

**МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ЛИНГВИСТИЧЕСКИЙ УНИВЕРСИТЕТ**

**Кафедра информационной безопасности**

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
И ПРОБЛЕМЫ ЕЕ ОБЕСПЕЧЕНИЯ В УСЛОВИЯХ  
МЕЖГОСУДАРСТВЕННОГО ПРОТИВОБОРСТВА**

***ЛЕКЦИЯ***

***27 сентября 2016 г.***

**ДЕРБИН Евгений Анатольевич,  
профессор кафедры, доктор военных наук  
тел.: 8-926-754-13-75**

## Вопросы для обсуждения:



**1.** Концептуальные основы обеспечения информационной безопасности в условиях не прямых действий.

**2.** Угрозы в информационной сфере и национальная безопасность России в условиях межгосударственного противоборства.

## Литература:

- 1.** Директивы СНБ США 1982-89 гг.: [www.fas.org/irp/offdocs/nsdd/index](http://www.fas.org/irp/offdocs/nsdd/index)
- 2.** Доктрина информационной безопасности Российской Федерации, 2000 г. Поручение Президента РФ 2000 г. № Пр-1895
- 3.** Закон ФЗ №310 «О безопасности», 26 декабря 2010 г.
- 4.** Стрельцов А.А. Информационная безопасность Российской Федерации. - М.: Высшая школа, 2003., С. 27-48

ИНФОРМАЦИЯ

**ИНФОРМАЦИЯ** – осмысляемые сигналы, а также данные и сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления.

ИНФОРМАЦИОННЫЙ  
И  
ОБЪЕКТ

**ИНФОРМАЦИОННЫЙ ОБЪЕКТ** – информация или ее носитель.

ИНФОРМАЦИОННАЯ  
ОБСТАНОВКА

**ИНФОРМАЦИОННАЯ ОБСТАНОВКА** – совокупность условий и факторов, оказывающих влияние на состояние информационной сферы и функционирование информационных объектов.

УГРОЗА

**УГРОЗА** – высший уровень опасности, характеризующийся наличием намерения, возможности и готовности субъекта (фактора) угрозы к нанесению (реализации) ущерба объекту, влекущего:

- ◆ утрату элементов структуры объекта;
- ◆ нарушение связей, программ и функций объекта;
- ◆ потерю способности объекта к развитию;
- ◆ утрату самоидентичности объекта.

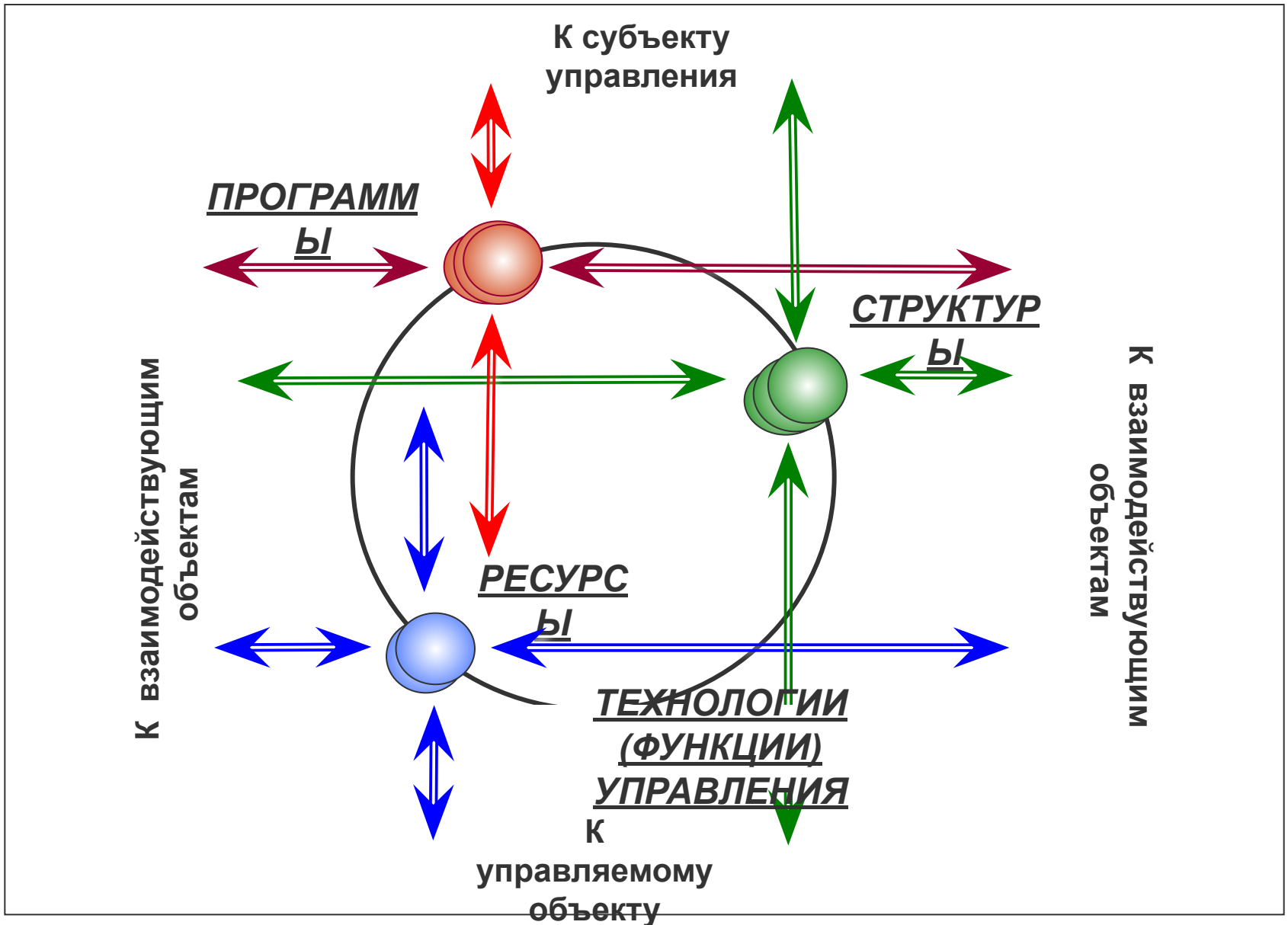
ОПАСНОСТЬ

**ИНФОРМАЦИОННАЯ ОПАСНОСТЬ** – состояние информационной обстановки, характеризующееся обострением рисков, вызовов для объекта, угроз объекту, реализация которых сделает его менее соответствующим своему предназначению

БЕЗОПАСНОСТЬ

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТА** – состояние информационной обстановки, характеризующееся отсутствием опасности, способностью и готовностью субъекта управления защитить объект от ущерба и (или) способностью объекта самостоятельно нейтрализовывать угрозы

# ТОПОЛОГИЯ ИНФОРМАЦИОННОГО ОБЪЕКТА

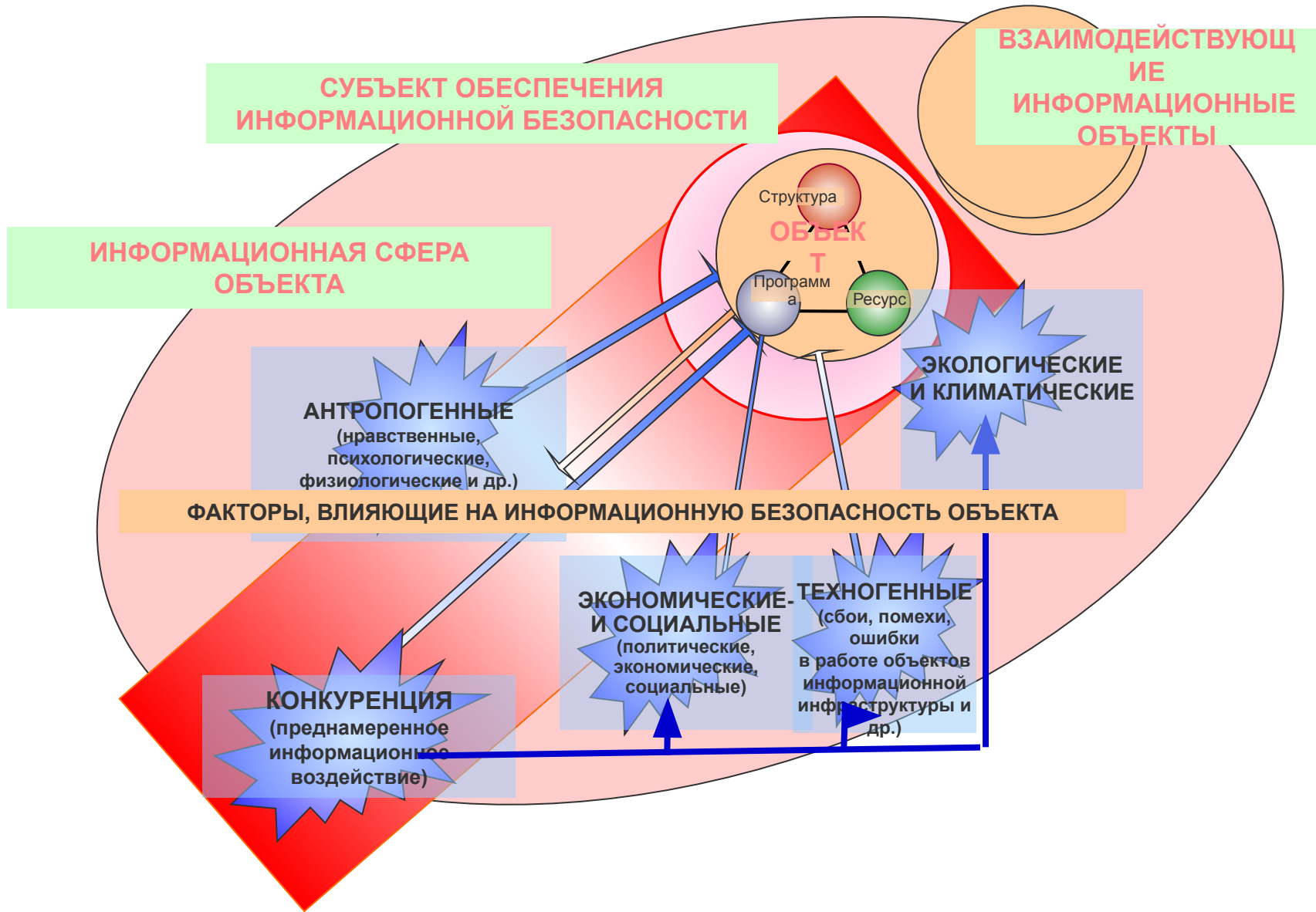


# УНИВЕРСАЛЬНЫЕ ПРИЗНАКИ ИНФОРМАЦИОННЫХ ХАРАКТЕРИСТИК ОБЪЕКТОВ С УЧЕТОМ СОДЕРЖАНИЯ ЭЛЕМЕНТОВ ИХ ТОПОЛОГИИ

ЭЛЕМЕНТЫ ТОПОЛОГИИ	ОБЪЕКТЫ:		
	ИНФОРМАЦИЯ	ИНФОРМАЦИОННО- ТЕХНИЧЕСКИЕ	ИНФОРМАЦИОННО- ПСИХОЛОГИЧЕСКИЕ
<b>Структуры</b>	Форма, логичность, последовательность), целостность, сохранность и др.	Конфигурация вычислительной сети, телекоммуникационных систем и пр.	<u>Для индивида:</u> структура личности, психологическая и биологическая структуры. <u>Для социальной группы:</u> политическая, социальная, психологическая, организационная и др. структуры
<b>Программы</b>	Смыслообусловленность	Уровень программного обеспечения и алгоритмов защиты информации и др.	Доминирующие духовные и материальные потребности; мировоззренческие, ценностно-смысловые аспекты, цели, задачи, планы, интересы, мотивы деятельности и др.
<b>Ресурсы</b>	Объем, качество (актуальность, новизна, важность, истинность) и др.	Объем ресурсов: информационного, энергетического и др., техническая надежность, защищенность и пр.	<u>Для индивида:</u> власть, социальный и профессиональный опыт, квалификация, компетентность, память, качество и объем знаний, состояние физического здоровья и психологической устойчивости; меры удовлетворения потребностей. <u>Для социальной группы:</u> экономические, психологические, моральные и др.
<b>Системные основы (функции, требования)</b>	Уровень обобщения; смысловой, когнитивный, аксиологический, мотивационной и др. аспекты, конфиденциальность, достоверность и др.	Принадлежность, роль и место в системе управления, зависимость от человеческого фактора и др.	Роль в обществе, важность, функций; моральные, нравственные и рационально-волевые качества, идеология. Слаженность коллектива и др.
<b>Связи</b>	Логические связи с другими объектами, принадлежность, направленность: причина-следствие; посылки-выводы; аргументы-факты и др.	Системные связи вычислительной сети	Субъектность в структуре, политические и социальные отношения, коммуникабельность, гибкость. Доминирующие отношения (противоборство, конкуренция, сосуществование, сотрудничество, дружба и пр.)

# **1. КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ НЕПРЯМЫХ ДЕЙСТВИЙ**

# ФАКТОРЫ, ОКАЗЫВАЮЩИЕ ВЛИЯНИЕ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ



# УНИВЕРСАЛЬНАЯ ВЗАИМОСВЯЗЬ ВИДОВ, ОБЪЕКТОВ И СРЕДСТВ БОРЬБЫ

## ОБЪЕКТЫ БОРЬБЫ

**ИНФОРМАЦИЯ МИРОВОЗЗРЕНЧЕСКОГО УРОВНЯ**  
(сущности, смыслы всеобщих длительных процессов, философские, религиозные концепции и др.)

**ИНФОРМАЦИЯ АНАЛИТИЧЕСКОГО И ХРОНОЛОГИЧЕСКОГО УРОВНЯ,**  
позволяющая выделить из общих процессов частные (фундаментальная наука, культурное наследие и др.)

**ИНФОРМАЦИЯ КАК ОПИСАНИЕ ЧАСТНЫХ ПРОЦЕССОВ** (прикладная наука, теории и др.)

**ЗНАНИЯ И ИНФОРМАЦИОННЫЕ РЕСУРСЫ ОБЛАСТЕЙ ПРАКТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ**  
(в т.ч. конфиденциальные, промышленные, социальные, информационные и др. технологии и пр.)

**ПОЛИТИЧЕСКАЯ ВЛАСТЬ**

**ЭКОНОМИЧЕСКОЕ ГОСПОДСТВО, МАТЕРИАЛЬНЫЕ РЕСУРСЫ**

## ВИДЫ БОРЬБЫ

**ИНФОРМАЦИОННОЕ  
ПРОТИВОБОРСТВО**

**ЭКОНОМИЧЕСКАЯ**

**ПОЛИТИЧЕСКАЯ  
БОРЬБА**

**ВООРУЖЕННАЯ  
БОРЬБА**

**ИДЕОЛОГИЧЕСКАЯ  
БОРЬБА**

## СРЕДСТВА БОРЬБЫ

Информация (знания), информационные технологии, **информационное оружие**

Средства разрушения социальных объектов и среды обитания  
(климатические, геофизические, наркотические, генно-инженерные)

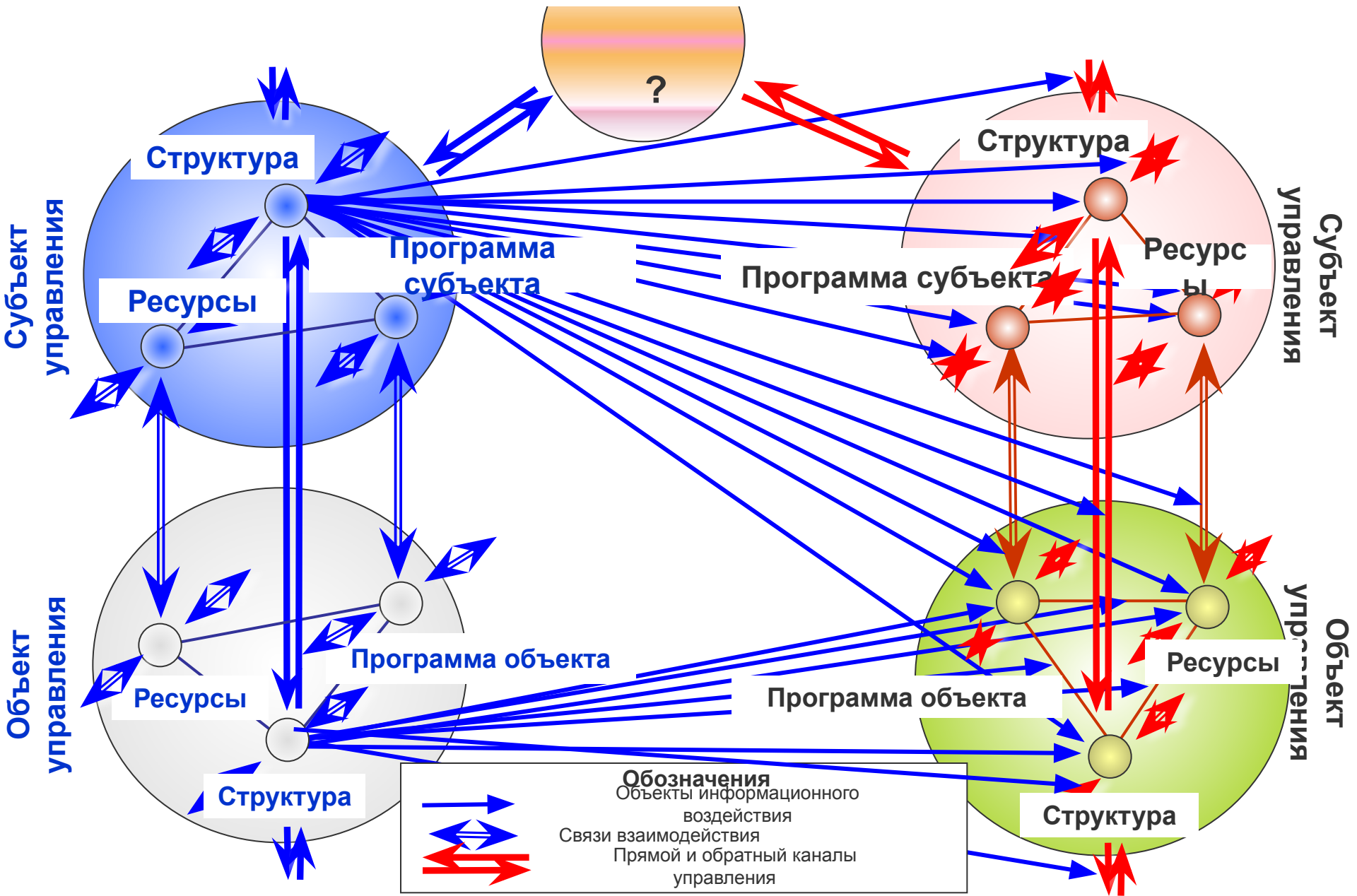
Традиционные средства поражения  
**(средства вооруженной борьбы)**

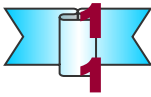
Средства поражения на новых физических  
принципах и нелетального воздействия





# МОДЕЛИ СИСТЕМ УПРАВЛЕНИЯ И НАПРАВЛЕННОСТЬ ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ



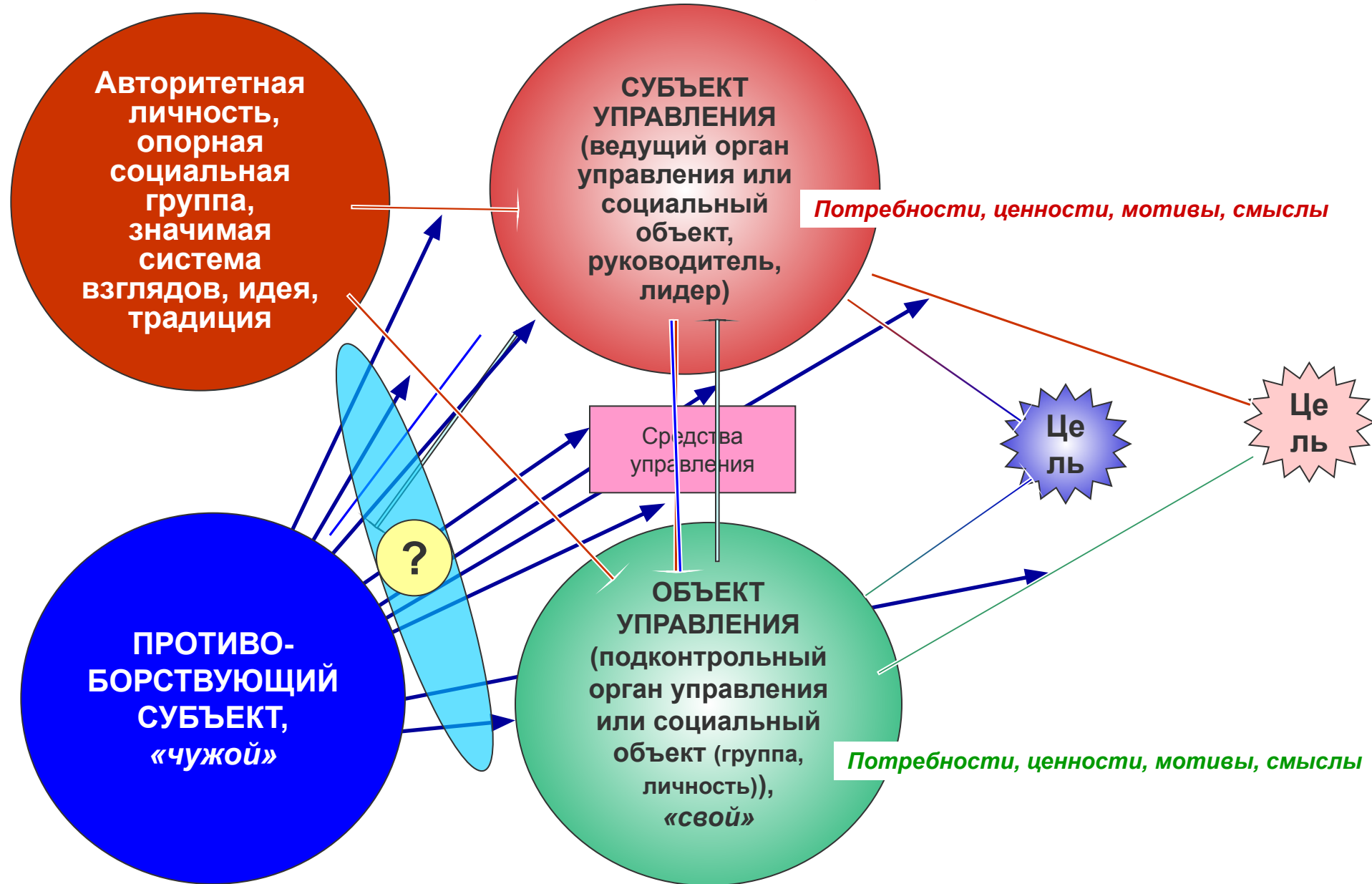


## **2. УГРОЗЫ В ИНФОРМАЦИОННОЙ СФЕРЕ И НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ РОССИИ**

# ГОСУДАРСТВА И СТРАНЫ КАК ОБЪЕКТЫ ВОЗДЕЙСТВИЯ В МОДЕЛИ US AIR FORCE DEPARTMENT



# КОНФЛИКТНЫЕ ВЗАИМОДЕЙСТВИЯ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ ПРОТИВОБОРСТВУЮЩИХ СИСТЕМ



# ДЕКОМПОЗИЦИЯ СТРУКТУРЫ ГОСУДАРСТВА ИНФОРМАЦИОННЫЕ ВОЗДЕЙСТВИЯ КАК ИНФОРМАЦИОННОГО ОБЪЕКТА НА ИНФОРМАЦИОННЫЙ ОБЪЕКТ СОГЛАСНО АНАЛОГОВОЙ МОДЕЛИ КОРПОРАЦИИ «RAND»

Перепрограммирование  
группового сознания  
руководства

Поддержка деятельности  
оппозиционных  
и сепаратистских сил

здравоохранения, экология

Разрушительное  
реформирование науки,  
здравоохранения, образования,  
СМИ

Инициирование военных угроз,  
терроризм

Скрытое инициирование  
дисфункций и аварийности  
в национальной  
инфраструктуре

Генно-инженерные,  
наркотропные и пр.  
воздействия на население

Агентурные внедрения в  
спецслужбы, разрушительные  
организационные воздействия

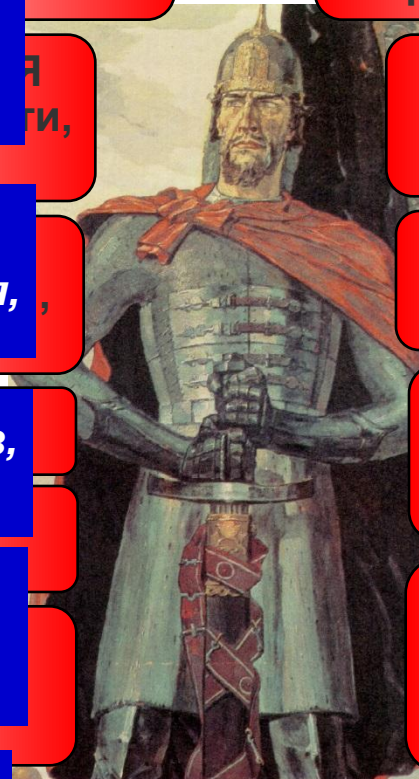
Формирование кризисных  
ситуаций в международных  
отношениях, оказание  
внешнеполитического давления  
и др.

– общественное сознание

Перепрограммирование  
массового сознания

Подрывные финансовые,  
и экономические операции

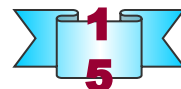
Разрушительные воздействия  
на экологию  
и климатические процессы



НОГИ» – социально-  
экономические основ  
изнедательности и  
безопасности



# МЕТОДЫ И СРЕДСТВА ИНФОРМАЦИОННО-ТЕХНИЧЕСКОГО ВОЗДЕЙСТВИЯ



## А) Оперативно-технические методы

- 1) хищение носителей информации;
- 2) уничтожение (стирание) информации, программ и разрушение технических средств;
- 3) копирование программ и вирусов;
- 4) внедрение технических и программных закладок;
- 5) нарушение работы технических устройств;
- 6) внесение изменений в программы и внедрение несанкционированного программного обеспечения

## Б) задачи и средства РЭБ

- 1) радиоэлектронное поражение (подавление);
- 2) электромагнитные метательные устройства;
- 3) электромагнитные боеприпасы;
- 4) электронные излучатели;
- 5) генераторы электронных (электромагнитных) импульсов;
- 6) средства радиоэлектронного подавления

## В) Методы и средства программных воздействий

- 1) НСД (взлом парольных систем; создание ложных серверов; подмена клавиатурного почерка);
- 2) внедрение логических бомб, троянских программ, программ-«червей», программ-«разведчиков»;
- 3) вирусные атаки;
- 4) нейтрализация тестовых программ;
- 5) применение чипов-«мин»;
- 6) атаки систем управления ЛВС и ЦАТС, маршрутизаторов и коммутаторов;
- 7) использование супер-сетей для контроля информационных потоков в глобальных сетях;
- 8) внедрение искусственных иммунных систем;
- 9) распространение «квантовых микробов»

## Г) Методы и средства радиоэлектронной разведки

- 1) радиоперехват;
- 2) криптография и криптографический анализ;
- 3) применение радиоэлектронных закладок;
- 4) использование виброакустических и визуально-оптических каналов утечки;
- 5) электромагнитное облучение технических устройств;
- 6) воздействие по сети электропитания и заземления;
- 7) компьютерная стеганография;
- 8) применение микромеханических электронных устройств

# МЕТОДЫ И СРЕДСТВА ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ С ПРИМЕНЕНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ



## **А) Электронные аудио- и визуальные методы и средства**

- 1) манипулирование общественным сознанием посредством электронных СМИ (радиовещание, спутниковое и кабельное телевидение, Интернет) и мобильных систем связи (сотовых, транкинговых, пейджинговых, персональные коммуникаторов и др.);
- 2) голосовая дезинформация на основе технологий синтеза речи;
- 3) применение компьютерных технологий синтеза видео ряда;
- 4) применение голографических проективных систем и др.

## **Б) Методы и средства компьютерного и психотронного воздействия**

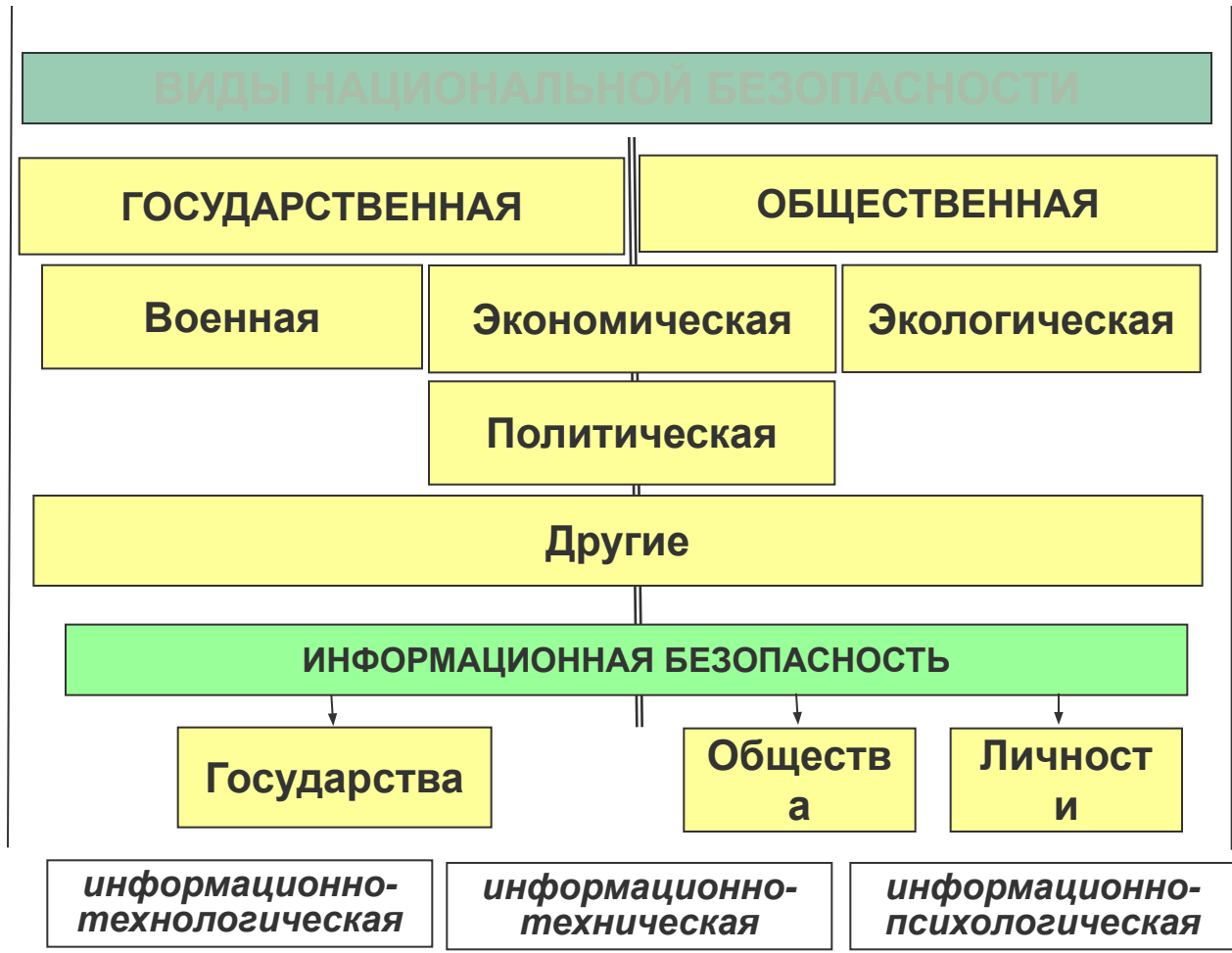
- 1) психокорректирующие компьютерные игры;
- 2) программы скрытого воздействия на психику в виде нейролингвистических закладок;
- 3) применение компьютерных пси-вирусов;
- 4) применение компьютерных психотехнологий (полиграфов, психосемантических алгоритмов исследования неосознаваемой информации и др.);
- 5) применение пси-генераторов и др.

## **В) Системы ситуационно-аналитического моделирования и прогнозирования**

- 1) текстово-аналитические системы (гипертекстовые, data-mining и т.д.);
- 2) системы ситуационного моделирования;
- 3) системы прогнозирования и принятия решений в кризисных ситуациях (СЦ);
- 4) системы управляемого хаоса;
- 5) геоинформационные системы оценки обстановки в реальном времени;
- 6) нейросетевые системы управления документооборотом (Excalibur и др.)



# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СТРУКТУРЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ



**СОСТОЯНИЕ ЗАЩИЩЕННОСТИ НАЦИОНАЛЬНЫХ ИНТЕРЕСОВ  
В ИНФОРМАЦИОННОЙ СФЕРЕ, ОПРЕДЕЛЯЮЩИХСЯ СОВОКУПНОСТЬЮ  
СБАЛАНСИРОВАННЫХ ИНТЕРЕСОВ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА**

ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ, ст. 1, п.3

## 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

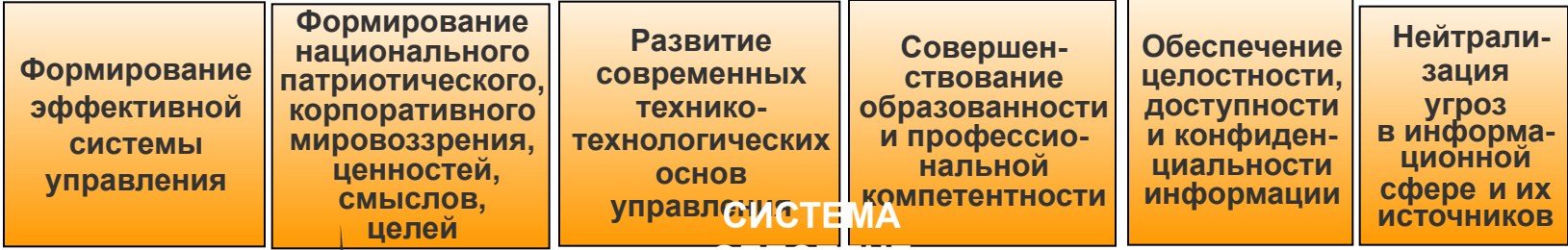
## ЭКОНОМИЧЕСКИЕ

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

# МЕТОДИЧЕСКИЙ АППАРАТ ФОРМИРОВАНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е  
Н  
И  
Я  
И  
Н  
Ф  
О  
Р  
М  
А  
-  
Ц  
И  
О  
Н  
Н

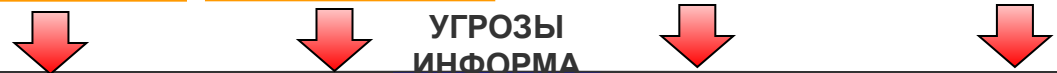
## ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



## ИНФОРМА



## ВИДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



УГРОЗЫ  
ИНФОРМАЦИОННОЙ  
БЕЗОПАС

О  
Й  
ПОДДЕРЖАНИЕ УСЛОВИЙ ЭФФЕКТИВНОГО УПРАВЛЕНИЯ  
П  
СОХРАНЕНИЕ ПОЗИТИВНЫХ ТЕНДЕНЦИЙ РАЗВИТИЯ  
С  
СОХРАНЕНИЕ ОСНОВ И КУЛЬТУРЫ, РАЗВИТИЕ И ПОДДЕРЖАНИЕ ОБЩЕСТВЕННОГО СОГЛАСИЯ