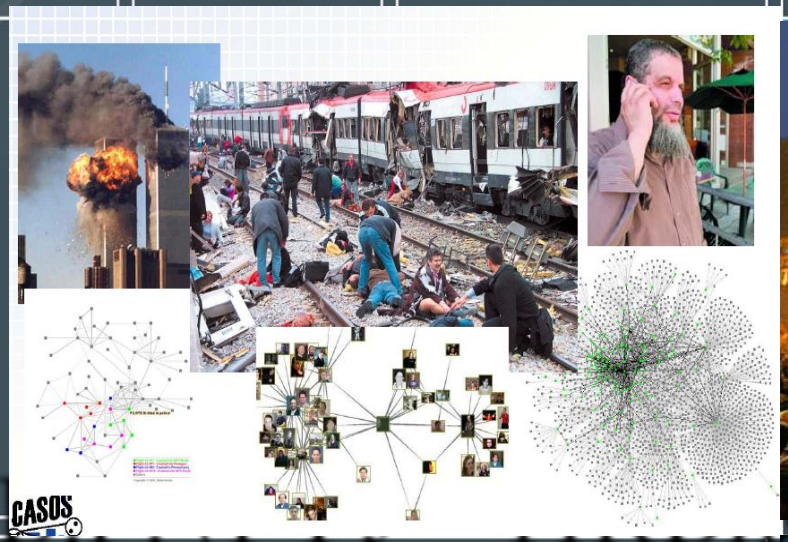
НАЦИОНАЛЬНАЯ СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(вводная лекция)

Российский технологический университет -МИРЭА

(Институт комплексной безопасности и специального приборостроения)



Григорьев В.Р. (РТУ - ИКБиСП)

зав. кафедрой «Информационное противоборство», зам. директора ИКБСП

к.т.н., доцент, член-корр. РАЕН

ЭПИГРАФЫ

“...Тот, кто умеет вести войну, покоряет чужую армию, не сражаясь, берет чужие крепости, не осаждая; сокрушает чужое государство, не держа свое войско долго” **(гл. III, п. 3).**
“Поэтому сто раз сразиться и сто раз победить — это не лучшее из лучшего; лучшее из лучшего — покорить чужую армию не сражаясь” **(гл. III, п. 1).**

Сунь Цзы (孫子) — китайский стратег и мыслитель, предположительно, живший в VI или, по другим источникам, в IV веке до н. э. Автор знаменитого трактата о военной стратегии «Искусство войны»

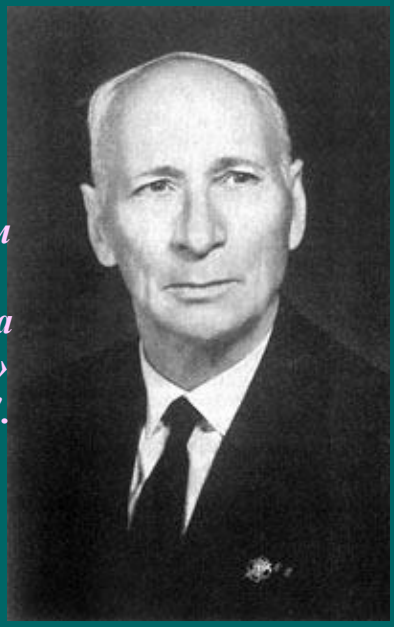
"...всему есть мать безконфузство, ибо сие едино войско возвышает и низвергает"

ПЕТР I ВЕЛИКИЙ (1672-1725), российский царь с 1682 (правил с 1689), первый российский император (с 1721),

"Слухи преувеличивают действие",- **писала Екатерина II Потемкину, советуя тревожить турок пугающими слухами в дополнение к боевым действиям.**

ЭПИГРАФЫ

- *«Мятежевойна - это война всех против всех, причем врагом бывает и соплеменник, а союзником - и иноплеменный. У каждого человека должен быть колчан с психологическими стрелами и психологический щит».*
- *«В мятежевойне психология мятежных масс отодвигает на второй план оружие войска и его психологию и становится решающим фактором победы или поражения..»*
- *«В прежних войнах важным почиталось завоевание территории. Впредь важнейшим будет почитаться завоевание душ во враждующем государстве.»*
- *«Война на нервах в эпоху, когда народы неврастеничны, требует от стратегов весьма продуманного обращения с главным фактором войны - с психикой воюющего народа...»*
- *"Народная масса мало восприимчива к логике ума, но легко поддается логике чувств".*



Генерального штаба полковник профессор Евгений Эдуардович Месснер (1891-1974), один из крупнейших представителей военной мысли Русского Зарубежья.
Автор работ "Мятеж - имя третьей всемирной", "Современные офицеры", "Всемирная мятежевойна", изданных в 1960-1971 гг. в Буэнос-Айресе и Нью-Йорке.

«Идет борьба за умы и души - лишь затем за жизни и территории».

«Бои - лишь эпизоды, похожие на взрыв ракеты. Умелая организация мобилизует универсальные духовные силы».

генерал А.Е.Снесарёв (1.12.1865 — 4.12.1937)

Русский военачальник и учёный-востоковед. Герой Труда (1928). В Советской Армии с 1918. Окончил матем. фак. Моск. ун-та (1888), пех. уч-ще (1890) и Академию Генштаба (1899); владел 14 языками. С 1888 на воен. службе в Туркестане, занимался изучением и военно-геогр. описанием Ср. Востока. Совершил поездки по Индии, Афганистану, Тибету и Кашгарии. С 1904 в Генштабе, одновременно преподавал воен. географию в воен. училищах. С 1910 нач-к штаба казачьей дивизии. В 1-ю мировую войну командовал полком, бригадой и дивизией, ген.-лейтенант (1917). Георгиевский кавалер.

Директива 20/1 СНБ США от 18 августа 1948 г., более известная как «План Аллена Даллеса»

Так какие цели мы должны искать в отношении любой некоммунистической власти, которая может возникнуть на части или всей русской территории в результате событий войны? Следует со всей силой подчеркнуть, что независимо от идеологической основы любого такого некоммунистического режима и независимо от того, в какой мере он будет готов на словах воздавать хвалу демократии и либерализму, мы должны добиться осуществления наших целей, вытекающих из уже упомянутых требований. Другими словами, мы должны создавать автоматические гарантии, обеспечивающие, чтобы даже некоммунистический и номинально дружественный к нам режим:

а) не имел большой военной мощи;

б) в экономическом отношении сильно зависел от внешнего мира;

в) не имел серьезной власти над главными национальными меньшинствами;

г) не установил ничего похожего на железный занавес.

В случае, если такой режим будет выражать враждебность к коммунистам и дружбу к нам, мы должны позаботиться, чтобы эти условия были навязаны не оскорбительным или унизительным образом. Но мы обязаны не мытьем, так катаньем навязать их для защиты наших интересов...

«Россия – побеждённая держава. Она проиграла титаническую борьбу. И говорить „это была не Россия, а Советский Союз“ – значит бежать от реальности. Это была Россия, названная Советским Союзом. Она бросила вызов США. Она была побеждена. Сейчас не надо подпитывать иллюзии о великодержавности России. Нужно отбить охоту к такому образу мыслей… Россия будет раздробленной и под опекой». «Новый мировой порядок при гегемонии США создается против России, за счёт России и на обломках России».

Бжезинский Зб. Выбор. Глобальное господство или глобальное лидерство. М., 2010. С. 127.

Медаль «За победу в холодной войне»

ЭПИГРАФЫ

- "Холодная война на самом деле была Третьей мировой войной, а сейчас США ввязались в Четвертую мировую войну, которая продлится много лет", - признал бывший директор ЦРУ США Джеймс Вулси, выступая в Калифорнийском университете 3 апреля 2003 года.

- "С целью управления всем миром, Соединенные Штаты вступили в войну, до конца которой мы не доживем", - вторил ему вице-президент США Ричард Чейни.

«…Против России действительно идет информационная война. … Информационная война — это реакция «оппонентов» России на укрепление страны…Эффективный, суверенный игрок мало кому нужен, его стараются осадить. Если бы вели себя тише воды ниже травы, были бы хорошими для всех, но утрачивали бы значение, а следующим шагом — утрата суверенитета и перспектив на будущее».

Из выступления Президента Российской Федерации Владимира Путина на «Форуме действий. Регионы», который провел Общероссийский народный фронт (ОНФ) 24.04.16 в Йошкар-Оле (Марий-Эл).

Ряд стран уже фактически поставили информационные технологии на военную службу: формируют свои кибервойска, а также активно используют информационное поле для ослабления конкурентов, продвижения своих экономических и политических интересов, решения геополитических задач в целом, в том числе в качестве фактора так называемой мягкой силы.

В этой связи мы должны чётко представлять тенденции развития глобальной информационной сферы, прогнозировать потенциальные угрозы и риски. И главное – наметить дополнительные меры, которые позволят нам не просто своевременно выявлять угрозы, а активно реагировать на них.

Из выступления Президента РФ В.В.Путина на заседании Совета Безопасности РФ 26 октября 2017 годаоктября 2017 года

Раздел 1. Информационная безопасность и ее место в системе национальной безопасности РФ

Введение. Предмет и задачи курса. Особенности изучаемой дисциплины. Основные сферы обеспечения информационной безопасности

Виды воздействий в условиях ведения информационных войн

Роль и место информационной безопасности в обеспечении национальной безопасности России

Информационная безопасность как объект анализа

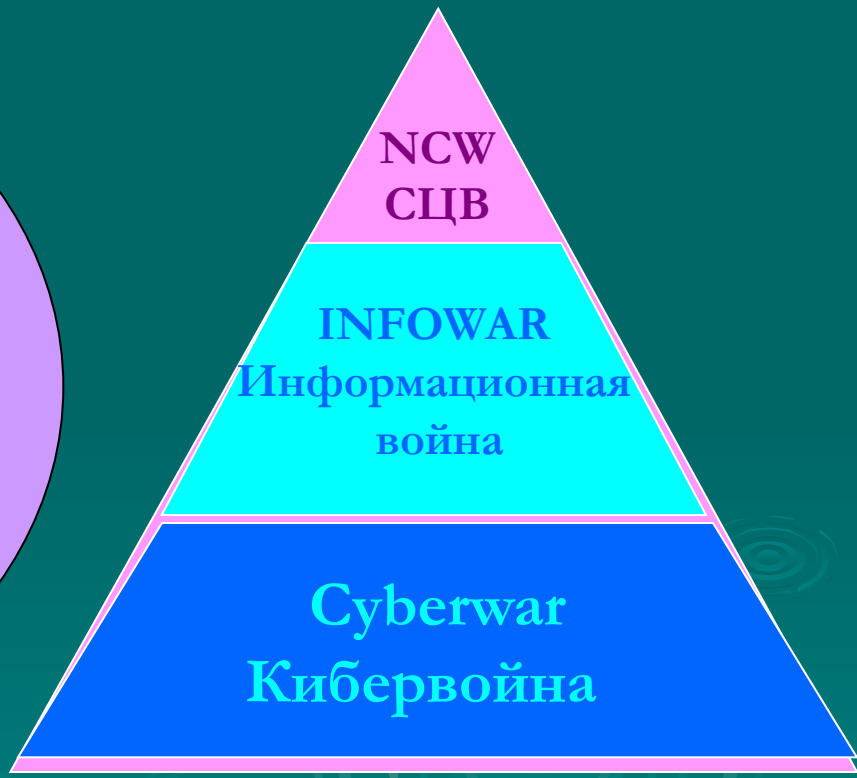
Система информационной безопасности

функциональная система, отражающая процессы взаимодействия интересов и угроз

Система обеспечения информационной безопасности

организационная система органов, сил, средств, различных организаций, призванных решать задачи по обеспечению информационной безопасности

Три области обращения информации



Духовная война

- перекодировка национального самоосознания,
- смена веры(ований), уничтожение (подмена) знаний,
- искажение(подмена) языка(логоса),
- уничтожение (подмена) культурных артефактов (письменных источников, памятников архитектуры, эпоса, песенного и танцевального фольклора, замена национального костюма на одежду «унисекс» и т.д.)

Психотронная война

- HAARP,
- психотроника: генераторы НЧ, СВЧ;
- пси-вирусы;
- психокорректирующие игры;
- НЛП

Информационно-психологическая война

- дуплексные коммуникативные каналы воздействия:
- социальные сети, ЖЖ, блогосфера;
- интерактивное ТВ, мобильные платформы коммуникаторов;

однонаправленные каналы воздействия:

- электронные СМИ (ТВ, радио, печать),

Информационно-техническая война:

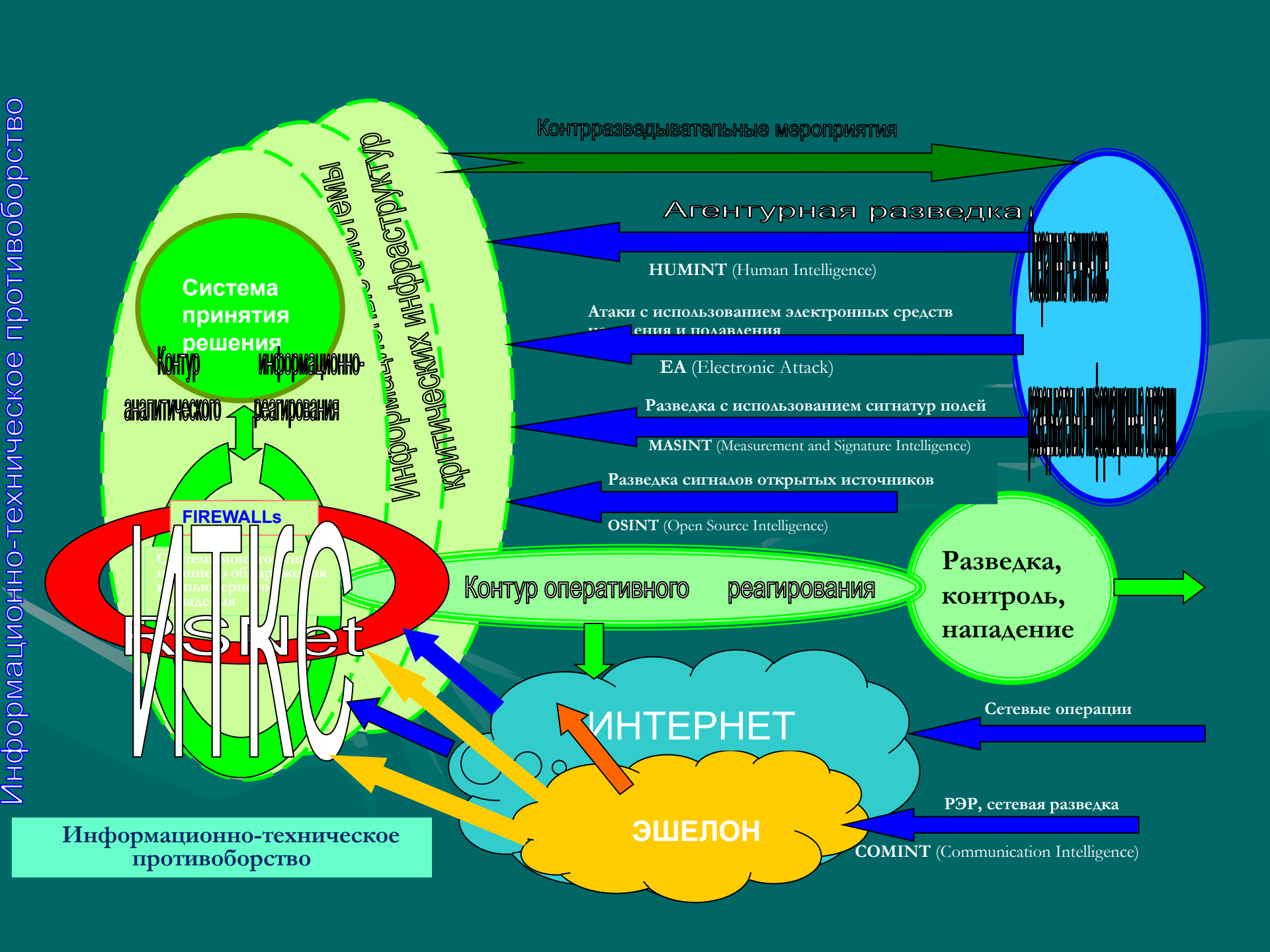
- глобальные и локальные сети, телекоммуникации, СУБД,
- ЦАТС, маршрутизаторы, трансляторы,
- SCADA-системы, АСУ ТП и т.д.)

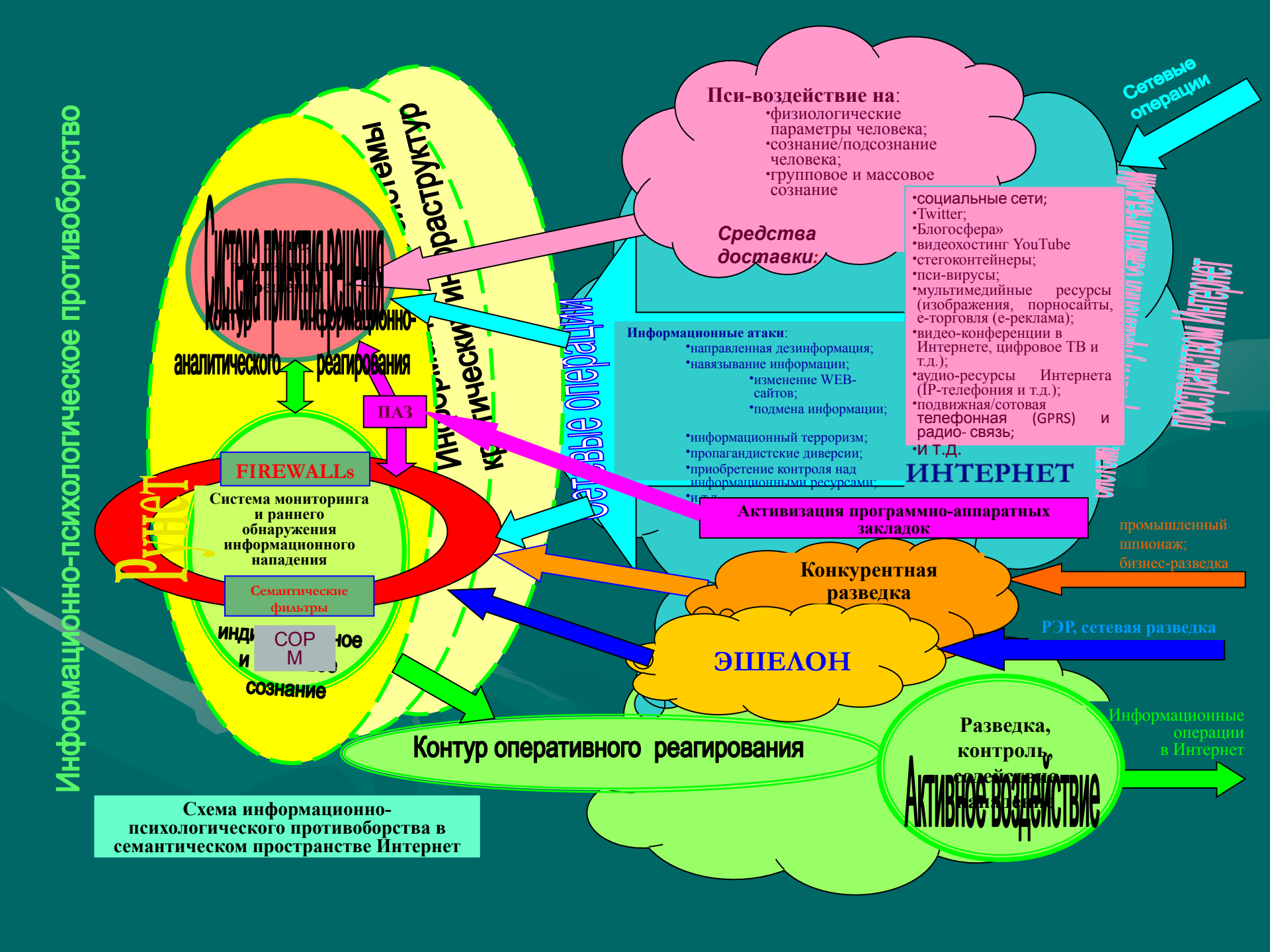
Информационно-биологическая война (рассовое оружие)

- информационное воздействие на генном уровне: генномодифицированные и синтетические продукты, наркотики, лекарства, алкоголь, «энергетические» напитки,
- воздействие на среду обитания (биофизические воздействия, воздействия на климат).

Информация как объект противоборства

Объекты интереса	Борьба за информацию	Борьба против информации	Борьба посредством информации
Информационно-телекоммуникационные системы (техносфера)	Все виды технической разведки: РЭР; РТР; Космическая разведка; Компьютерная разведка; И т.д.	Средства защиты информации: ОС, каналов связи, СУБД, сетевых ресурсов, облачных технологий, и т.д.	Информационные операции в техносфере: вирусы, черви, программно-аппаратные закладки, и др.
Индивидуальное, групповое и общественное сознание (гуманитарная сфера)	Агентурная разведка. Дипломатия.	Защита сознания: человека, групп населения, социума.	Информационные операции в инфосфере: пропаганда, вербовка, агитация, пси-воздействие и др. (СМИ, социальные ресурсы Интернет)


Информационно-техническое противоборство
Контрразведывательные мероприятия
Агентурная разведка
HUMINT (Human Intelligence)
Атаки с использованием электронных средств
EA (Electronic Attack)
Разведка с использованием сигнатур полей
MASINT (Measurement and Signature Intelligence)
Разведка сигналов открытых источников
OSINT (Open Source Intelligence)
Система принятия решения
Контур аналитического реагирования
информационно-
Инфраструктуры критических
FIREWALLs
ИТКС
FSNet
Контур оперативного реагирования
Разведка, контроль, нападение
ИНТЕРНЕТ
Сетевые операции
ЭШЕЛОН
РЭР, сетевая разведка
COMINT (Communication Intelligence)
Информационно-техническое противоборство


Информационно-психологическое противоборство
Пси-воздействие на:
•физиологические параметры человека;
•сознание/подсознание человека;
•групповое и массовое сознание
Средства доставки:
•социальные сети;
•Twitter;
•Блогосфера»
•видеохостинг YouTube
•стегоконтейнеры;
•пси-вирусы;
•мультимедийные ресурсы (изображения, порносайты, е-торговля (е-реклама);
•видео-конференции в Интернете, цифровое ТВ и т.д.);
•аудио-ресурсы Интернета (IP-телефония и т.д.);
•подвижная/сотовая телефонная (GPRS) и радио- связь;
•и т.д.
Сетевые операции
Информационные атаки:
•направленная дезинформация;
•навязывание информации;
•изменение WEB-сайтов;
•подмена информации;
•информационный терроризм;
•пропагандистские диверсии;
•приобретение контроля над информационными ресурсами;
ИНТЕРНЕТ
Активизация программно-аппаратных закладок
Рунет
FIREWALLs
Система мониторинга и раннего обнаружения информационного нападения
Семантические фильтры
ПАЗ
Контур информационно-аналитического реагирования
Системы принятия решений
Инфраструктура
Сетевые операции
промышленный шпионаж;
бизнес-разведка
Конкурентная разведка
РЭР, сетевая разведка
ЭШЕЛОН
Контур оперативного реагирования
Разведка, контроль
Активное воздействие
Информационные операции в Интернет
Схема информационно-психологического противоборства в семантическом пространстве Интернет

Основные понятия и определения в области информационной безопасности

Термины, определяющие научную основу информационной безо- пасности

- К этой группе относятся термины, которые используются во многих областях знаний и являются однозначными, семантически унифицированными и стилистически нейтральными. Это: *информация, коммуникация, конфликт, воздействие, угроза, опасность, безопасность, система.*
- Термины этой группы отвечают требованиям однозначности и устойчивости, т. е. эти термины однозначно употребляются в одной области знаний и сохраняют свой особый смысл в каждой другой об- ласти знаний, а также являются общепризнанными – они употребля- ются в обиходе. Однако термину «информация» присуще специфиче- ское свойство: в разных областях знаний, и даже в одной области зна- ния он может характеризовать предмет, явление, процесс и их свойст- ва и отношения одновременно.

Термины, определяющие предметную основу информационной безопасности

- Ко второй группе относятся термины, обозначающие понятия и их соотношение с другими понятиями в пределах информационной безопасности как специальной сферы или области знаний. К таковым относятся: *информатика, информатизация, информационная система, информационные технологии, информационные процессы, информационный объект, информационный ресурс, информационная инфраструктура, информационная сфера, информационный потенциал*.

Термины, определяющие характер деятельности по обеспечению информационной безопасности

- К третьей группе относятся термины, служащие обозначениями характерных для этой сферы предметов, явлений, процессов, их свойств и отношений (в том числе сил, средств и методов их использования при решении задач обеспечения информационной безопасности). Термины этой группы обозначают широкий круг понятий различного уровня: от технического канала утечки информации до информационного противоборства. К ним относятся: *информационное противоборство, информационное превосходство, информационная безопасность, угрозы информационной безопасности, обеспечение информационной безопасности, система обеспечения информационной безопасности, информационная защищенность, безопасность информации, защита информации, объект защиты информации, носитель информации, доступ к информации, доступность информации, целостность информации, конфиденциальность информации, несанкциони-рованный доступ к информации, утечка информации, канал утечки информации, канал передачи информации, воздействие на информацию, информационно-психологическое воздействие, информационно-психологическая сфера.*

- Важной специфической особенностью терминологической системы информационной безопасности является ее тесная связь с правовой лексикой. Это следствие того факта, что информационная безопасность давно перестала быть технической дисциплиной, частью информатики. В связи с этим выработка единообразия в терминологии по проблеме обеспечения информационной безопасности создает предпосылки для целенаправленного развития всех работ по теории информационной безопасности и методологии защиты информации.

Правовая база обеспечения информационной безопасности Российской Федерации

Конституция Российской Федерации

Конституция РФ является основным источником права в области обеспечения информационной безопасности в России.

Согласно Конституции РФ:

- **каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (статья 23);**
- **сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (статья 24);**
- **каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, перечень сведений, составляющих государственную тайну, определяется федеральным законом (статья 29);**
- **каждый имеет право на достоверную информацию о состоянии окружающей среды (статья 42).**

Место ИБ в системе национальной безопасности РФ

СТРАТЕГИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Утверждена Указом Президента Российской Федерации от 31 декабря 2015 г. N 683

- Настоящая Стратегия является базовым документом стратегического планирования, определяющим национальные интересы и стратегические национальные приоритеты Российской Федерации, цели, задачи и меры в области внутренней и внешней политики, направленные на укрепление национальной безопасности Российской Федерации и обеспечение устойчивого развития страны на долгосрочную перспективу.

СТРАТЕГИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

- 12. Укрепление России происходит на фоне новых угроз национальной безопасности, имеющих комплексный взаимосвязанный характер. Проведение Российской Федерацией самостоятельной внешней и внутренней политики вызывает противодействие со стороны США и их союзников, стремящихся сохранить свое доминирование в мировых делах. Реализуемая ими политика сдерживания России предусматривает оказание на нее политического, экономического, военного и информационного давления.
- 21. Все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории.
- 22. Появляются новые формы противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких технологий. Обостряются угрозы, связанные с неконтролируемой и незаконной миграцией, торговлей людьми, наркоторговлей и другими проявлениями транснациональной организованной преступности.

43. Основными угрозами государственной и общественной безопасности являются:

- деятельность террористических и экстремистских организаций, направленная на насильственное изменение конституционного строя Российской Федерации, дестабилизацию работы органов государственной власти, уничтожение или нарушение функционирования военных и промышленных объектов, объектов жизнеобеспечения населения, транспортной инфраструктуры, устрашение населения, в том числе путем завладения оружием массового уничтожения, радиоактивными, отравляющими, токсичными, химически и биологически опасными веществами, совершения актов ядерного терроризма, нарушения безопасности и устойчивости функционирования критической информационной инфраструктуры Российской Федерации;

43. Основными угрозами государственной и общественной безопасности являются:

- деятельность радикальных общественных объединений и группировок, использующих националистическую и религиозно-экстремистскую идеологию, иностранных и международных неправительственных организаций, финансовых и экономических структур, а также частных лиц, направленная на нарушение единства и территориальной целостности Российской Федерации, дестабилизацию внутриполитической и социальной ситуации в стране, включая инспирирование "цветных революций", разрушение традиционных российских духовно-нравственных ценностей;
- деятельность, связанная с использованием информационных и коммуникационных технологий для распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма, нанесения ущерба гражданскому миру, политической и социальной стабильности в обществе;

IV. Обеспечение национальной безопасности

47. В целях обеспечения государственной и общественной безопасности:

совершенствуется система выявления и анализа угроз в информационной сфере, противодействия им;

принимаются меры для повышения защищенности граждан и общества от деструктивного информационного воздействия со стороны экстремистских и террористических организаций, иностранных специальных служб и пропагандистских структур;

53. Для противодействия угрозам качеству жизни граждан органы государственной власти и органы местного самоуправления во взаимодействии с институтами гражданского общества:

обеспечивают развитие информационной инфраструктуры, доступность информации по различным вопросам социально-политической, экономической и духовной жизни общества, равный доступ к государственным услугам на всей территории Российской Федерации, в том числе с использованием информационных и коммуникационных технологий;

V. Организационные, нормативно-правовые и информационные основы реализации настоящей Стратегии

- 112. Информационную основу реализации настоящей Стратегии составляет федеральная информационная система стратегического планирования, включающая в себя информационные ресурсы органов государственной власти и органов местного самоуправления, системы распределенных ситуационных центров и государственных научных организаций.
- 113. При реализации настоящей Стратегии особое внимание уделяется обеспечению информационной безопасности с учетом стратегических национальных приоритетов.

Военная доктрина Российской Федерации

Утверждена Указом Президента Российской Федерации от 25 декабря 2014 г. N Пр-2976

II. Военные опасности и военные угрозы Российской Федерации

11. Наметилась тенденция смещения военных опасностей и военных угроз в информационное пространство и внутреннюю сферу Российской Федерации. При этом, несмотря на снижение вероятности развязывания против Российской Федерации крупномасштабной войны, на ряде направлений военные опасности для Российской Федерации усиливаются.

12. Основные внешние военные опасности:

м) использование информационных и коммуникационных технологий в военно-политических целях для осуществления действий, противоречащих международному праву, направленных против суверенитета, политической независимости, территориальной целостности государств и представляющих угрозу международному миру, безопасности, глобальной и региональной стабильности;

- 13. Основные внутренние военные опасности:

в) деятельность по информационному воздействию на население, в первую очередь на молодых граждан страны, имеющая целью подрыв исторических, духовных и патриотических традиций в области защиты Отечества;

- 15. Характерные черты и особенности современных военных конфликтов:

а) комплексное применение военной силы, политических, экономических, информационных и иных мер невоенного характера, реализуемых с широким использованием протестного потенциала населения и сил специальных операций;

- 21. Основные задачи Российской Федерации по сдерживанию и предотвращению военных конфликтов:

у) создание условий, обеспечивающих снижение риска использования информационных и коммуникационных технологий в военно-политических целях для осуществления действий, противоречащих международному праву, направленных против суверенитета, политической независимости, территориальной целостности государств и представляющих угрозу международному миру, безопасности, глобальной и региональной стабильности.

- 35. Основные задачи развития военной организации:

к) совершенствование системы информационной безопасности Вооруженных Сил, других войск и органов;

46. Задачи оснащения Вооруженных Сил, других войск и органов вооружением, военной и специальной техникой:

- в) развитие сил и средств информационного противоборства;
- г) качественное совершенствование средств информационного обмена на основе использования современных технологий и международных стандартов, а также единого информационного пространства Вооруженных Сил, других войск и органов как части информационного пространства Российской Федерации;
- ж) создание базовых информационно-управляющих систем и их интеграция с системами управления оружием и комплексами средств автоматизации органов управления стратегического, оперативно-стратегического, оперативного, оперативно-тактического и тактического масштаба.

55. Задачи военно-политического сотрудничества:

- е) развитие диалога с заинтересованными государствами о национальных подходах к противодействию военным опасностям и военным угрозам, возникающим в связи с масштабным использованием информационных и коммуникационных технологий в военно-политических целях;

«Доктрина информационной безопасности Российской Федерации»

(Указ Президента Российской Федерации № 646 от 05.12.2016 г.)

1. Настоящая Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.
2. В настоящей Доктрине на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации.
3. Правовую основу настоящей Доктрины составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, федеральные законы, а также нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации.
4. Настоящая Доктрина является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности.

- **Информационная безопасность Российской Федерации** - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.
- **Информация** - сведения (сообщения, данные) независимо от формы их представления.

Основным *содержанием* обеспечения ИБ должна являться работа по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности Российской Федерации:

- **прогнозирование** (выявление) угроз ИБ;
- **защита** информационных объектов;
- комплексное **противодействие** угрозам ИБ;
- целенаправленное **воздействие** на объекты, представляющие угрозу ИБ.

Составляющие информационной безопасности, согласно Доктрине информационной безопасности (Указ Президента Российской Федерации № 646 от 05.12.2016 г.)

Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации.

Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности. При этом практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

Стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

В Ы В О Д

«Доктрина информационной безопасности Российской Федерации» (Указ Президента Российской Федерации № 646 от 05.12.2016 г.)

Сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательных решений таких з а д а ч, как:

1. Разработка основных направлений в области обеспечения информационной безопасности, а также мероприятий и механизмов, связанных с реализацией этой политики

2. Развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области

3. Разработка федеральных целевых программ обеспечения информационной безопасности

4. Разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Российской Федерации

5. Совершенствование нормативной базы обеспечения информационной безопасности

6. Установление ответственности должностных лиц органов государственной власти субъектов РФ, органов местного самоуправления, юридических лиц за соблюдением требований информационной безопасности

7. Развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны

Выписка из Доктрины информационной безопасности Российской Федерации

утвержденной Указом Президента РФ № 646 от 5 декабря 2016 года

12. Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий.

Наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.

13. Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

- 21. В соответствии с военной политикой Российской Федерации основными направлениями обеспечения информационной безопасности в области обороны страны являются:

д) нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества.

- 23. Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;

к) нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей.

УКАЗ ПРЕЗИДЕНТА УКРАИНЫ № 47/2017

О решении Совета национальной безопасности и обороны Украины от 29 декабря 2016 года «О Доктрине информационной безопасности Украины»

2. Цель и принципы Доктрины

Целью Доктрины является уточнение принципов формирования и реализации государственной информационной политики, прежде всего по противодействию разрушительному информационному воздействию Российской Федерации в условиях развязанной ею гибридной войны.

3. Национальные интересы Украины в информационной сфере

2) жизненно важные интересы общества и государства:

защита украинского общества от агрессивного воздействия деструктивной пропаганды, прежде всего со стороны Российской Федерации;

защита украинского общества от агрессивного информационного воздействия Российской Федерации, направленного на пропаганду войны, разжигание национальной и религиозной вражды, изменение конституционного строя насильственным путем или нарушение суверенитета и территориальной целостности Украины;

- **5. Приоритеты государственной политики в информационной сфере**
  - выявление и привлечение к ответственности в соответствии с законодательством субъектов украинского информационного пространства, которые созданы и/или используются государством-агрессором для ведения информационной войны против Украины, и пресечения их подрывной деятельности;
  - невозможность свободного оборота информационной продукции (печатной и электронной), прежде всего происхождением с территории государства-агрессора, содержащей пропаганду войны, национальной и религиозной вражды, изменения конституционного строя насильственным путем или нарушение суверенитета и территориальной целостности Украины, провоцирует массовые беспорядки;
- **6. Механизм реализации Доктрины**
  - Министерство культуры Украины, Государственное агентство Украины по вопросам кино, Национальный совет Украины по вопросам телевидения и радиовещания, Государственный комитет телевидения и радиовещания Украины согласно компетенции должны участвовать в обеспечении защиты украинского информационного пространства от пропагандистской аудиовизуальной и печатной продукции государства-агрессора; разрабатывать приоритеты и стимулы развития украинского кино, телевизионного контента, книгопечатания, в частности освещение героического сопротивления Украинского народа российской агрессии.

Организационная структура системы обеспечения информационной безопасности Российской Федерации

Раздел 2. Угрозы информационной безопасности Российской Федерации

Управляемый хаос – *это новая технология борьбы без правил за геополитическое могущество, не контролируемая международными нормами.*

Збигнев Бжезинский, политолог, социолог, автор книги «Великая шахматная доска: господство Америки и ее геостратегические императивы»

Джин Шарп, общественный деятель, автор книги «198 методов ненасильственных действий»

Стивен Манн, автор статья «Теория хаоса и стратегическая мысль»

«Сегодня «гибридные действия» - это контроль над средствами информации, экономические санкции, деятельность в киберпространстве, поддержка внутренних волнений, наконец, использование специальных подразделений и специалистов для совершения терактов, диверсий и саботажа. Данный перечень, наверное, можно продолжать и дальше, но есть важная деталь. Для их успешной реализации в наш век необходимы глобальные и всепроникающие СМИ, обладание и превосходство в информационных и телекоммуникационных технологиях, сосредоточение у себя рычагов управления мировой финансовой системой, а также опыт использования сил специального назначения в других странах. Кто, кроме США и Великобритании, обладает ещё таким потенциалом?».

Министр обороны РФ С.К. Шойгу

Сегодня в эпоху глобализации, ослабления государственных границ, развития средств коммуникации важнейшим фактором стало изменение форм разрешения межгосударственных противоречий. В современных конфликтах все чаще акцент используемых методов борьбы смещается в сторону комплексного применения политических, экономических, информационных и других невоенных мер, реализуемых с опорой на военную силу. Это так называемые гибридные методы.

Их содержание заключается в достижении политических целей с минимальным вооруженным воздействием на противника. Преимущественно за счет подрыва его военного и экономического потенциала, информационно-психологического давления, активной поддержки внутренней оппозиции, партизанских и диверсионных методов. В качестве главного средства используются «цветные революции», которые, по мнению инициирующих их сторон, должны привести к ненасильственной смене власти в стане оппонента. По сути любая «цветная революция» – это государственный переворот, организованный извне. А в основе лежат информационные технологии, предусматривающие манипуляцию протестным потенциалом населения в сочетании с другими невоенными средствами.

Важное значение при этом приобретает массированное, целенаправленное воздействие на сознание граждан государств – объектов агрессии посредством глобальной сети Интернет. Информационные ресурсы стали одним из самых эффективных видов оружия. Широкое их использование позволяет в считаные дни раскачать ситуацию в стране изнутри.

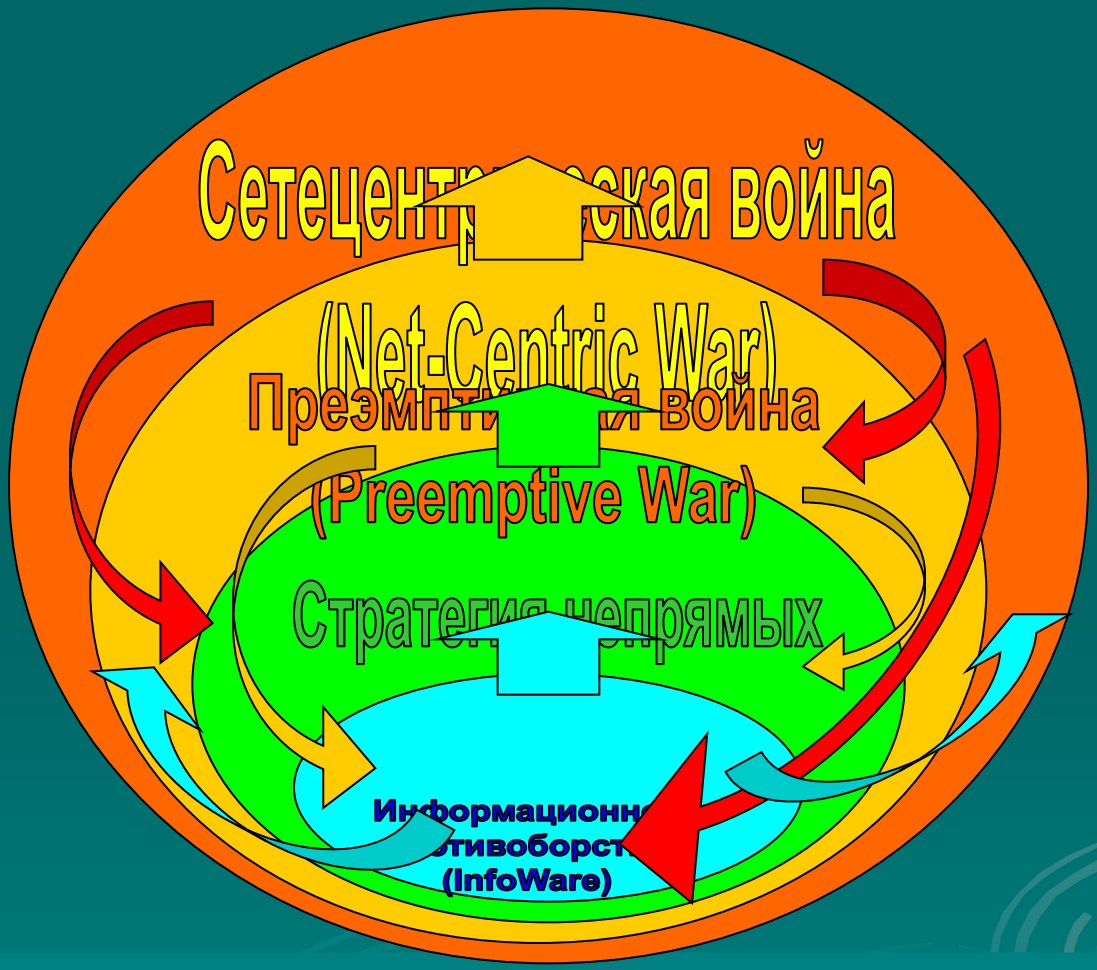
Начальник Генерального штаба Вооруженных С ил РФ , генерал армии Валерий Герасимов

Угрозы ИБ РФ определяются:

- **сферами информационного противоборства:**
  - **информационно-техническая;**
  - **информационно-психологическая**
- **форматом глобальной гибридной войны;**
- **сетецентрической организацией согласованных информационных операций против РФ;**
- **стратегией непрямых действий**

Сетецентрический формат глобальной гибридной войны

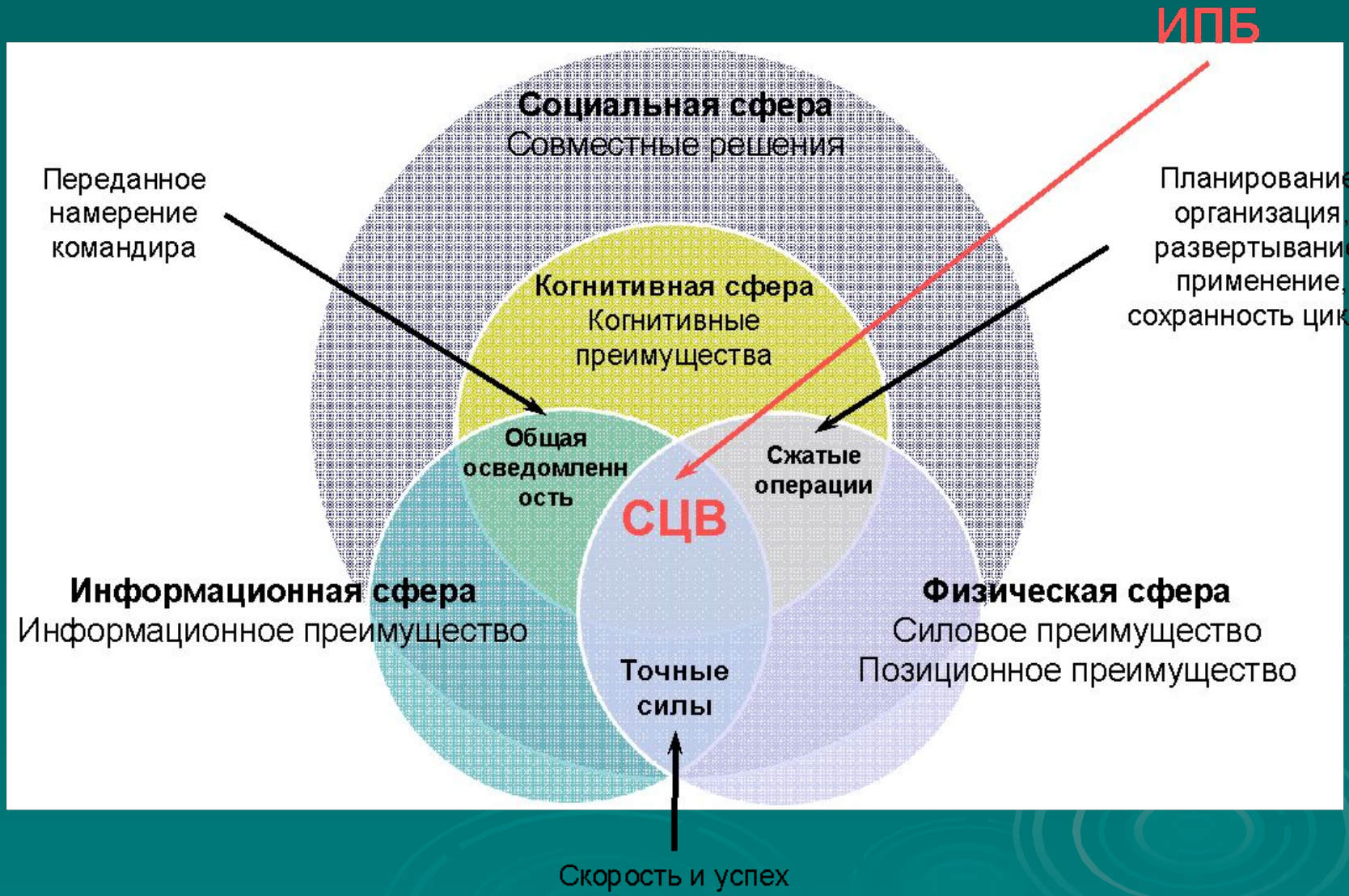
Соотношение составляющих концептов действующих в США доктрин достижения стратегической униполярной гегемонии в XXI веке



-

- прямые воздействия «по восходящей» траектории;
- обратные воздействия «по нисходящей» траектории.

ИПБ: сферы и конфликты



Этапы ведения гибридной войны

1 этап. Формализация модели ведения гибридной войны

2 этап. Определение критериев упреждающего выявления на ранней стадии признаков потери устойчивости СДС

3 этап. Создание технологий выявления признаков информационных атак на СДС на ранней стадии («социальный радар»

4 этап. Ситуативный анализ обстановки.

- Создание технологий анализа выявленных деструктивных воздействий, их источников, используемых сил и средств.
- Выявление значимых параметров.
- Определение сценариев возможного развития событий по складывающейся ситуации.
- Выработка мер и задействование необходимых сил и средств по перехвату управления развитием ситуации.
- Прогнозирование развития ситуации и определения степени достаточности и необходимости задействования сил и средств при организации ответных действий.
- Принятие решения по ответным мерам.
- Выдача управляющих указаний (приказов) на проведение от

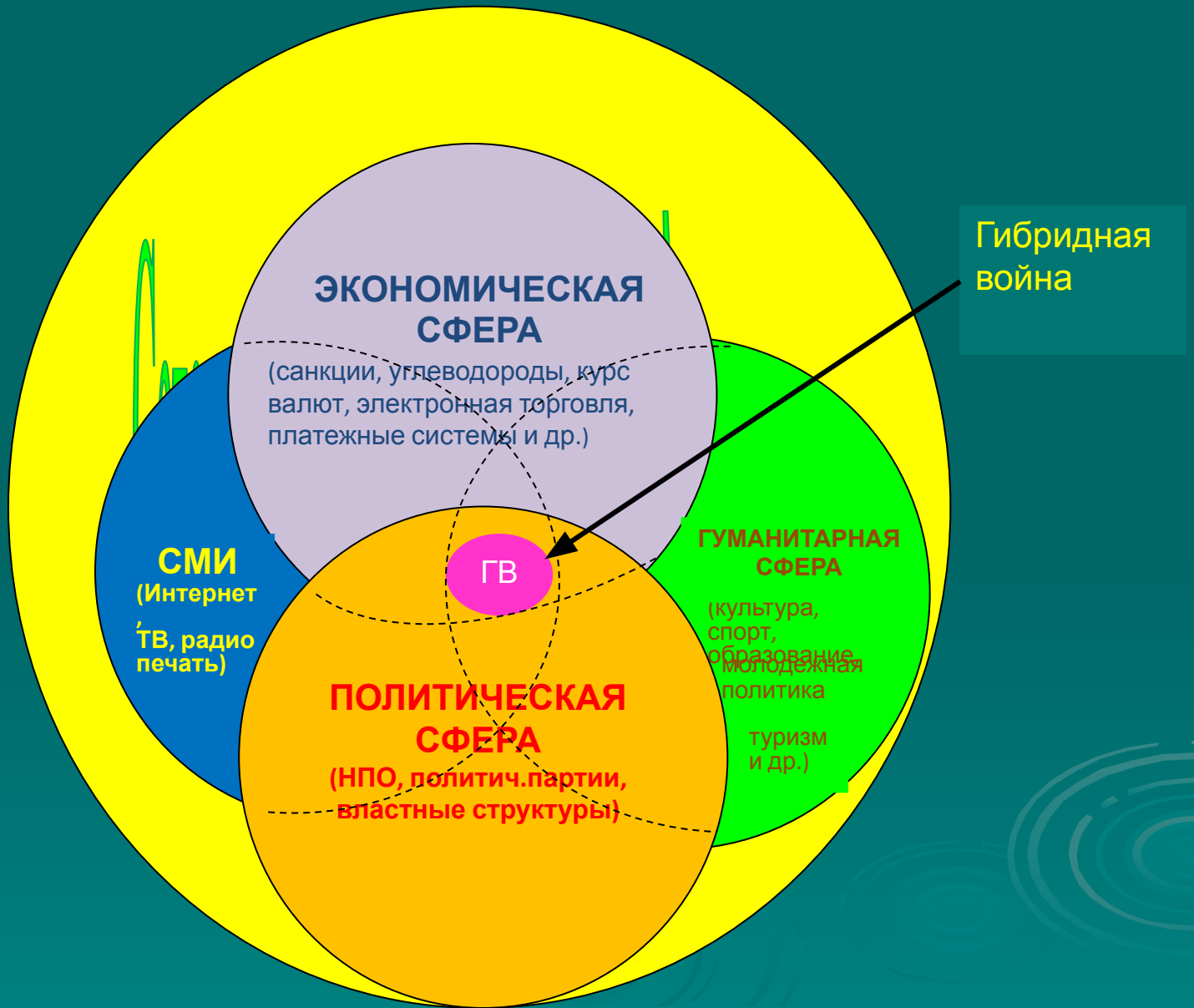
5 этап. Проведение ответной информационной операции

- Перехват сценарного управления развитием критической ситуации.
- Запуск рефлексивных механизмов управления действиями противника.
- Схлопывание критическим развитием ситуации потери устойчивости СДС.
- Расстройка когерентности «социального лазера»: недопущение возникновения «инверсии населенности» верхнего уровня «протестной энергии масс».
- Запуск механизмов управляемой диффузии боевых мемов в информационных ресурсах противника.
- Применение стратегического информационного оружия как против ПАП, так и против общественного и группового сознания.
- Запуск «социального лазера» разрушения СДС противника.

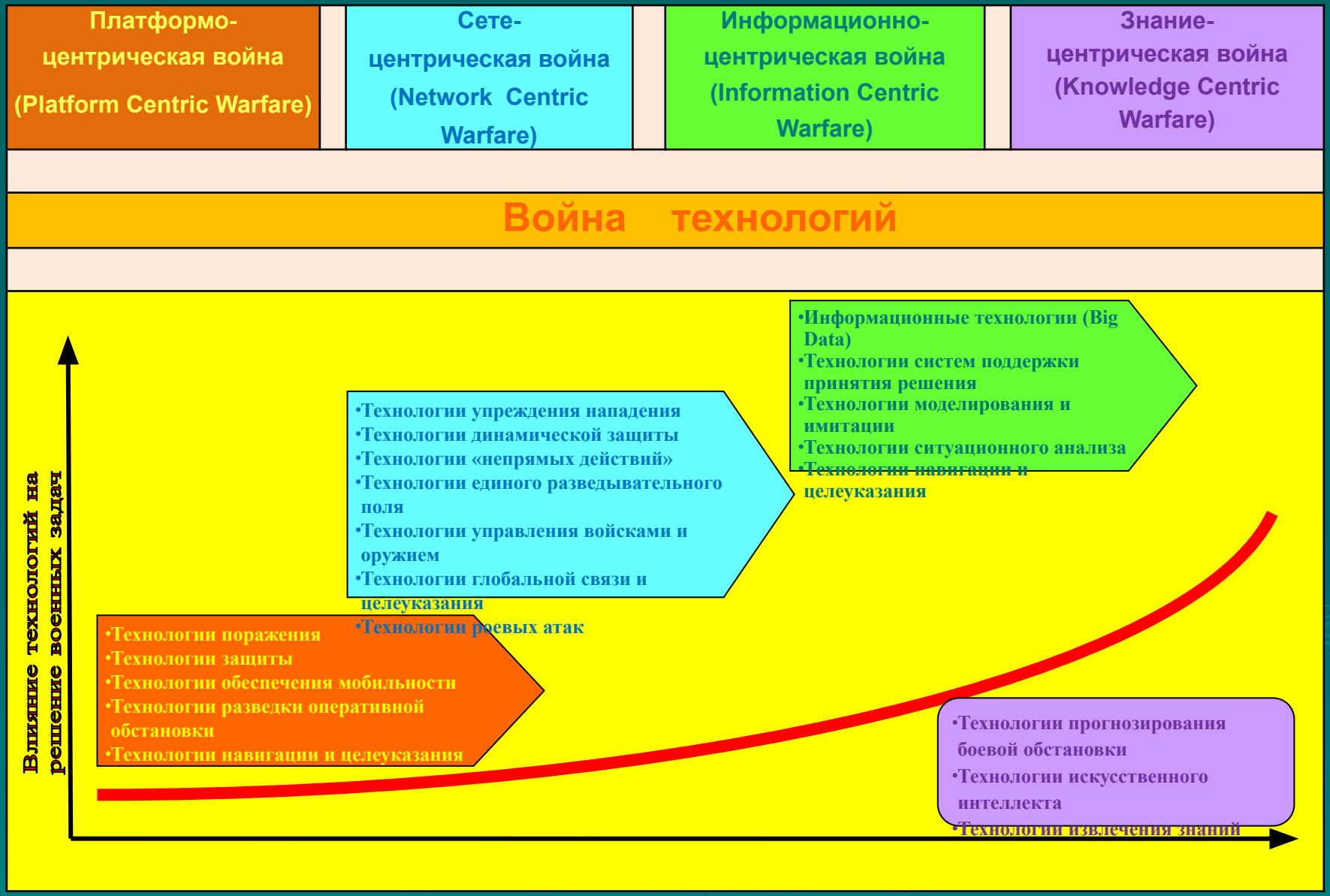
Сущность сетецентрического формата гибридной войны

- Под гибридной войной следует понимать комбинацию традиционных элементов обычной войны с нетрадиционными аспектами террора, подрывных действий, а также технологиями интенсивного управления общественным мнением личного состава Вооруженных Сил и населения противоборствующих сторон (государств) посредством сил и средств современного информационно-коммуникативного технологического уклада.
- Центральным звеном гибридной войны является ≪сетевая агрессия≫, сетецентрический формат гибридной войны. В концептуальном плане, сетецентризм гибридной войны основан на обеспечении превосходства над вероятным противником за счет применения современных инфокоммуникационных систем, позволяющих интегрировать потенциальных участников боевых действий и всю совокупность звеньев боевого управления в единую сеть.
- Концептуальная модель сетецентрической войны включает в себя три подсистемы: информационную, сенсорную (разведывательную), боевую (средства поражения, боевая техника, личный состав). При этом основу сетецентрической системы составляет информационная подсистема, характер которой определяется характером и уровнем развития физической и когнитивной сфер.
- Идеология ≪сетецентризма≫ базируется на активном применении в современной гибридной войне тактических приемов арсенала социальных сетей и новых медиа: ≪традиционных СМИ, интегрированных в пространство интернет-коммуникаций; СМИ, изначально созданных как Интернет-медиа; в принципе всей системы контента сетевых ресурсов≫

Сетецентрический формат гибридной войны



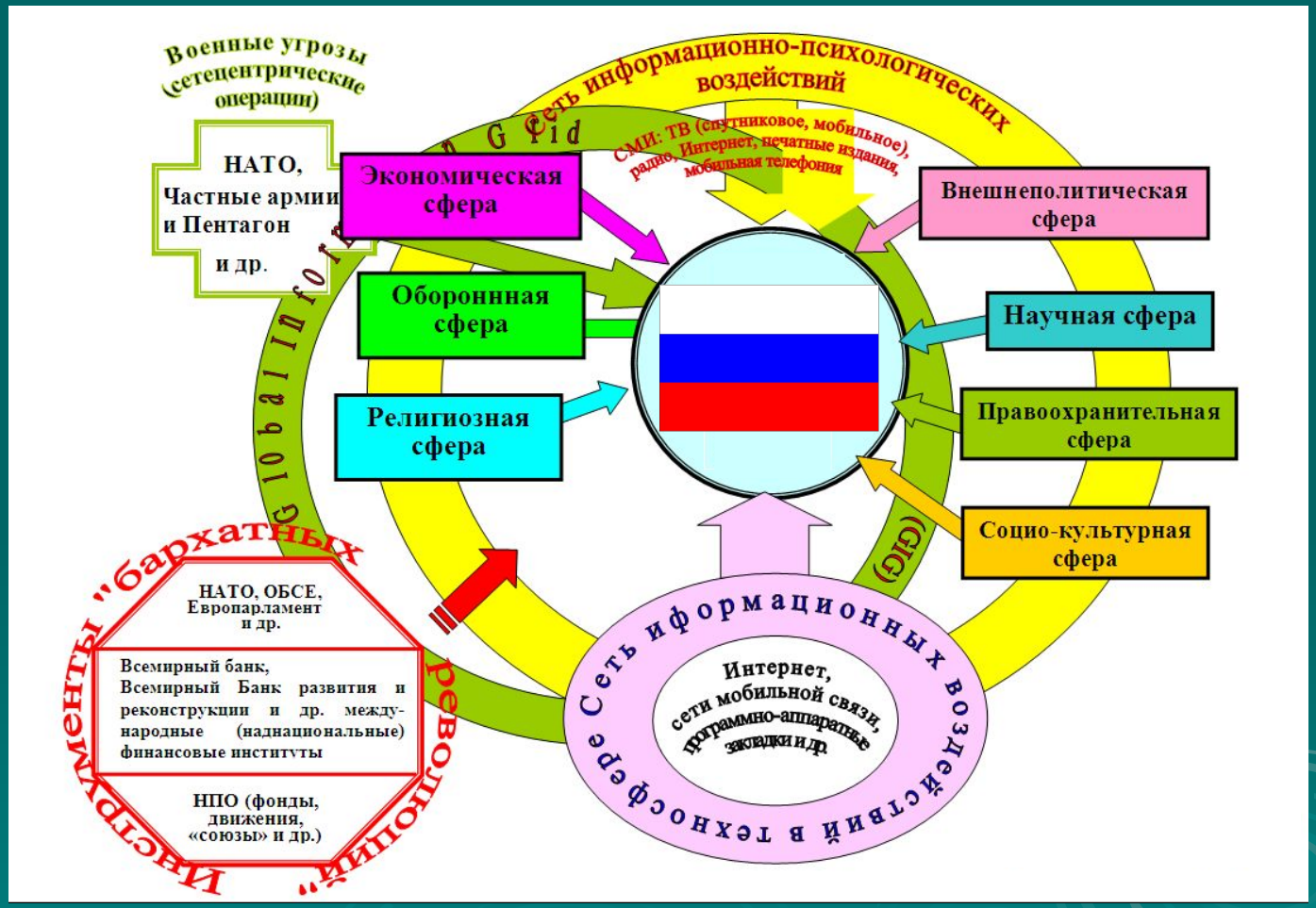
Эволюционное развитие концепций ведения боевых действий



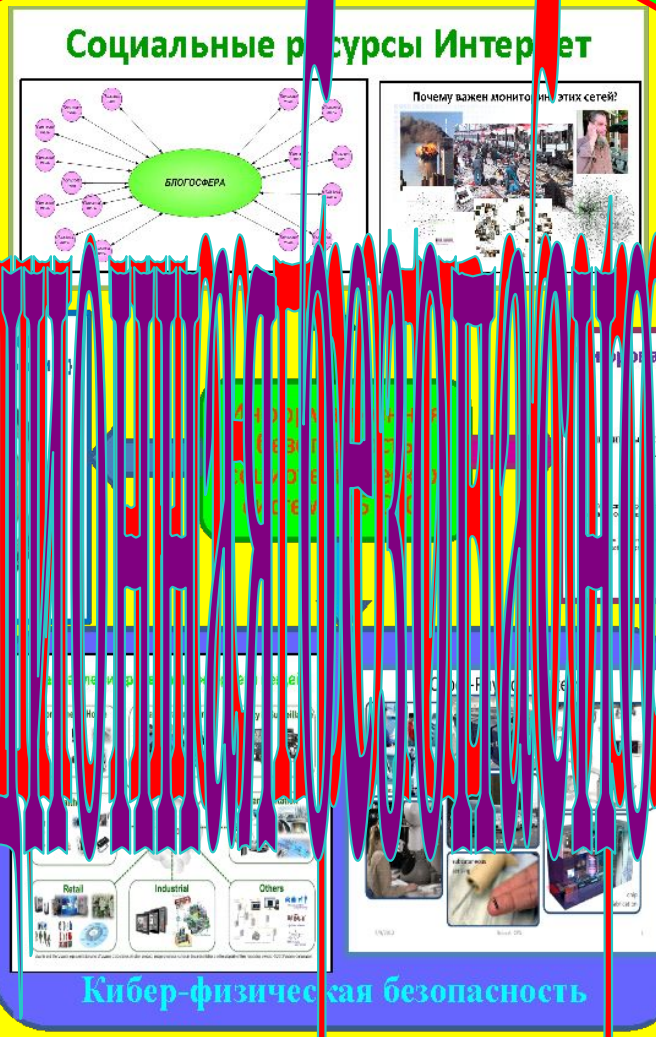
СЕТЕЦЕНТРИЧЕСКИЕ ОПЕРАЦИИ ПРОТИВ РОССИИ

Сетевая организация неправительственных фондов

Многомерное пространство ведения сетецентрических операций против России



Информационная безопасность в сети



- Благодарю за внимание!

70. Для решения задач национальной безопасности в области науки, технологий и образования необходимы: развитие перспективных высоких технологий (генная инженерия, робототехника, биологические, информационные и коммуникационные, когнитивные технологии, нанотехнологии, природоподобные конвергентные технологии);

79. Угрозами национальной безопасности в области культуры являются размывание традиционных российских духовно-нравственных ценностей и ослабление единства многонационального народа Российской Федерации путем внешней культурной и информационной экспансии (включая распространение низкокачественной продукции массовой культуры), пропаганды вседозволенности и насилия, расовой, национальной и религиозной нетерпимости, а также снижение роли русского языка в мире, качества его преподавания в России и за рубежом, попытки фальсификации российской и мировой истории, противоправные посягательства на объекты культуры.

82. Укреплению национальной безопасности в области культуры способствуют:

обеспечение культурного суверенитета Российской Федерации посредством принятия мер по защите российского общества от внешней идейно-ценностной экспансии и деструктивного информационно-психологического воздействия, осуществление контроля в информационной сфере и недопущение распространения продукции экстремистского содержания, пропаганды насилия, расовой, религиозной и межнациональной нетерпимости;