обеспечения

Оборонительная (защитная) составляющая ИО - защита от информационного воздействия - *согласованный по целям, задачам, месту и времени комплекс мероприятий, направленных на нейтрализацию или снижение эффективности*

- программного и электронного воздействия *на* **информационно-технические объекты**,

- информационно-психологического воздействия *иностранных государств, а также на*

- защиту собственной **информации.**

Оборонительная (защитная) составляющая информационного обеспечения – защита от информационного воздействия

Мероприятия по защите информации и информационных объектов от воздействия иностранных государств.

Защита информации, защита от программного и электронного воздействия

Мероприятия по радиоэлектронной защите (РЭЗ)

Мероприятия по (ПД ТСР) противодействию техническим средствам разведки противника

Защита РЭС от РРТР

Мероприятия по радиоэлектронной защите (РЭЗ) - обеспечение работы радиоэлектронных средств (РЭС) управления войсками и оружием)

При ведении РЭБ противником

Защита РЭС от радиоподавления

Защита РЭС от возд. сильных изл.

Защита РЭС от поражения СНО и ВТО

При возникновении помех между своими РЭС

Обеспечение электромагнитной совместимости (ЭМС) РЭС

Технические мероприятия

Организационные мероприятия

Мероприятия по противодействию техническим средствам разведки (ПД ТСР)

Уменьшение семантической доступности - защита содержания передаваемой информации путем ее скрытия от РР противника

Уменьшение энергетической, пространственной, частотной , временной и структурной доступности - скрытие радиоизлучений и их структур

Уменьшение структурной и признаковой доступности системы управления - устранение демаскирующих признаков

Применение аппаратуры автоматического закрытия и обеспечение ее безопасности

Шифрование или кодирование передаваемой оперативной или служебной информации

Сокращение количества открытых связей для управления подразделениями и ограничение круга лиц, имеющих право пользования ими

Соблюдение требований скрытого управления войсками, правил пользования аппаратурой закрытия, установления и ведения связи

Выявление и пресечение нарушений требований скрытого управления войсками и безопасности связи

2. РЭБ – основной компонент ИО вооружённой борьбы. Определение РЭБ и её составные части.

Радиоэлектронная борьба (далее – РЭБ) – совокупность согласованных по целям, задачам, месту и времени мероприятий и действий войск (сил) по радиоэлектронному поражению радиоэлектронных объектов систем управления войсками (силами) и оружием противника, радиоэлектронной защите своих радиоэлектронных объектов систем управления войсками (силами) и оружием.

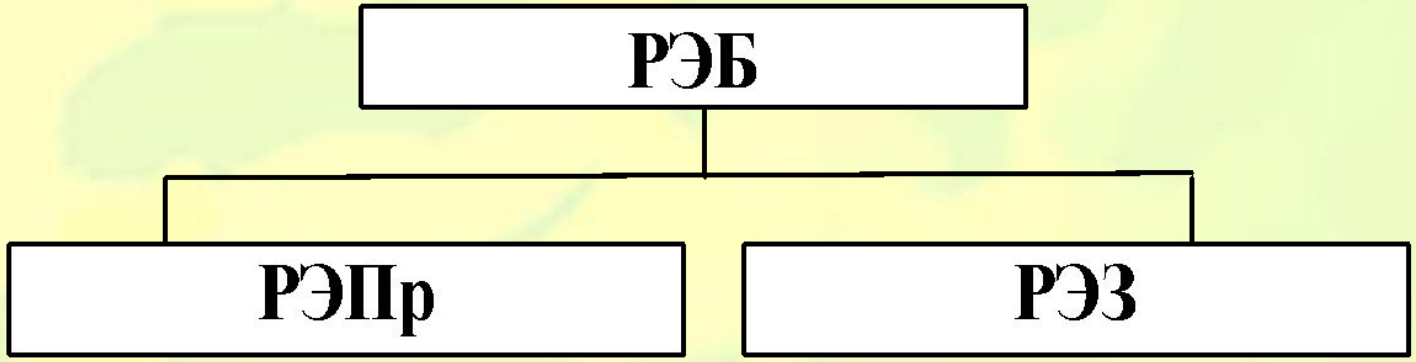
В операциях и боевых действиях РЭБ является одним из основных видов оперативного (боевого) обеспечения.

Объектами РЭБ являются радиоэлектронные объекты систем управления войсками (силами) и оружием

Под **радиоэлектронным объектом** понимается совокупность радиоэлектронных средств (далее – РЭС), используемых для управления войсками (силами) и оружием, ведения разведки и РЭБ, размещенных на одном пункте управления (далее – ПУ), в определенном районе или на отдельном боевом средстве.

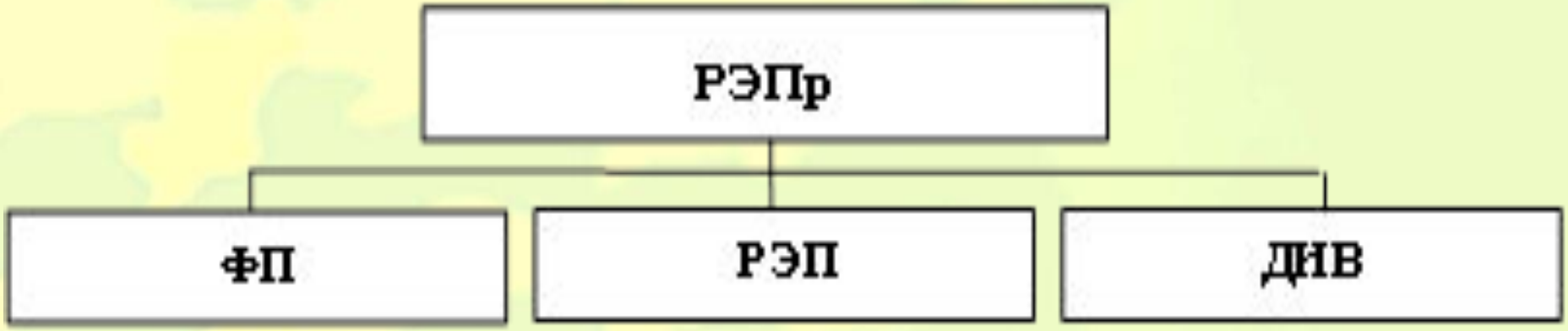
РЭБ организуется и ведется в целях дезорганизации управления войсками (силами) противника, снижения эффективности применения его оружия, боевой техники и РЭС, а также для обеспечения устойчивости работы систем управления своими войсками (силами) и оружием.

РЭБ осуществляется в тесном сочетании с огневым поражением (захватом, выводом из строя) основных объектов систем управления войсками (силами) и оружием противника, другими видами оперативного (боевого) обеспечения (разведка, маскировка…) и включает в себя две составные части:.



В вооруженных силах США РЭБ рассматривается как особый вид боевых действий за«завоевание превосходства в эфире».

1. РЭПр – составная часть РЭБ, представляющая собой совокупность мероприятий и действий войск (сил) по воздействию на радиоэлектронные объекты систем управления войсками (силами) и оружием противника средствами **функционального поражения**, **радиоэлектронного подавления** (далее – РЭП) и **дезинформирующего воздействия** (далее – ДИВ).



1.1 **ФП** – вид РЭПр, заключающийся в разрушении (повреждении) элементов и узлов радиоэлектронных объектов противника путем поражения электромагнитным излучением (далее – ЭМИ) или самонаводящимся на излучение оружием (далее – СНО).

1.1.1 **Поражение ЭМИ** заключается в разрушении (повреждении) элементов и узлов радиоэлектронных объектов противника специальными средствами с мощными излучениями различных диапазонов частот.

1.1.2 **Поражение СНО** заключается в уничтожении, выводе из строя, повреждении радиоизлучающих устройств радиоэлектронных объектов противника путем применения авиационных, ракетно-артиллерийских систем и средств.

1.2 РЭП – основной вид РЭПр, заключающийся в снижении качества функционирования радиоэлектронных объектов систем управления войсками (силами) и оружием противника путем воздействия на приемные устройства РЭС мешающими ЭМИ (далее – радиоэлектронные помехи).

Целями радиоэлектронных помех являются РЭС радиосвязи, разведки, управления оружием и навигации, подлежащие РЭП в соответствии с замыслом (планом) операции (боевых действий).

В зависимости от используемого диапазона частот (длины волн) РЭП включает в себя радиоподавление (далее – РП) и оптико-электронное подавление.

1.2.1 Радиоподавление (далее – **РП**) заключается в нарушении работы радио-, радиорелейных, тропосферных и спутниковых средств связи, средств радиолокации и радионавигации, радиовзрывателей артиллерийских снарядов противника путем воздействия на их приемные устройства мешающими ЭМИ в диапазоне радиоволн (далее – радиопомехи).

1.2.2 Оптико-электронное подавление (далее – **ОЭП**) заключается в нарушении работы инфракрасных, тепловизионных, телевизионных, лазерных и оптико-визуальных средств разведки, наблюдения, связи и управления оружием путем воздействия на их приемные устройства мешающими ЭМИ в оптическом диапазоне волн (далее – оптические помехи).

Для РЭП РЭС противника применяются комплексы и средства активных радиоэлектронных помех, состоящие на вооружении в наземных воинских частях и авиационных подразделениях РЭБ, а также устанавливаемые на военной технике или забрасываемые передатчики помех (далее – ЗПП).

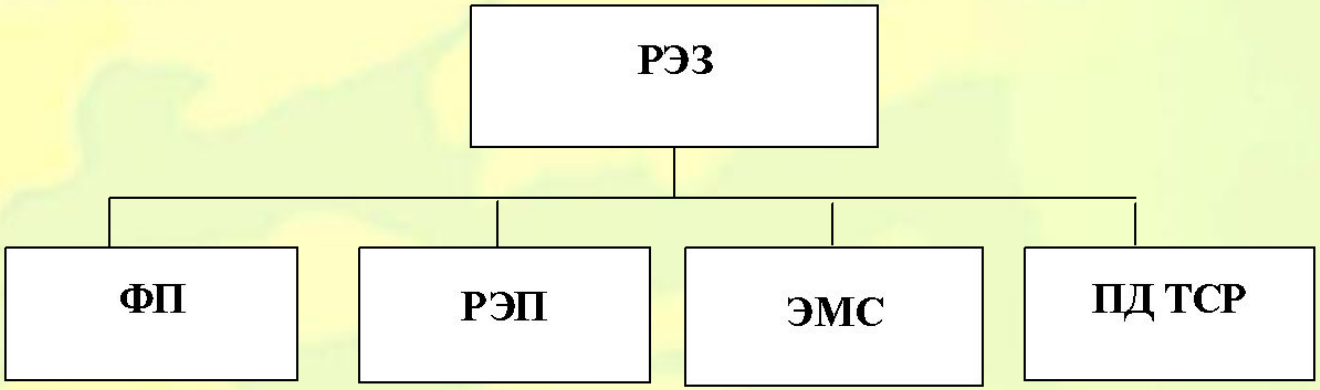
1.3 **ДИВ – вид РЭПр, заключающийся во внесении информационно-управляющих ошибок в системы управления оружием (боевыми средствами) противника путем воздействия на их радиоэлектронные объекты специальными дезинформирующими радиосигналами.**

Способами ДИВ являются радиоэлектронная симуляция и радиоэлектронная имитация.

1.3.1 **Радиоэлектронная симуляция** (далее – РэС) заключается в воспроизведении средством ДИВ характеристик сигналов и режимов работы РЭС в сети радиосвязи (РНС) противника с целью внесения ложной информации о принадлежности средства ДИВ этой же сети (РНС).

1.3.2 **Радиоэлектронная имитация** (далее – РэИ) заключается в воздействии средством ДИВ на РЭС противника специальными радио- и (или) оптическими сигналами, имитирующими структуру полезных сигналов с целью внесения в РЭС противника ложной информации о радиоэлектронных объектах своих войск (сил) (их типе, количестве, местонахождении, параметрах движения).

2. РЭЗ – составная часть РЭБ, представляющая собой совокупность мероприятий и действий войск (сил) по устранению (ослаблению) воздействия на свои радиоэлектронные объекты средств **ФП и РЭП** противника, защите своих РЭС от непреднамеренных радиоэлектронных помех (обеспечению их электромагнитной совместимости (далее – **ЭМС**)) и противодействию техническим средствам разведки (далее – **ПД ТСР**)



В целях обеспечения РЭЗ в войсках проводятся организационные мероприятия и принимаются технические меры.

2.1 **Защита от средств ФП** противника включает в себя защиту РЭС от ЭМИ и защиту средств управления от поражения СНО.

2.2 **Защита от РЭП** противника включает в себя защиту от активных и пассивных помех.

2.3 **Защита от непреднамеренных радиоэлектронных помех** (обеспечение ЭМС своих РЭС) достигается проведением организационных мероприятий и принятием технических мер, направленных на снижение (исключение) взаимного влияния РЭС при их совместном применении

2.4 **ПД ТСР** – совокупность организационных и технических мероприятий, проводимых с целью исключения или существенного затруднения добывания разведками с помощью технических средств достоверных сведений об объектах защиты, а также проводимых в штабах (организациях), войсках мероприятиях, составляющих государственные секреты.

3. Успешное решение **задач РЭПр** радиоэлектронных объектов систем управления противника и **РЭЗ** радиоэлектронных объектов своих войск достигается проведением мероприятий и действий войск (сил) сбору, анализу и обобщению данных радиоэлектронной обстановки (далее – РЭО), необходимых для организации и ведения РЭБ.

3.1 **РЭО** – совокупность данных, характеризующих положение, состояние, возможности и характер действий радиоэлектронных объектов систем управления войсками (силами) и оружием, разведки и РЭБ, а также параметры различных излучений искусственного и естественного происхождения в заданном районе в определенный промежуток времени.

3.2 **Сбор, анализ и обобщение данных РЭО** являются важнейшей задачей всех органов военного управления и осуществляются непрерывно в мирное время, период нарастания военной угрозы, при подготовке и в ходе ведения операции (боевых действий) для эффективного ведения РЭБ. В целях выполнения этой задачи используются все возможные источники получения

Основным способом выявления радиоэлектронных объектов противника является радиоэлектронная разведка (далее – РЭР).

3.2 РЭР включает в себя радио-, радиотехническую, радиолокационную, оптико-электронную разведки и подразделяется на **общую** и **непосредственную** (исполнительную).

3.2.1 **Общая РЭР** ведется соединениями (воинскими частями) разведки видов Вооруженных Сил, родов войск и специальных войск в целях обеспечения командующих и начальников штабов данными о РЭО, необходимыми для организации и ведения РЭБ в операциях (боевых действиях).

3.2.2 **Непосредственная (исполнительная) РЭР** ведется силами воинских частей (подразделений) РЭБ в целях добывания данных и уточнения сведений о технических характеристиках и режимах работы РЭС, линий (каналов) связи противника, являющихся объектами РЭПр. Данные непосредственной (исполнительной) РЭР используются для целераспределения, наведения и выбора способов применения средств ФП, режимов работы средств и комплексов РЭП.

4. Цели РЭБ определяются в соответствии с замыслом операции (боевых действий) и достигаются выявлением радиоэлектронных объектов систем управления войсками (силами) и оружием противника, их радиоэлектронным поражением (далее – РЭПр), а также радиоэлектронной защитой своих РЭС систем управления войсками (силами) и оружием.

5. Успех при ведении РЭБ достигается: соответствием целей и решаемых задач РЭБ замыслу операции (боевых действий), характеру действий противника; всесторонней подготовкой войск и средств РЭБ к выполнению задач РЭБ в операциях (боевых действиях); своевременным и полным обеспечением органов управления и воинских частей РЭБ данными РЭО; рациональным построением группировки сил и средств РЭБ; применением разнообразных способов выполнения задач РЭБ; согласованием действий и мероприятий по РЭБ с действиями соединений и воинских частей родов войск и специальных войск по дезорганизации управления противника, РЭЗ своих войск и объектов; своевременным и быстрым маневром (перенацеливанием) воинскими частями и средствами РЭБ с учетом реально складывающейся и прогнозируемой оперативной обстановки и РЭО; организацией обмена информацией с воинскими частями радио- и радиотехнической разведки; осуществлением мероприятий по обеспечению устойчивого управления, надежной защиты, охраны и обороны воинских частей РЭБ, всестороннему обеспечению их действий, а также своевременным восстановлением их боеспособности.

3. Цели, принципы организации и ведения РЭБ.

Цели РЭБ определяются в соответствии с замыслом операции (боевых действий) и достигаются выявлением радиоэлектронных объектов систем управления войсками (силами) и оружием противника, их радиоэлектронным поражением (далее – РЭПр), а также радиоэлектронной защитой своих РЭС систем управления войсками (силами) и оружием.

Успех при ведении РЭБ достигается:

1. Своевременным добыванием разведданных о РЭС и СУ В и О противника.
2. Надежным поражением их или выводом из строя.
3. Быстрой и скрытой подготовкой сил и средств РЭБ к боевому применению, умелым их распределением по направлениям и задачам, своевременным быстрым маневром (перенацеливанием) с учетом сложившейся обстановки.
4. Устойчивым управлением частями РЭБ, их четким и непрерывным взаимодействием с частями Р и РТР.
5. Умелой организацией и непрерывным осуществлением всеми родами войск (сил) и специальными войсками мероприятий по РЭЗ и комплексному ПД ТР.

6. Основными принципами РЭБ являются: целеустремленность, активность, внезапность, массированное и комплексное применение воинских частей (подразделений), непрерывность и оперативность.

7. Эффективность РЭБ в операциях (боевых действиях) **определяется** ее вкладом в дезорганизацию управления войсками (силами) и оружием противника, обеспечение устойчивого функционирования своих РЭС аналогичных систем и **оценивается** следующими степенями дезорганизации управления противника:

7.1 Срыв управления достигается уничтожением (выводом из строя) не менее 50-60% наиболее важных ПУ и радиоэлектронных объектов системы управления войсками (силами) и оружием противника и РЭП не менее 75% его сохранившихся важных РЭС.

7.2 Нарушение управления достигается уничтожением (выводом из строя) не менее 30-50% наиболее важных ПУ и радиоэлектронных объектов системы управления войсками (силами) и оружием противника и РЭП не менее 50% его сохранившихся важных РЭС.

7.3 Затруднение управления достигается уничтожением (выводом из строя) не менее 15-30% наиболее важных ПУ и радиоэлектронных объектов системы управления войсками (силами) и оружием противника и РЭП не менее 30% его сохранившихся важных РЭС.

Основными принципами РЭБ являются: целеустремленность, активность, внезапность, массированное и комплексное применение воинских частей (подразделений), непрерывность и оперативность.

Эффективность РЭБ оценивается следующими степенями дезорганизации управления противника:

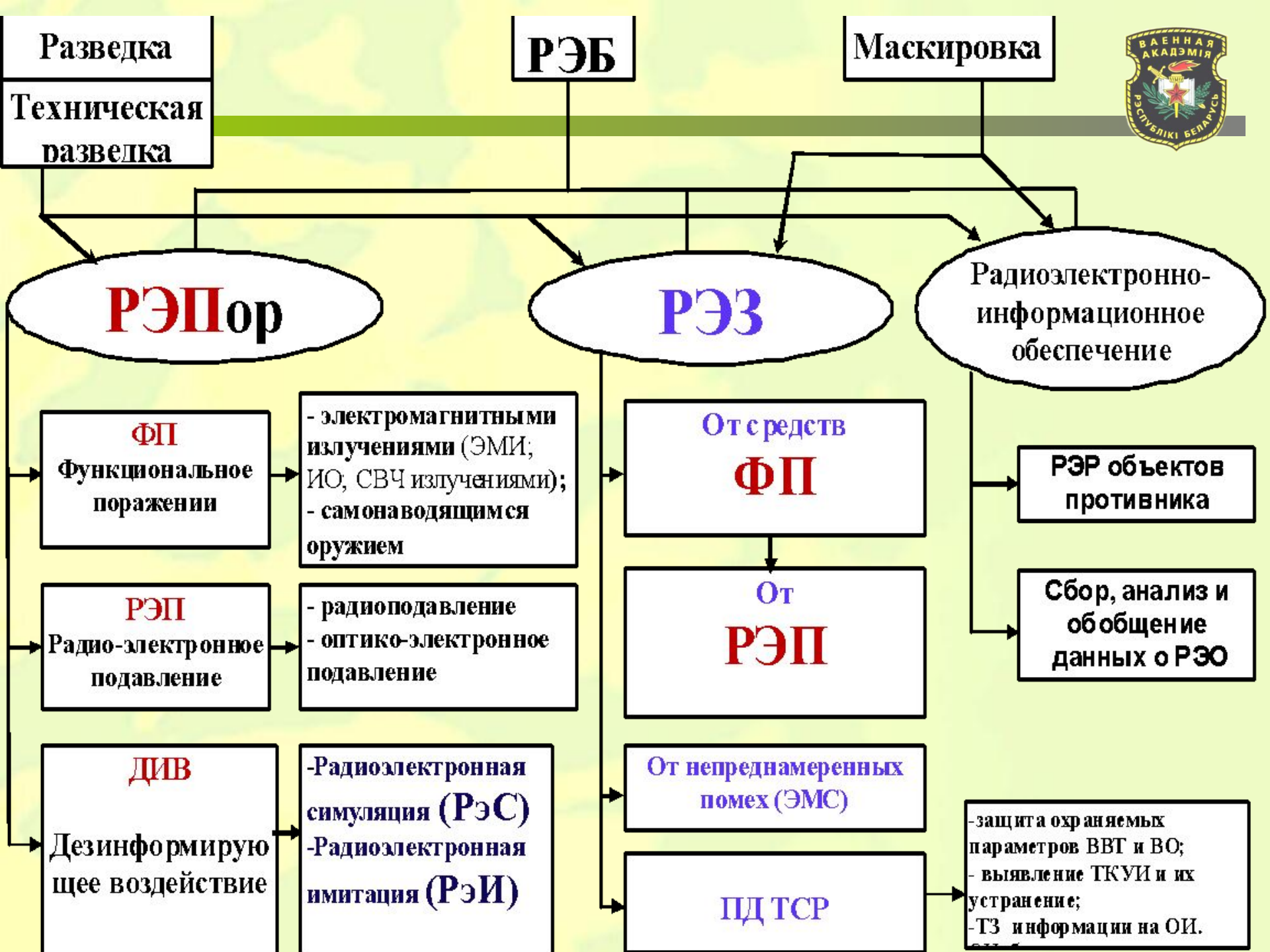
Срыв управления достигается уничтожением (выводом из строя) не менее 50-60% наиболее важных ПУ и радиоэлектронных объектов системы управления войсками (силами) и оружием противника и РЭП не менее 75% его сохранившихся важных РЭС.

Нарушение управления достигается уничтожением (выводом из строя) не менее 30-50% наиболее важных ПУ и радиоэлектронных объектов системы управления войсками (силами) и оружием противника и РЭП не менее 50% его сохранившихся важных РЭС.

Затруднение управления достигается уничтожением (выводом из строя) не менее 15-30% наиболее важных ПУ и радиоэлектронных объектов системы управления войсками (силами) и оружием противника и РЭП не менее 30% его сохранившихся важных РЭС.

3.2. Сбор анализ и обобщение данных радиоэлектронной обстановки являются важнейшей задачей всех органов управления, привлекаемых к проведению мероприятий радиоэлектронной борьбы, и осуществляются для эффективного ее ведения.

Для выполнения этой задачи **используются все возможные источники получения информации**. Сбор, анализ и обобщение данных радиоэлектронной обстановки осуществляется непрерывно в мирное время, угрожаемый период, при подготовке и в ходе ведения операций (боевых действий).


Разведка
Техническая разведка
РЭБ
Маскировка
РЭПор
РЭЗ
Радиоэлектронно-информационное обеспечение
ФП
Функциональное поражении
- электромагнитными излучениями (ЭМИ; ИО; СВЧ излучениями);
- самонаводящимся оружием
РЭП
Радио-электронное подавление
- радиоподавление
- оптико-электронное подавление
ДИВ
Дезинформирующее воздействие
-Радиоэлектронная симуляция (РэС)
-Радиоэлектронная имитация (РэИ)
От средств ФП
От РЭП
От непреднамеренных помех (ЭМС)
ПД ТСР
РЭР объектов противника
Сбор, анализ и обобщение данных о РЭО
-защита охраняемых параметров ВВТ и ВО;
- выявление ТКУИ и их устранение;
-ТЗ информации на ОИ.

Выводы:

1. **РЭБ – вид боевого обеспечения**.
2. Ведение **РЭБ** – решающий **фактор** для победы в противоборстве двух сторон.
3. **РЭБ** из вида боевого обеспечения переходит в способ ведения боевых действий.