Кафедра международной и национальной безопасности

Москва-2017

ДИПЛОМАТИЧЕСКАЯ АКАДЕМИЯ МИД РОССИИ

Кафедра Национальной и международной безопасности

Курс: «Проблемы войны и мира в СМО»

Магистратура факультета «Международные отношения»

Программа «Международная безопасность»

Профессор кафедры национальной и международной безопасности
Миронов Сергей Иванович

Тема лекции: ПРОТИВОБОРСТВО И БЕЗОПАСНОСТЬ РОССИИ В ИНФОРМАЦИОННОЙ СФЕРЕ

Целевая установка занятия

1. Дать основные теоретические подходы к понятиям «информационная борьба» и «информационное противоборство».
2. Раскрыть сущность новых вызовов и угроз России в информационной сфере, а также мер по обеспечению ее информационной безопасности.

ВОПРОСЫ ЛЕКЦИИ

1. Теоретические подходы к информационной борьбе (информационному противоборству).
2. Новые вызовы и угрозы России в информационной сфере и меры по обеспечению ее информационной безопасности.

Литература :

- Анненков В.И., Баранов С.Н., Волохов В.И., Миронов С.И. Международная безопасность: геополитические и военно-политические аспекты современности / Под общей ред. проф. Анненкова В.И. Учебник. – М.: РУСАВИА, 2015. – 512 с.
- Попов И.М., Хамзатов М.М. Война будущего: Концептуальные основы и практические выводы. Очерки стратегической мысли – М.: Кучково поле, 2016. – 832 с.
- Безопасность и противоборство в информационной сфере: аспекты национальной безопасности. Учебное пособие / Под общей редакцией профессора В.И.Анненкова. М.:РУСАВИА. 2010. С. – 68.
- Война и мир в терминах и определениях. Военно-политический словарь / Под общ. ред. Д.О.Рогозина. – М.: Вече, 2011. – 640 с.
- Доктрина информационной безопасности РФ. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646
- «Основы государственной политики в области международной информационной безопасности до 2020 года». Утверждены Президентом Российской Федерации В. Путиным 24 июля 2013 г., № Пр-1753.
- Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Первый учебный вопрос

1. Теоретические подходы к информационной борьбе (информационному противоборству).

«Информация» (от латинского **informatio** – разъяснение, изложение).

Основные аспекты понятия «информация»

обыденный | **естественнонаучный** | **философский**

В обыденном понимании информация – это сведения об окружающем мире и протекающих в нем процессах, воспринимаемые различными потребителями (человеком, другими живыми организмами или специальными техническими устройствами) для обеспечения целенаправленной деятельности.

В естественнонаучном смысле информацию можно определить как свойство материи, состоящее в том, что в результате взаимодействия объектов между их состояниями устанавливается определенное соответствие. Чем сильнее выражено это соответствие, тем полнее состояние одного объекта отражает состояние другого объекта, тем больше информации один объект содержит о другом.

В философском понимании понятие информации рассматривается как фундаментальное свойство материи, являющееся аспектом свойства отражения.

ИНФОРМАЦИЯ

В широком смысле

свойство объектов (процессов) окружающего материального мира порождать разнообразие состояний, которые посредством отражения передаются от одного объекта к другому.

В узком смысле

сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Обобщая все вышесказанное можем сказать, что **информация – это**:

- **сведения об объектах и процессах** любой природы, **обладающие определенной**, зависящей от времени, **полезностью для некоторого лица**, принимающего решение **(прагматический аспект)**;
- **отражающие существенные** (с точки зрения этого лица) **свойства объектов или процессов** с определенной степенью точности и достаточности **(семантический аспект)**;
- представляемые с помощью определенной знаковой системы **(синтаксический аспект)**;
- **материально существующие** с помощью вещественно-энергетических носителей (электромагнитные излучения, бумага, магнитные носители и т.п.).

УРОВНИ ИНФОРМАЦИОННОЙ БОРЬБЫ (ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА):

вещественно-энергетический – борьба на уровне носителей информации, то есть все виды скрытия информации и уничтожения информационных систем, каналов и информации в них

синтаксический – борьба на уровне структур знаковых систем, то есть все виды кодирования, использование шифров и т.п.

семантический – борьба на уровне смыслового содержания информации, то есть предоставление противнику бессмысленной или недостоверной информации (дезинформация)

прагматический – борьба на уровне полезности информации, то есть либо изменения целей противостоящей стороне по отношению к использованию информации, либо предоставление ему бесполезной информации

Противоборство

тип взаимоотношений между сторонами, характеризующихся наличием антагонистических противоречий или состояние, характеризующее взаимоотношение сторон, при котором между ними существуют антагонистические противоречия

Борьба

активное столкновение общественных групп, противоположных направлений, интересов и т.д., в котором каждая сторона стремится получить господство, перевес

Противоборство

это состояние, которое может продолжаться неопределенно долго (например, ядерное противоборство сверхдержав или современное информационное противоборство) и может иметь место в политической, военной (военная и военно-политическая конфронтация), экономической, энергетической, морально-психологической, идеологической, информационной и других сферах.

Некоторые определения в области информационного противоборства

Достаточно широкое **определение "информационного противоборства"** предлагают Г.М. Шушков И.В. Сергеев: **«**соперничество субъектов информационного конфликта с целью усиления влияния на те или иные сферы социальных отношений**,** итогом которых становится получение преимущества одной противоборствующей стороной и утрата подобных преимуществ другой**»**

Информационное противоборство — соперничество социальных систем в информационно-психологической сфере с целью усиления влияния на те или иные сферы социальных отношений и установления контроля над источниками стратегических ресурсов**,** в результате которого одни участники соперничества получают преимущества**,** необходимые им для дальнейшего развития**,** а другие их утрачивают**.**

Информационная война

Процесс противоборства человеческих общностей, направленный на достижение политических, экономических, военных или иных целей стратегического уровня, путём воздействия на гражданское население, власти и (или) вооруженные силы противостоящей стороны, посредством распространения специально отобранной и подготовленной информации, информационных материалов, и, противодействия таким воздействиям на собственную сторону.

Термин «информационно-психологическая война» был заимствован в русский язык из словаря военных кругов США. Перевод этого термина («information and psychological warfare») с английского языка может звучать и как «информационное противоборство», и как «информационная, психологическая война».

Целенаправленные действия, предпринятые для достижения информационного превосходства путём нанесения ущерба информации, информационным процессам и информационным системам противника при одновременной защите собственной информации, информационных процессов и информационных систем

Некоторые определения в области информационной борьбы

Информация существует и движется в некоторой части материального мира, которую, как правило, называют «информационной средой».

Не следует путать геофизическое понятие «среда» и понятие «сфера», которое определяет границы взаимодействия сторон в конкретной «среде» (средах).

Движение информации в пространстве и времени называется «информационным процессом».

Процессы **сбора, обработки, накопления, хранения, поиска и распространения информации – это информационные процессы.**

Информационную сферу можно определить как часть информационной среды, в которой возникают, развиваются, существуют и исчезают информационные процессы, которые в свою очередь являются следствием взаимоотношений конкретных сторон (государств, коалиций государств и т.д.).

Некоторые определения в области информационной борьбы

Совокупность **структурированной по определённому правилу информации, предназначенной для органов управления (**лиц принимающих решение**)** при решения конкретных задач**,** будем называть **информационным полем.**

Возрастание роли и значения информационной составляющей в отношениях между сторонами (государствами) привело к возникновению терминов

- **«информационная борьба»**
- **«информационное противоборство»**
- **«информационная война»**

Информационный ресурс

В соответствии с Федеральным законом от **27** июля **2006** г. № **149**-ФЗ «Об информации, информационных технологиях и о защите информации» понятие информационного ресурса сводится лишь к **совокупности массивов документированной информации (документов).** В статье **2** данного Закона прямо указывается, что его действие **«распространяется на конкретный класс информации – на информацию документированную, то есть уже полученную, объективированную и зафиксированную на материальном носителе».**

Данное положение **недопустимо сужает смысл исследуемого понятия – информационный ресурс, особенно в военной области.**

Множество документированной информации является лишь частью всей информации, циркулирующей в военных органах управления и различных системах. Так, передаваемые распоряжения, команды (сигналы) по линиям связи, сведения с датчиков разведки, навигации, метеорологии и др., вся эта и многая другая информация явно не укладываются в понятие документа.

Информационный ресурс

Необходимо учитывать при определении информационного ресурса в военной области

информацион-ные системы (включая людей, занимающихся восприятием, обработкой, хранением и передачей информации и принимающих решения)

информационные каналы (образуемые системами-источниками информации, системами-получателями информации, а также среду существования (распространения) носителей информации)

собственно **информацию**, находящуюся и циркулирующую в информационных системах (библиотеках, архивах, фондах, банках данных)

Информационный ресурс

Воздействие на материальные элементы (информационные объекты) информационного ресурса – один из аспектов достижения цели при поражении информационного ресурса противника.

ЦЕЛЬ

воздействие непосредственно на информацию (ее достоверность, полноту, целостность

Информационное воздействие – специально организованное действие (процесс, совокупность приёмов), которое направлено на уменьшение (затруднение процесса наращивания, использования) информационного ресурса противостоящей стороны (сторон), а также создание в информационной сфере противостоящей стороны условий (ситуации), при которых она принимает выгодные для нас решения.

Информационное оружие

Информационное оружие – технические, программные и иные специальные средства, конструктивно предназначенные для воздействия на информационные объекты информационного ресурса.

Понятие «информационное оружие» в широком смысле определить однозначно, в настоящее время, **не представляется возможным,** поэтому целесообразно использовать понятие **«средство информационной борьбы (информационного противоборства)»,** или **«средство информационного воздействия»,** которое конкретизируется при определении воздействия

Средства информационной борьбы (информационного противоборства) это специальные технические устройства, информационные технологии, лингвистические и программные продукты, с помощью которых обеспечивается информационное воздействие на информационный ресурс (объекты информационного ресурса) противника и осуществляется защита своего информационного ресурса (объектов информационного ресурса).

Средства информационной борьбы (информационного противодействия)

- средства радиоэлектронной борьбы, включая средства технической дезинформации
- специальные программные и другие средства воздействия на АСУ и ЭВТ
- психотропные генераторы
- специальные фармакологические средства и иные средства воздействия на личный состав вооруженных сил и население противостоящей стороны
- средства массовой информации (в том числе синтезаторы аудио и видео сообщений по ним), создания голографических изображений в атмосфере

Информационное превосходство в сфере управления

Это превосходство

- в своевременности, достоверности, полноте получения информации всеми органами управления
- в скорости и качестве её переработки и своевременности принятия решения
- в своевременном и достоверном доведении принятых решений (приказов) до исполнителей и достоверном контроле за их исполнением

Полное определение информационной борьбы

Совокупность действий и мероприятий, проводимых специальными силами по единому замыслу и планам органов управления различного уровня для достижения информационного превосходства в сфере управления за счет информационного воздействия на информационный ресурс противника и защиты своего информационного ресурса.

Второй учебный вопрос

2. Новые вызовы и угрозы России в информационной сфере и меры по обеспечению ее информационной безопасности

Нередко в упрощенном виде под **информационным противоборством** понимают **комплексное информационное воздействие на систему государственного и военного управления** противостоящей стороны, на ее военно-политическое руководство и население.

Интенсивное внедрение информационных технологий

Рост удельного веса безопасности информации в обеспечении национальной безопасности государства

Информационный ресурс становится сегодня таким же богатством страны как и традиционные ресурсы

Превращение информации в товар

Резкое **обострение международной конкуренции за обладание информационными рынками, технологиями и ресурсами**, а **информационная сфера** в значительной мере определяет и влияет на состояние экономической, оборонной, социальной, политической и других составляющих национальной безопасности страны.

Возросшее и принимающее все более острые формы за последние годы соперничество в информационной сфере позволяет **назвать это соперничество – информационным противоборством.**

Суть информационного противоборства состоит **в достижении какой-либо страной** (или группой стран) **подавляющего преимущества в информационной области, позволяющего** с достаточно высокой степенью достоверности **моделировать поведение «противника» и оказывать на него** (в явной или скрытой формах) **выгодное для себя влияние.**

Особенности информационного противоборства и угрозы национальной безопасности России в этой сфере

Страны, проигравшие информационную войну, проигрывают ее «навсегда», поскольку их возможные шаги по изменению ситуации требуют колоссальных материальных и интеллектуальных затрат и будут контролироваться и нейтрализоваться победившей стороной.

Операции таких войн не обязательно должны проводиться только вооруженными силами и быть направлены против военных объектов. Другие правительственные ведомства, агентства и организации, промышленные и коммерческие структуры также могут принимать в них участие и самостоятельно проводить информационные операции, которые могут существенно влиять на ход и исход любого конфликта.

Информационное противоборство – это война без линии фронта, а проведение многих операций информационной войны практически невозможно обнаружить, а если такие факты и отмечаются, они с большой вероятностью остаются анонимными. Какие-либо международные, юридические и моральные нормы ведения информационной войны полностью отсутствуют.

Невысокая стоимость технических средств, которые могут быть использованы в информационной войне, существенно расширяет круг ее возможных участников

- **отдельные страны и их органы разведки**
- **коммерческие фирмы**
- **преступные, террористические и наркобизнесные группировки**
- **лица, действующие без преступных намерений**

Все формы информационной войны сводятся к воздействию на инфраструктуру противника, его телекоммуникационные системы с целью уничтожения или искажения получаемой информации, лишения его возможности получения новой достоверной информации, уничтожения его информационных средств, а также к обеспечению защиты собственных информационных ресурсов от аналогичных действий противника.

Основная стратегическая цель информационной войны состоит в перепрограммировании личности человека. Другими словами, цель состоит в том, чтобы человек сам, по доброй воле, а не под угрозой физической расправы воспринял за белое то, что до него годами считалось черным. Зачастую такое изменение взглядов идет во вред самому человеку, но он, оболваненный пропагандой, этого совершенно не воспринимает. Понятно, что одномоментно реализовать такое невозможно, необходима долгая, многолетняя и кропотливая работа. У человека должны сформироваться новые координаты его собственного миропонимания: что он воспринимает в качестве добра и зла, к чему стремится. И здесь огромную роль играют телевидение, кинематограф, мультимедийные продукты в компьютерной среде.

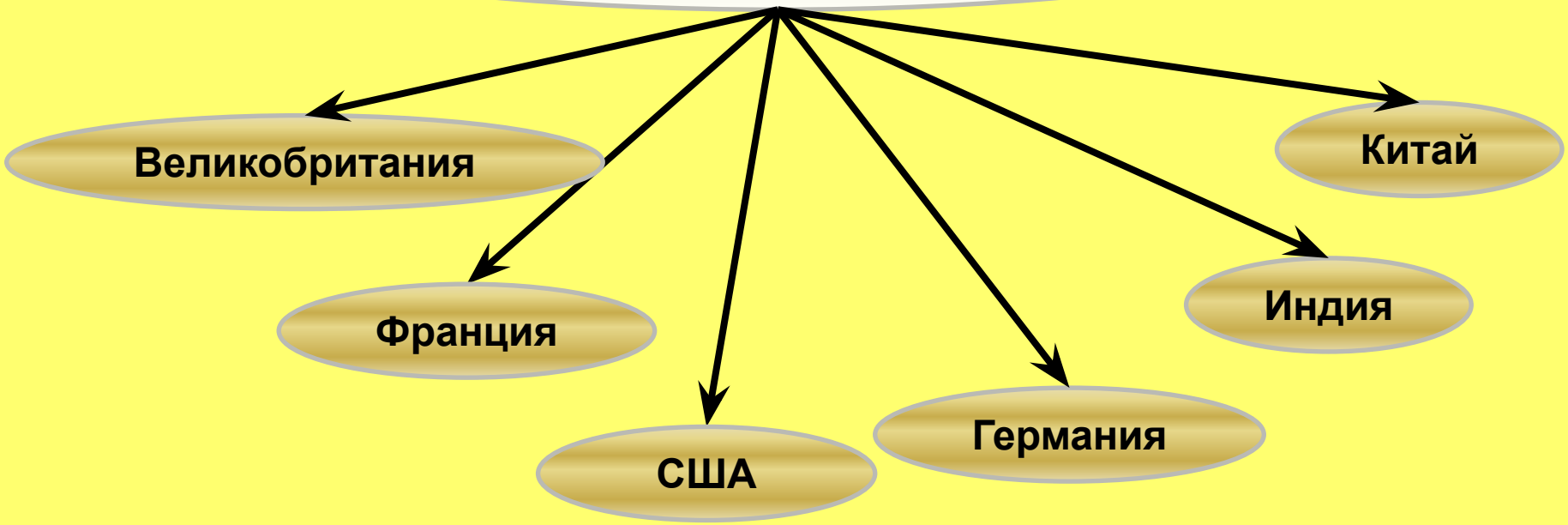
Известен фетиш – «американский стиль жизни». А что он реально из себя представляет? Массу проблем этнических групп в самих США, чудовищный государственный долг, банкротство целых городов по примеру Детройта, участившиеся случаи массовых расстрелов в американских школах, университетах и улицах городов. А кто главные герои многих американских фильмов: это как правило, либо бандит, либо нечистый на руку финансист, либо умственно неполноценный идиот, либо еще кто-то с непонятными целями в жизни. А какие американские «телевизионные штампы» копируют наши коммерческие ТВ-каналы типа ТНТ – они рассчитаны на самые низменные запросы человека: плоские, тупые шутки, на которые надо реагировать смехом, на что указывает закадровый смех, постоянное жевание фастфуда и т.д.

Стратегия информационной войны

Но для победы в информационной войне мало сформировать «образ героя», к кому должен тянуться человек, необходимо еще показать ущербность, неполноценность твоей истории и твоего текущего восприятия жизни. Но история хранится в «народной памяти» и надо «работать» с этой самой памятью, чтобы стереть то, что противоречит новым установкам и сохранить то, что в них укладывается. И вот когда, спустя годы, сформировавшийся таким образом человек вливается в общество и занимает руководящие посты в нем, вот тогда можно говорить о торжестве проводимой стратегической линии: для такого индивида все его наследие и гроша не стоит, он преклоняется перед теми фетишами, которые созерцал все предыдущие годы. Можно ли ждать национальных решений от такого руководителя? Чьи интересы он будет скорее защищать?

С сожалением следует признать, что сегодня мы проигрываем в стратегии информационной войны. Сегодня недостаточно фильмов, мало книг о российской истории издается не только в дальнем и в ближнем зарубежье, но и в самой России. Совершенно недостаточно снимается художественных фильмов о нашей истории, а те, что получают финансирование – далеки от исторической правды. Сегодня в кинематографе не принято пользоваться услугами профессиональных консультантов – результат этого весьма плачевен.

Ряд развитых государств мира активно наращивают усилия по достижению глобального доминирования в информационной сфере, что ведет к усилению всего спектра стратегических угроз безопасности Российской Федерации.



Наиболее активную роль в этом процессе играют США и их союзники. Согласно концепции «информационного превосходства», отраженной в документе о стратегии развития ВС США «Единая перспектива – 2020», преимущество в информационной сфере является одним из ключевых факторов успешного ведения боевых действий.

Для достижения целей концепции в **2009** году создано **Министерство кибербезопасности**, существенно **увеличен размер финансирования мероприятий**, направленных на развитие системы информационного противоборства США, совершенствование информационного оружия, форм, методов и способов его применения, а также проведение наступательных информационно-психологических операций (ИПО) в различных регионах мира, в число которых они включают, прежде всего, **регион под названием «БОЛЬШОЙ БЛИЖНИЙ ВОСТОК».**

В событиях в Ливии активно подключались, в том числе, подразделения «психологической войны» из стран Западной Европы.

В Сирии наряду с военными действиями со стороны т.н. оппозиции проводится информационно-психологическая операция с целью изменения существующего в стране режима.

Но самым большим полигоном по обкатке новейших средств информационной войны в настоящее время является Украина.

Новые угрозы информационной безопасности России

- использование информационных и коммуникационных технологий в военно-политических целях для осуществления действий, направленных против политической независимости, территориальной целостности и суверенитета, а также представляющих угрозу региональной и глобальной стабильности;
- усиление контроля со стороны США и их союзников над международным информационным пространством и, в первую очередь, над телекоммуникационными системами;
- формирование единой информационной инфраструктуры НАТО, отвечающей современным требованиям управления боевыми действиями и обеспечивающей повышение степени боеготовности вооруженных сил стран – участниц блока;
- введение и расширение против России экономических санкций, основанных на ее обвинении в эскалации военного конфликта на Украине;
- навязывание руководству европейских стран политических решений в отношении России, выгодных в основном США;

Новые угрозы информационной безопасности России

- противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов;
- создание условий для усиления технологической зависимости России в области современных информационных технологий;
- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
- увеличение оттока за рубеж специалистов в области информационных технологий.

Существенная роль в реализации замыслов ведения информационного противоборства отводится руководством США манипулированию общественно значимой информацией через средства массовой информации в планетарном масштабе.

Непосредственную угрозу безопасности России создают такие действия как:

- обоснование путей и сроков возможной дезинтеграции РФ на автономные территориальные образования с повышением самостоятельности ряда субъектов и регионов России (Калининградская область, Северный Кавказ, Поволжье, Сибирь, Дальний Восток и др.)
- усиленное формирования мирового общественного мнения об агрессивной и неконструктивной позиции России в отношении Украины
- распространение дезинформации о снижении роли России на международной арене как страны, не предсказуемой во внешнеполитических вопросах и, не самостоятельной в решении вопросов внутриэкономических, а также проблем безопасности личности и общества
- дезориентация мировой общественности в отношении способности руководства стран СНГ решать политические и экономические проблемы без тесного сотрудничества с США
- внесение раскола во взаимоотношения России с другими странами СНГ в целях их переориентации на более тесное сотрудничество с Западом

Новые информационные технологии

Сегодня западный мир пытается обвинить Россию в агрессии по отношению к Украине. Но поскольку у Запада нет прямых доказательств участия регулярных вооруженных сил России в событиях на территории ДНР и ЛНР, ведется поиск новых обоснований агрессии России в отношении Украины и попытки обвинить Россию в развязывании войны в отношении соседнего государства. Это делается, в частности, введением в дипломатический язык и мировое информационное поле термина «гибридная война».

Бывший советник НАТО, генерал-майор в отставке Франк ван Каппен охарактеризовал гибридную войну как «смешение классического ведения войны с использованием нерегулярных вооруженных формирований. Государство, которое ведет гибридную войну, совершает сделку с негосударственными исполнителями – боевиками, группами местного населения, организациями, связь с которыми формально полностью отрицается. Эти исполнители могут делать такие вещи, которые само государство делать не может, потому что любое государство обязано следовать Женевской конвенции и Гаагской конвенции о законах сухопутной войны, договоренностям с другими странами. Всю грязную работу можно переложить на плечи негосударственных формирований».

Новые информационные технологии

На Украине были «обкатаны» афганские и сирийские методы ведения гибридной войны. Собственно, «Евромайдан» и националистический «Правый сектор» тоже укладываются в логику ведения гибридных войн. Ведь формально к «Евромайдану» правительство США не имело никакого отношения, если не считать раздачу пирожков официальным представителем Госдепа Викторией Нуланд. Но как неоднократно отмечали наблюдатели, США довольно активно направляли майдановцев – и посредством методов «мягкой силы» (через разнообразные НКО), и посредством уговоров, давления и даже провокаций. По сути, США задействовали методику ведения гибридной войны – устроили мятеж с помощью местных «подпольщиков» из националистических группировок и недовольство рядовых граждан действующим президентом.

Отдельное место в списке инновационных подрывных технологий занимают цветные революции (технологии управляемого хаоса).

«Цветная революция» – это процесс подготовки и смены правящего режима государства посредством ненасильственных выступлений граждан, когда давление на власть осуществляется в форме политического шантажа, а основной движущей силой таранного удара по власти выступает специально организованное молодежное протестное движение. Он направлен на создание иллюзии легитимности решений и действий, принятых под давлением толп и маскирующих силовую нелегальную деятельность иностранных резидентов, а также предательство национальных интересов внутригосударственными элитарными группами.

Вовлечение России в глобальное информационное пространство

Новый вид угроз – угрозы международного кибертерроризма

Использование террористическими и криминальными группировками в мировом масштабе современных информационно-телекоммуникационных технологий для проведения террористических операций по отношению к критически важным элементам национальной информационной инфраструктуры.

Некоторые эпизоды кибертерроризма

- В конце ноября 2010 года президент Ирана М.Ахмадинежад признал, что появившаяся недавно обновленная новая версия сетевого червя STUXNET все же повредила несколько урановых центрефуг, чем нанесла вред иранской ядерной программе
- В ноябре 2010 года масштабная компьютерная атака оставила Бирму (Мьянму) без Интернета накануне первых за последние 20 лет выборов
- Разразившийся скандал с сайтом Wikileaks, который сам по себе условно можно назвать кибертеррористическим, стал поводом для новых сетевых баталий сторонников и противников Ассанжа. Среди потерпевших такие компании, как MasterCard и Visa

Угрозу обеспечения национальной безопасности России в ряде случаев несет деятельность электронных средств массовой информации в условиях борьбы с терроризмом. Наиболее убедительное подтверждение это положение получило в ходе проведения в России террористических актов: особенно при захвате школы в г. Беслане, в ТЦ на Дубровке в Москве, попытка захвата г. Нальчика в КБР; взрывы в Московском метрополитене и в аэропорту «Домодедово».

Для парирования угроз национальной безопасности в информационной сфере в Российской Федерации формируется и реализуется на практике **государственная политика в области информационного противоборства**.

Эта политика наиболее тесно взаимодействует с политикой безопасности

- в информационной сфере
- в военной сфере
- в духовной сфере
- в научно-технической сфере

Цель – **в обеспечении национальных интересов России в информационной сфере** и зависит от многих условий и факторов.

Военно-политические факторы формирования государственной политики в области информационного противоборства следующие:

- осознание возрастающей роли информационного противоборства в решении внешнеполитических задач
- изменение характера современной войны
- интеграция военной политики США и их союзников с политикой информационной войны
- развязывание гонки вооружений в области информационного противоборства
- систематическое и целенаправленное блокирование руководством США международно-правовых ограничений на создание и использование информационного оружия

Проблемные направления реализации государственной политики в области информационного противоборства, вытекающие из национальных интересов государства, следующие

- **обеспечение духовного обновления России**
- **информационное обеспечение государственной политики РФ**
- **сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма; культурного и научного потенциала страны**

Их реализация состоит в следующем:

в необходимости определения политической идеи по обеспечению духовного обновления России

в сохранении и укреплении нравственных ценностей общества, традиций патриотизма и гуманизма

в модернизации информационного обеспечения государственной политики, путем укрепления координации, улучшения взаимодействия всех ведомств, государственного планирования этой работы, проведения на системной основе информационных операций и корректировки направлений деятельности федеральных органов государственной власти и организаций, включенных в государственную схему информационного противоборства

в создании постоянно действующего координирующего органа, обладающего полномочиями по оперативному руководству министерствами и ведомствами при решении ими задач информационного противоборства

Важным направлением деятельности государства является определение приоритетов развития информационной технологической и элементной базы, обеспечивающих выход из технологической зависимости России от иностранных государств в области информатики.

Попытки внедрения отечественных технологических новшеств и прорывных результатов в сфере информатики вызывает активное противодействие со стороны ведущих мировых государств, прежде всего США, которые любыми способами стремятся сохранить свое монопольное господство в области создания и распространения средств вычислительной техники, программного обеспечения и связи. Это осложняет решение проблемы преодоления технологического отставания России в области информатики.

Первоочередными шагами РФ в создании эффективной отечественной системы информационной безопасности должны быть:

- ✔**совершенствование действующей нормативно-правовой базы проведения комплексных мероприятий информационного противоборства во всех составляющих информационного пространства, как на территории России, так и за рубежом;**
- ✔**государственное планирование в области информационного противоборства России в мирное время должно осуществляться постоянно действующим координационным органом при Президенте РФ;**
- ✔**разработка и реализация политического механизма обеспечения государством безопасности системы формирования общественного мнения в РФ и противодействия деструктивному внешнему и внутреннему влиянию на социальную среду, духовную сферу, мировоззрение и психику российских граждан**

Примером создания такого эффективного механизма можно привести проведенную администрацией США в сентябре 2001 г. информационно-пропагандистскую кампанию как внутри страны, так и за рубежом.

В результате её проведения большинство стран мира, в том числе и Россия, включились и активно участвуют, при постоянном контроле со стороны администрации США, в борьбе с международным терроризмом.

Можно констатировать, что после трагедии 09.11.01. на территории США не было зафиксировано ни одного случая проведения теракта. В Америке, и в европейских странах создан на системной основе, при государственной поддержки, постоянно действующий комплекс профилактических мероприятий по своевременному выявлению и предупреждению терактов, в котором активно участвует как общество (в лице различных общественных организаций), так и граждане этих государств.

России же в ближайшую «пятилетку» предстоит создать подобную эффективную систему противодействия терроризму, участником которого должны стать не на словах, а на деле и общество, и отдельные граждане.