ГЛАВА 3
ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЕ ПРОТИВОБОРСТВА И ИНФОРМАЦИОННЫЕ ВОЙНЫ

3.1. Информационно-психологическое воздействие

Информационное воздействие - это организованное целенаправленное применение специальных информационных средств и технологий для внесения деструктивных изменений в сознание личности, социальных групп или населения (коррекция поведения), в информационно-техническую инфраструктуру объекта воздействия и (или) физическое состояние человека. Информационное воздействие стоит делить на информационно-техническое и информационно-психологическое.

Информационно-техническое воздействие (ИТВ) - это влияние на информационно-техническую инфраструктуру объекта с целью обеспечения реализации необходимых изменений в ее функционировании (остановка работы, несанкционированный доступ к информации и ее искажение (искажение), программирование на определенные ошибки, снижение скорости обработки информации), а также влияние на физическое состояние человека. ИТВ представляет угрозу безопасности информационно-технической инфраструктуры и физическому состоянию человека.

Безопасность информационно-технической инфраструктуры это состояние защищенности, который обеспечивает ее эффективное использование и защиту от возможного ИТВ.

Безопасность информационно-технической инфраструктуры делится на безопасность:

- машинно-технических средств (автоматизированных систем и сетей);
- программного обеспечения;
- режима защиты от несанкционированной утечки информации.

Информационно-психологическое воздействие (ИПсВ) - это воздействие на сознание и подсознание личности и населения с целью внесения изменений в их поведение и мировоззрение. Базовыми методами ИПсВ является убеждение и внушение. Убеждение направлено к собственному критическому восприятию действительности объектом воздействия. Оно имеет определенные алгоритмы воздействия:

– логика убеждения должна быть доступной для интеллекта объекта воздействия;

– убеждение следует осуществлять, опираясь на факты, известные о объекта;

– убедительная информация должна содержать обобщающие предложения;

– убеждение должна содержать логически непротиворечивые конструкты;

– факты, доносятся до объекта воздействия, должны иметь соответствующую эмоциональную окраску. Внушение, напротив, направлено на субъекты, которые некритически воспринимают информацию. Его особенностями являются:

– целеустремленность и плановость применения;

– конкретность определения объекта внушения (селективное влияние на определенные группы населения с учетом их основных социально-психологических, национальных других особенностей);

– некритическое восприятие информации объектом внушения (внушение основано на эффекте восприятия информации как инструкции к действию без ее логического анализа);

– определенность, конкретность поведения, инициируется (объекта необходимо дать инструкцию относительно его конкретных реакций и поступков, которые соответствуют цели воздействия).

Внушение или суггестия - это процесс воздействия на психику человека, связанный со снижением сознательности и критичности при восприятии навеянного содержания, не требующий ни развернутого личного анализа, ни оценки побуждения к определенным действиям. Суть внушения состоит в воздействии на чувства человека, а через них - на ее волю и разум.

Внушение является основным способом манипулирования сознанием, прямым вторжением в психическую жизнь людей. При этом манипулятивное воздействие организуется так, чтобы мнение, представление, образ непосредственно входили в сферу сознания и закреплялись в ней как данные бесспорные и уже доказанные. Это становится возможным при подмене активного отношения психики к предмету коммуникации преднамеренно созданной пассивностью восприятия.

ИПсВ направляется на индивидуальное или общественное сознание информационно-психологическими или другими средствами, что приводит к трансформации психики, изменению взглядов, мнений, отношений, ценностных ориентаций, мотивов, стереотипов лица с целью повлиять на его деятельность и поведение. Конечной его целью выступает достижения определенной реакции, поведения (действия или бездействия) личности, соответствующей целям ИПсВ.

Процесс восприятия индивидом ИПсВ, направленного на эмоциональную сферу сознания, специфический. В общем, он больше свернут, чем, например, процесс восприятия пропагандистского воздействия: в нем функционируют только восприятия и запоминания, деятельность мышления выражена достаточно слабо. Информацию личность воспринимает или не воспринимает, воспринимает полностью или частично, но в формировании определенных выводов практически не участвует. Процесс ИПсВ на эмоциональную сферу сознания включая произвольное восприятие и запоминание и характеризуется очень пониженным уровнем осознания смысла воздействия. Осмысление полученной информации происходит позже, при более высокой познавательной активности индивида.

Мощность и эффективность манипулятивного воздействия зависит от наличия определенных преимуществ у манипулятора над адресатом. Ранее уже отмечалось скрытый от адресата характер манипулятивного воздействия, сразу создает преимущества манипулятору. Есть и другие преимущества, которые позволяют манипулятору использовать специфические приемы воздействия и усиливает его эффект.

Уровень эффективности ИПсВ зависит от таких условий:

– содержания материала: его сложности, конкретности, общественной важности и тому подобное. Например, при равных условиях чем проще информация, тем больше шансов, что действия, на которые она побуждает, могут выполняться автоматически, особенно когда не противоречат убеждениям объекта. То есть, чем более конкретный призыв к действию, тем выше степень автоматизма ответной реакции;

– психического состояния, характеризующегося наличием высокого уровня автоматизма соответствующей реакции. Страх, подавленность, апатия способствуют некритическому и подсознательном восприятию воздействия. Степень автоматизма в ответе лица связан с уровнем осознанности и критичности восприятия информации. Если влияние воспринимается подсознательно и некритично, то ответ аудитории может быть автоматическим;

– временного интервала между воздействиями и соответствующей реакции: с увеличением временного интервала автоматизм реакции уменьшается вследствие повышения критичности и умственной активности объекта (объясняется включением содержания полученной информации в систему знаний лица и осознанием его).

Источники угроз информационно-психологической безопасности человека в межличностной коммуникации при осуществлении на нее манипулятивного воздействия целесообразно структурировать на три основные группы.

Первая группа включает угрозы, связанные с возможностями манипулятора влиять на сам процесс межличностной коммуникации. То есть, согласно к своей цели менять его ход, организацию, процедуру, информационное содержание, используя для этого определенные приемы.

Вторая группа объединяет угрозы, связанные с возможностями использования манипулятором внешних для адресата факторов, и делится на следующие подгруппы:

– условия внешней социальной среды (например, возможность использования других лиц для оказания влияния; социальных связей, сложившихся с адресатом и его окружением и т.д.);

– личный потенциал манипулятора (скажем, такие его статусные преимущества, как ролевая позиция, должность, возраст, материальное положение, квалификация, образование, способности, знания, коммуникативные навыки, умения и т.д.);

– условия внешней физической среды (выбор места и времени проведения межличностной коммуникации, создания соответствующей обстановки и т.п.).

Третья группа включает угрозы, связанные с возможностями использования манипулятором внутренних, психологических, индивидуально-личностных качеств адресата (в частности его состояния).

Применяя соответствующие приемы воздействия на различные психические структуры личности адресата, манипулятор достигает своей цели. В отличие от межличностного, манипулирование на политическом уровне обезличенное и предполагает воздействие на широкие массы. Воля меньшинства (а то и отдельной личности) в завуалированной форме навязывается большинству. Манипулирование сознанием является системой ИПсВ с целью внедрения в сознание определенного мировоззрения, ценностных установок, представлений о морали, нравственности, нормативность тех или иных форм поведения.

Для манипулирования используются такие методы, как искажение, сокрытие и способ представления информации. Искажение информации варьирует от откровенной лжи до частичных деформаций (подтасовка фактов или смещение в семантическом поле понятия).

Сокрытие информации скорее проявляется как замалчивание/сокрытие определенных тем. Гораздо чаще используется метод частичного освещения или дифференцированного представления материала. Способ подачи информации нередко играет решающую роль в том, чтобы содержание, которое передается, было воспринято так, как необходимо его отправителю.

Например, большое количество информации в "сыром" или несистематизированном виде позволяет заполнить эфир потоками незначительных сведений, что еще больше усложняет и без того безнадежные поиски индивидом их сути. Так же информация, представленная небольшими порциями, не дает возможности эффективно воспользоваться ею. В обоих случаях заранее снимается вопрос нарекания в сокрытии тех или иных сведений.

Сокрытие манипулятивного воздействия.

В литературе не раскрыто рефлексного различия между сокрытием факта манипулятивного воздействия, с одной стороны, и намерений манипулятора - с другой. Однако следует понимать, что наиболее тщательно скрываются именно намерения.

Средства принуждения.

Здесь речь идет о силе властных политических структур или средств массовой информации, а также о степени принуждения к силовому давлению, его неотвратимость, способы скрытого или явного принуждения, предпосылки силового давления. В отношении межличностного влияния в рамках официальных социальных структур обсуждается проявление сильной или слабой позиции. Так, "истинная" позиция строгого начальника, практикует тотальный контроль или часто обращается к явному использованию своей силы (преимущество по должности), расценивается как

слабая. То же касается и подчиненных: открытая конфронтация подчиненного по отношению к своему начальнику скорее означает слабость первого. И наоборот, косвенное запугивание или неявное (неформальное) насилие со стороны подчиненного является признаком слабости позиции начальника; это означает, что последний сделал какую-то ошибку.

Логика манипуляторов очевидна и закономерна однозначно: чем шире аудитория, на которую необходимо оказать влияние, тем более универсальными должны быть цели. Специализированность и точная направленность массового воздействия возможны тогда, когда его организатору известны специфические качества нужных слоев населения или групп людей. Соответственно, чем уже предполагаемая аудитория, тем точнее должна быть подстройка под ее особенности. В случаях, когда такая подстройка по каким-либо причинам не проводится, снова появляются универсальные возбудители: гордость, стремление к удовлетворению, комфорта, желание иметь семейный уют, продвижение по службе, известность - вполне доступные большинства людей ценности. Если же при этом что-то не срабатывает, то это можно рассматривать как неизбежную плату за исходную экономию.

Более "продвинутые" технологии манипулирования предусматривают предварительную подготовку мнений или желаний, закрепление их в массовом сознании или представлениях конкретного человека для того, чтобы можно было к ним потом апеллировать (например, создание мифа о заботливом президенте или респектабельность компании, убеждение партнера в том, что ему хотят помочь или ему угрожает небезопасность).

Роботизация.

Особо следует выделить лейтмотив роботоподобности, который заключается в том, что люди - объекты манипулятивной обработки – превращаются в марионеток, управляемых властными силами с помощью "ниточек" - средств массовой информации. На социально-ролевом уровне обсуждается зависимость подчиненных от давления организации,

преобразования служащих на "прислужников". На межличностном уровне внимание обращается на наличие запрограммированных действий в ответ на те или иные воздействия со стороны партнеров в общении.

Кроме использования готовых к "употреблению" программ стереотипного поведения, усилия манипуляторов направленные на унификацию способов мышления, оценки и реагирования больших масс людей, что приводит к деиндивидуализации и деперсонификации лиц, превращение их в податливых объектов манипулирования.

Виды изменений в индивидуальном сознании, которые может повлечь ИПсВ:

1. изменения психики, психического здоровья человека. Поскольку в случае информационного воздействия сложно определить границы нормы и патологии, показателем изменений может быть потеря адекватности по отражению мира в сознании и индивидуальном отношении к миру. Можно говорить о деградации личности, если формы отражения действительности упрощаются, реакции грубеют и осуществляется переход от высших потребностей (в самоактуализации, социальном признании) до низших (физиологических, бытовых)

2. изменения в ценностях, жизненных позициях, ориентирах, мировоззрении личности. Такие изменения вызывают антисоциальные поступки и представляют опасность для всего общества, государства.

ИПсВ создают угрозу информационной безопасности личности, общества и государства. Информационная безопасность личности и общества является составной информационной безопасности государства: ее обеспечение занимает особое место в государственной политике. Эта особенность определяется спецификой угроз и их источников, особым характером принципов и задач государственной политики в этой сфере. Объектом информационно-психологической защиты (ИПсЗ) лица является состояние его духовного и физического комфорта. Объект защиты составляют и условия, факторы, которые обеспечивают развитие всех сфер

жизнедеятельности человека и общества, в частности культуры, науки, искусства, религиозных и межнациональных отношений.

К объектам относятся также языковую среду, социальные, идеологические, политические ориентиры, общественные и социальные связи, психофизические факторы, проявляющиеся в виде физических, химических и других воздействий природного, антропогенного и техногенного происхождения; генофонд народов, входящих в состав населения государства и тому подобное.

Наиболее важными объектами ИПсЗ в современных условиях является индивидуальное и массовое сознание. Для личности главными системообразующими качествами выступают целостность (тенденция к устойчивости) и развитие (тенденция к изменению). При разрушении или искажении этих качеств личность перестает существовать как социальный субъект. Это означает, что любое ИПсВ на лицо должно оцениваться с позиции сохранения или разрушения ее целостности. Для эффективной ИПсЗ необходимо знать признаки, которые позволяют выявить манипулятивность информационного воздействия через СМИ.

Эти признаки можно разделить на организационные (присуща системность и организованность) и содержательные.

К организационным относятся:

1.Массовое привлечение специалистов со знанием языка государства - субъекта действия (журналистов, писателей, редакторов, теле-, радиоведущих и т.д.) иностранными субъектами.

2.Сосредоточенность компании (организации, государства, других субъектов) на информационном обеспечении собственной деятельности, а не на решении проблем (снимают сюжет о безопасности производства и замечательных условиях труда вместо того, чтобы выделить средства на утилизацию нечистот и очистные сооружения).

3.Наличие в структуре организации информационно-аналитических служб (пресс-центр, информационная служба, собственные издания, интернет-страница).

4.Наём специалистов из сферы пиара, редакторов информационных служб, известных телеведущих (talking heads) и др.

5.Трансляция и ретрансляция теле- и радиопрограмм (прежде всего информационных) иностранного производства.

6.Привлечение журналистов издания или телеканала к участию в тренингах, которые проводят иностранные общественные организации (в процессе подготовки к выборам популярны тренинги по анализу источников информации; обработка результатов социологических исследований; сбор информации о конкретных политиках; психологических аспектов формирования общественного мнения; специфики освещения экономической, социальной и политической тематики; технологий журналистских расследований и т.п.).

7.Получение финансовой помощи (в обмен на заказную направленность материалов).

8.Формирование собственного "agenda" - Перечень информационных сообщений будут освещены в СМИ, основных новостей, порядка их представления. Наглядной формой реализации этого организационного мероприятия является подготовка и распространение так называемых "темников" (государственных рекомендаций СМИ, которые содержат подробные инструкции относительно того, каким образом необходимо освещать в новостях политические события, чтобы власть была представлена в благоприятном свете).

9.Информационная изоляция или введение цензуры на информацию, которая попадает к субъекту.

10.Удержание до поры до времени (межгосударственные официальные переговоры, зарубежные визиты, выборы), нераспространение компрометирующей информации, которая стала известна СМИ.

11.Время выхода материалов – публикация материалов в то время, когда у ответчика нет возможности для ответа или когда этот ответ не будет услышан.

12.Информация с манипулятивными признаками синхронно появляется сразу в нескольких источниках (организовать это может только единый координационный центр). Известны случаи, когда материал с ссылкой на первоисточник выходил раньше, чем его обнародовал первоисточник.

13.Акцентирование внимания источником на событиях, которые являются заведомо конфликтными в государстве. Этот признак фиксируется путем сравнения количества повторов конфликтных тем в разных источниках информации (осуществляется по заранее определенным перечням конфликтных тем). Организация пресс-конференций с целью формирования собственного перечня информационных сообщений, освещаемых в СМИ.

14.Информация появляется в заранее определенных рубриках с негативным контекстом: "неудачник года", "разочарование года", "ссора года" ...

15.Обнародование информации через интернет, который содержит "специализированные" общедоступные сайты для "слива" компромата (например, reporter.com.ua, compromat.ru, informacia.ru, Regnum.ru, vlasti.net и т.д.).

16.Источником информации выступает лицо (организация), деятельность которой связана с иностранными спецслужбами.

17.Осветителем информации являются так называемые "шоумены от политики": скандально известные личности (Н. Шуфрич, В.Жириновский).

К содержательным признакам осуществления манипулятивного информационного воздействия относятся:

18.Растерянность, неопределенность, многовариантность и ужасно общий контекст информации. Любое лицо психологически стремится к стабильности, определенности, конкретных целей и безопасности. Путевой

камень с тремя вариантами выбора дороги ставил в тупик даже эпических богатырей.

19.Количество повторов ключевых слов, которые определяют суть сообщения и могут привязывать к тексту негативные штампы: фашизм, нацизм, коррупция, предательство, боль, террор и т. д.

20.Присутствие сенсации искусственного происхождения (взрывы, катастрофы, преступления и т.п., а не стихийные бедствия или явления природы).

21.Анонимность, использование псевдонимов авторами информации: " по сообщению нашего информированного источника "; "В кулуарах власти ходят слухи", "источник, пожелавший остаться неизвестным" ...

22.Ссылки на другой СМИ, а не на первоисточник информации: Как сообщает информагентство "Риа-нововсти": "…Сейчас все то же самое, только берут больше. Только ставка за риск увеличилась …", - сказал Президент о коррупции.

23.Использование мнения авторитетов: "как доказано учеными", "не соответствует мировым стандартам", "эксперты ФБР", "В то время как еще Аристотель (Маркс, Пушкин) отмечал" и другие. Ссылка на авторитеты используется, когда надо без рационального доказательства подтвердить свою позицию.

24.Использование готовых утверждений без аргументации (доказательства): "Россия лишена выходов в мировое информационное пространство", "у нас всегда так ...", "Россия отстает от развитых стран в развитии информационных технологий на несколько десятилетий",

25.Использование общеупотребительных штампов: "демократические страны", "мировой терроризм", "права человека", "клановo-олигархическая система", "антисемит", "бюрократ" и другие.

26.Оперирование так называемыми "идеальными понятиями": свобода, демократия, справедливость, порядочность, честность, истина, любовь, Родина, Бог, вера, святость, счастье. Джордж Буш в своей ежегодной речи в

Конгрессе в 2004 году 52 раза употребил слово "свобода" в разных сочетаниях, демаскируя истинный смысл послания, авторское прочтение которого ассоциируется с понятиями "преимущество" (primacy), "война", "агрессия", "новый мировой порядок ".

27.Несоответствие общего контекста информационного сообщения задекларированному названию.

28.Наличие неоднозначного факта, эффект которого пытаются смягчить, на общем положительном фоне (набожный, рассудительный, мудрый священник, имеющий уважение прихожан, помогает им, возрождает и оберегает помещения церкви от корыстолюбивых олигархов и ... благословляет однополые браки). Или же наоборот: представление положительного факта, лица на общем негативном фоне.

29.Освещение материала в виде диалога. Читатель (зритель, слушатель) выступает пассивным потребителем готовых идей, в то время как в процессе обсуждения потребитель информации подводится к нужному выводу.

30. Количество прилагательных по объему текста. Прилагательные придают тексту эмоциональной окрашенности, тогда как новости должны точно отражать факты, а не давать им эмоциональную оценку. Любое выступление, документ, решение можно охарактеризовать таким образом, что их текст будет иметь характер темного, страшного, агрессивного, а эти характеристики вызывают негативные эмоции. Вам нужно отрицательное отношение к нововведениям? -Напечатайте их черными буквами на красном фоне.

31.Использование метафор (поэтически, образно выражена мысль), гипербол (преувеличений), сравнений. Это, опять же, свидетельствует о субъективизме, эмоциональности (а не объективности) оценок.

32.Использование глаголов для обозначения умственной действия и его временных границ ("сосредоточиться", "представлять", "начинать", "заканчивать", "продолжать", "кажется" и т.д.).

33.Постановка вопросов, которые постепенно подводят читателя (зрителя, слушателя) к требуемой мысли: "Сколько средств бюджета США необходимо выделить на иракскую кампанию?" Вместо "Является ли иракская кампания легитимной? Поддерживают граждане эту кампанию?».

34.Использование псевдонаучных терминов (вроде "корреляция детерминированных дефиниций") приводит к потере внимания или даже отпугивания львиной доли аудитории.

35.Использование неологизмов (вновь слов).

36.Использование синонимов с нужным контекстом. Вместо "война" - "принуждение к миру", "миротворческая операция", "умиротворение"; вместо "блокада" - "эмбарго"; вместо "акции неповиновения", "бунт" - "проявления протестов" и другие. И наоборот.

37.Несоответствие содержания (текст, звук) и видеоряда: сообщения о деятельности радикальной политической группировке показывают на фоне картинки о столкновении в Северной Ирландии или террористической атаки 11сентября 2001г. Терроризм - это всегда плохо, значит, событие, о котором идет речь, - отрицательное.

38.Использование технического приема съемки снизу, известного как перспектива "Жабы", или показ объекта сверху (перспектива "птичьего полета"). Этот ракурс вызывает антипатию к объекту, создает впечатление слабости, позорности.

Положительная установка создается с помощью фронтальной съемки на уровне глаз, так как психологами доказано, что это вызывает симпатию к объекту, впечатление покоя, непринужденности.

39.Прямые указания в СМИ на желаемое для внешнего субъекта поведение.

40. Использование только части фактов из общего объема в нужном контексте.

Необходимо понимать, наличие только одного из признаков еще не предусматривает высокую вероятность того, что мы имеем дело с

манипулятивным информационным влиянием как составной спецоперации. Оценке подлежит соответствие информации сразу ряда признаков. Объективность и беспристрастность оценок на основе перечисленных критериев может обеспечить или коллектив специалистов-аналитиков, или применения математической теории вероятности.

Для оценки содержания текстовых сообщений широко используется контент-анализ (от англ. Content- содержание) - формализованный метод изучения текстовой и графической информации, который заключается в переводе изучаемой, в количественные показатели и ее статистической обработки [34].

3.2. Специальные информационные операции и акции информационного воздействия

Специальные информационные операции (далее - СИО) - это спланированные действия, направленные на врага, дружескую или нейтральную аудиторию путем воздействия на его сознание и поведение посредством использования определенным образом организованной информации и информационных технологий для достижения определенной цели.

Они помещают в себя психологические действия со стратегическими целями, психологические консолидирующие действия и психологические действия с непосредственной поддержки боевых действий. Они подразделяются на следующие виды:

– Операции, направленные против субъектов, принимающих решения.

– Операции, направленные на компрометацию, причинение вреда оппонентам.

– Операции, направленные на политическую (экономическую) дестабилизацию.

Следует иметь в виду, что СИО происходит на макро- и микроуровне. То есть, СИО макроуровня - это любая агитационно-пропагандистская и разведывательно-организационная деятельность, которая ориентирована на конкретные социальные группы людей и осуществляемая в основном через средства массовой информации и по каналам коммуникаций. СИО микроуровня, со своей стороны, олицетворяет любую агитационно-пропагандистскую и разведывательно-организационную деятельность идеологического характера, прицельно персонализированную и осуществляемую преимущественно через межличностное общение. Для этого часто используется деятельность, направленная на распространение слухов или возбуждения другими методами запланированного негативного поведения населения государства-объекта информационной войны.

Если же мы затрагиваем понятия СИО в контексте мероприятий политической разведки, то следует отметить, что с ее помощью должны решаться определенные политические проблемы, достигаться стратегические цели общества определенного государства или иного субъекта разведывательной деятельности. Для объекта, на который направлено СИО, должны наступить или образоваться угрозы или опасности возникновения негативных последствий. Итак, такое влияние на объект по своей сути является также отрицательным. Влияние, как таковой, применяется как к отдельной личности или группы лиц, так и на все общество в целом или определенный его социальный слой. Отсюда, в контексте информационной войны, СИО должно быть деятельностью, которая проводится, как правило, специальными органами иностранных государств или транснациональных структур (в последние годы даже частных лиц с мировым уровнем авторитета, капитала, потребностей и интересов), которые уполномочены субъектом информационной войны осуществлять подобную деятельность. То есть - это специальные службы, прежде всего разведывательные, которые применяются для достижения общей политической цели путем реализации оперативных задач.

Итак, СИО _- это проведение спецслужбами, прежде всего, иностранных государств тайных операций и акций негативного или даже деструктивного идеологического, идейно-политического и социального воздействия на личность, группу лиц или общество в целом с целью их переориентации на другие ценности и идеалы, подтолкнуть к совершению противоправных действий в направлении подрыва и ослабления государственного и общественно-политического строя для решения задач осуществления выгодного влияния.

Следует отметить, что СИО проводится путем распространения информации определенного рода (правдивой или ложной) различными способами. Это использование коммуникативных технологий по влиянию на массовое сознание с долговременными или кратковременными целями. Надо подчеркнуть, что СИО создает угрозу не столько своим существованием как явление вообще, а тем, что она "включает" и запускает в действие вещественно-энергетические процессы, а также контролирует их. Суть как раз и состоит в том, что она может возбуждать и направлять такие процессы, масштабы которых во много раз больше самой операции.

Именно этот вид информационной борьбы, как правило, направлен на переориентацию отдельных лиц, их групп или общества в целом на другие ценности и идеалы для ослабления политического и социально-политического устройства. В случае, когда меры непосредственного информационного подрыва является инструментом политической разведки, их цель также носит политический характер. Итак, СИО предполагает указано причинение вреда жизненно важным интересам в политической, экономической, научно-технической, социальной или любой другой общественной сферах жизни государства-противника и на этой основе осуществления выгодного влияния для получения преимуществ в той или иной области.

Рассмотрим теперь в каких конкретных формах осуществляется деструктивное влияние в процессе информационного противоборства и приемы и методы при этом используются.

Можно выделить следующие основные методы специальных информационных операций соответствующими структурами для осуществления скрытого выгодного влияния на иностранные государства с целью создания благоприятной политической, идеологической, социальной, экономической обстановки при реализации собственной правящей элитой внешнеполитического курса:

- дезинформации;
- пропаганда;
- диверсификация общественного сознания;
- психологическое давление;
- распространения слухов.

Рассмотрим более подробно каждую из форм, ее сущность, основные черты и виды.

Дезинформации - форма СИО, которая специализируется на обмане или введении объекта направлений в заблуждение относительно подлинности намерений для побуждения его к запрограммированных субъектом СИО действий.

Исторический опыт свидетельствует, что существуют различные методы проведения мероприятий по дезинформации, каждый из которых обычно имеет собственные положительные и отрицательные черты. Конкретный выбор того или иного метода напрямую зависит от оперативной обстановки, которая складывается на конкретном участке деятельности спецслужбы, стоящих перед ней поставлены и тому подобное. Чаще всего в мировой практике применяются следующие методы:

1. тенденциозное изложение фактов - вид дезинформации, который заключается в предвзятом освещении тех или иных фактов или другой информации о событиях с помощью специально подобранных правдивых

данных в определенные промежутки времени. Как правило, с помощью этого метода объекта направлений приходится дозировано, к постоянно растущему напряжения, и поддерживается в таком состоянии специально сформированная информация и поддерживается такой напряженное состояние объекта путем постоянного "подбрасывания" новых порций строго ограниченных и дозированных данных в среду информационного дефицита;

2. дезинформации от "обратной" - происходит путем предоставления правдивых сведений в искаженном виде или в такой ситуации, когда они воспринимаются объектом устремлений как лживые. В результате применения подобных мер возникает ситуация, когда объект фактически знает правдивую информацию о намерениях или конкретные действия противоположной стороны, но воспринимает ее адекватно, не готов противостоять негативному влиянию;

3. терминологическое "минировании" - заключается в искажении первичной правильной сути принципиально важных, базовых терминов и толкований общих мировоззренческого и оперативно-прикладного характера.

В обобщенном виде акции дезинформации могут проводиться путем создания видимости успехов разведки иностранных партнеров, использование средств массовой информации, включая собственные информационные агентства, теле-, радиокомпании, печатные издания и отдельных "карманных" журналистов, или же создание видимости случайной утечки закрытой информации.

Пропаганда - распространение различных политических, философских, научных, художественных, других художественных идей с целью их внедрения в массовое сознание общества и активизации, тем самым, использование этих идей в массовом практической деятельности населения. Одновременно, к пропаганде относятся сообщения, которые распространяются для осуществления выгодного влияния на общественное мнение, провоцирование запрограммированных эмоций и изменения

отношения или поведение определенной группы людей в направлении, прямо или косвенно выгодном организаторам.

По своей сути пропаганда делится на "белую", "серую" и "черную". Так, "белая" пропаганда представляет откровенно лояльную по объекту направлений позицию, которая проводится через любые СМИ по официальным каналам без утайки ее направленности и источники. "Серая" - нелояльная до адресата пропаганды, проводится через СМИ по официальным каналам, но с сокрытием ее источники и достоверной направленности. "Черная" - проводится по официальным каналам через оперативные возможности спецслужб от имени несуществующих или специально созданных под соответствующими легендами подпольных оппозиционных организаций.

Методы проведения пропаганды:

– пропаганда образа жизни (социологическая) - натуральный показ достижений, преимуществ, перспектив и т. д. конкретного государства;

– использование средств массовой информации и печатных научных и художественных изданий;

– Резонансная" - корректировка уже существующих мнений, а не формулировки и создание новых.

Психологическое давление - воздействие на психику человека путем запугивания, угроз с целью побуждения его к определенной запланированной модели поведения.

Методы психологического давления:

– доведение до объекта сведений о реальных или мнимые угрозы и опасности;

– прогнозы о репрессиях, преследований, убийств и т.д.;

– шантаж;

– осуществления взрывов, поджогов, массовых отравлений, захват заложников, других террористических или диверсионных акций.

Диверсификация общественного сознания - распыление внимания правящей элиты государства для решения различных искусственно акцентированных проблем и отвлечения тем самым ее внимания от решения насущных первоочередных задач общественно-политического и экономического развития, которые необходимы для нормального функционирования общества и государства.

Методы диверсификации общественного сознания:

– дестабилизация обстановки в государстве или отдельных ее регионах;

– активизация кампании против политического курса правящей элиты государства и отдельных ее лидеров в различных международных учреждениях;

– инициирование антидемпинговых кампаний и другого рода скандальных судебных процессов, применения международных санкций по другим причинам.

Распространение слухов - деятельность по распространению различной информации (как правило, ложной) среди широких слоев населения, в основном, по неофициальным каналам с целью дезорганизации общества и государства или же их отдельных учреждений или организаций.

Одно из толкований определяет, что слухи - это циркулирующая форма коммуникации, с помощью которой люди, которые находятся в неоднозначной ситуации, объединяются, образуя понятную им интерпретацию этой ситуации, совместно используя при этом собственные интеллектуальные возможности.

Слухи по своей характеристике является самораспространяемыми. Их природа базируется на такого рода информации, которую трудно удержать. Лицо обязательно должен рассказать об услышанном кому-то другому. Достаточно создать соответствующую слух и запустить ее в обращение в нужном месте в нужное время. "Человеческий шум" сделает остальных. Положительный фактор использования данной формы СИО заключается еще

и в том, что практически не существует эффективных средств противодействия слухам. На официальном уровне остановить их невозможно: официальные меры противодействия вызывают прямо противоположный эффект. Фактически это означает для людей, которых непосредственно интересуют эти слухи, подтверждения их правдивости. Чем больше попыток их опровергнуть, тем больше становится уверенность и обоснованность достоверности слухов. Единственно возможный вариант преодоления эффективности слухов - полное их игнорирование. Как правило, через некоторые время напряжение спадает, излишняя активность в обсуждении уже неактуальных новостей угасает, интерес к затронутой в слухах проблемы исчезает. Появление новых проблем полностью нейтрализует возможные опасные последствия для дезорганизации общества и государства.

Перечисленные выше формы и методы, условия их применения на определенном промежутке времени и территории, задачи, которые должны быть достигнуты при их применении, - обусловливают использование соответствующих сил и средств, способных проводить необходимые специфические меры непосредственного подрыва или предоставления скрытого выгодного влияния. В каждом отдельном случае они могут быть разными. Целесообразно подчеркнуть, что все тайные подготовительные действия и акции такого рода используются в политической разведке для создания необходимых условий проведения государственной политики по той или иной страны, международной структуры или внутренних оппозиционных кругов. А значит, если разведка поднята до такого высокого уровня, то в таком случае могут быть привлечены в качестве прикрытия ("подкрышевые структуры") практически все государственные ресурсы, включая неразведовательные государственные органы и учреждения, неправительственные организации (благотворительные и благотворительные организации, фонды поддержки демократических ценностей , организации

культурологической направленности и т.д.), подконтрольные субъекту разведывательной деятельности.

В разное время к осуществлению операций информационной борьбы привлекались различные силы с разной степенью организации и отношение к государственно-правительственных структур. В частности упоминалось, что специальные подразделения информационной (психологической) борьбы в структуре государственных органов появились только во время первой мировой войны в государствах-участниках последней. Дальнейшее опыт организации информационной борьбы показал, что силы, которые привлекаются к созданию необходимых благоприятных условий реализации политических и военных мер в рамках государственной внешней политики, могут относиться как к специально созданных подразделений специальных учреждений и организаций, так и к таким, которые не имеют в своих основных функциональных обязанностях задач взрывного характера.

Примером первой категории могут служить специальные подразделения войны, например, армии США (группы и отдельные батальоны психологической борьбы). На вооружении указанных подразделений сил специальных операций находятся передвижные теле- и радиоцентры, типографии, оборудование для проведения устных агитационных программ на личный состав и население иностранного государства, соответствующие технические средства: так называемые "агитационные" снаряды, бомбы, воздушные шары и т.д., с помощью которых забрасываются на территорию противника и распыляются спецпропагандические печатные материалы (листовки, газеты, брошюры и т.д.).

Наличие подобных средств позволяет указанным подразделениям за короткий промежуток времени наладить целенаправленную работу по осуществлению выгодного идеологического и психологического воздействия на противника на определенных театрах военных действий в ходе проведения различных специальных или непосредственно военных операций

вооруженными силами США. Наглядными примерами оперативной деятельности подразделений специального назначения США могут служить события в годы "холодной войны" вокруг СССР (1945-1991 гг.), ГДР (1953-1954 гг.) Венгрии (в 1956 г..), Чехословакии (1968г.), Польши (1968, 1980-1982 гг.), Румынии (1985-1990 гг.) которые разворачивались по сценарию руководства Соединенных Штатов в направлении свержения коммунистических режимов.

Целесообразно отметить, что в последнее время наблюдается постоянно растущая активность неправительственных структур, также задействованные в осуществлении выгодного психологического воздействия с целью создания благоприятных политико-идеологических условий в государстве-объекте воздействия.

К указанных организаций и учреждений относятся разного рода миссионерские религиозные структуры, навязывают чужие для нашего народа культы, верования и вероучения, нередко даже противоправным путем с использованием методик и технологий нейропсихического программирования, гипноза, с применением наркотических и психотропных веществ, которые подавляют волю человека.

Активно действуют также организации и лица, участвующие в гуманитарных программах сотрудничества между государствами: культурные и образовательные центры, ассоциации, фонды и др. Под видом просветительских акций они занимаются идеологической обработкой, агитацией и пропагандой собственного образа жизни как единственно верного, распространяют слухи о невозможности положительных сдвигов в государстве без существенных изменений социально-политического строя и т. Как правило, координацией подобной деятельности указанных организаций и учреждений занимаются культурно-гуманитарные, научно-технические отделы при посольствах и консульствах иностранных государств и других дипломатических представительствах международных организаций.

С целью организации противодействия СИО, необходимо знать факторы, способствующие возникновению рисков, угроз и опасностей в идеологически-информационной области государства, выяснить их сущность, уметь оценивать и определять реальность и уровень негативного воздействия на общество и государство.

К главным факторам, которые влияют на состояние морально-идеологической стабильности и безопасности в государстве, относятся:

– отсутствие целостной системы информационно-аналитического обеспечения органов государственной власти и управления;

– разрушения интеллектуального потенциала, неготовность существующей системы образования к поддержанию процессов опережающего развития государства;

– медлительность процесса осознания прослойкой бывшей советской партийно-хозяйственной номенклатуры, научной и творческой интеллигенции, ростков новой буржуазии своего места в обществе и формирование собственно элиты, что приводит к невозможности сформировать правящими кругами понятной и привлекательной для общества национальной идеи;

– низкий общий уровень развития информационной инфраструктуры, что не исключает возможность экспансии иностранных компаний на рынке информационных услуг; разрушения национального информационного пространства и возникновения возможности его использования в антигосударственных интересах;

– недостаточный профессиональный, интеллектуальный и творческий уровень отечественных производителей информационного продукта и услуг, их неконкурентоспособность на мировом информационном рынке;

– информационная экспансия со стороны ведущих иностранных государств; разработка и использование ими, международными или отечественными преступными организациями различных современных способов непосредственного подрыва, в частности СИО;

– малоконтролируемая деятельность отдельных политических сил, СМИ и лиц, которая направлена на разрушение нравственных ценностей, сознания, подрыв морального и физического здоровья нации; использование средств массовой информации с позиций, противоположных интересам граждан, политических и общественных организаций, государства; манипулирование информацией (дезинформация, искажение фактографических данных, замалчивание истинных сведений и т.п.);

– потеря доверия к власти со стороны значительной части населения вследствие распространения компромата, применение грязных политических технологий, особенно во время избирательных кампаний;

– навязывание путем информационно-психологического воздействия на сознание и подсознание, применением различных информационных ресурсов и социотехнических систем лицам, обществу желательных для иностранцев решений определенных вопросов в жизненно важных сферах общественной и государственной жизни;

– конкурентная борьба за обладание СМИ, процесс их монополизации и концентрация в их пределах информационной и политической власти [35].

3.3. Информационные войны

На концептуальном уровне можно сказать, что государства стремятся приобрести информации, обеспечивающую выполнение их целей, воспользоваться ей и защитить ее. Эти использование и защита могут осуществляться в экономической, политической и военной сферах. Знание об информации, которой владеет противник, является средством, позволяющим усилить нашу мощь и понизить мощь врага или противостоять ей, а также защитить наши ценности, включая нашу информацию.

Информационное оружие воздействует на информацию, которой владеет враг и его информационные функции. При этом наши информационные функции защищаются, что позволяет уменьшить его волю

или возможности вести борьбу. Поэтому дадим определение **информационной войне** (ИВ) - это любое действие по использованию, разрушению, искажению вражеской информации и ее функций; защите нашей информации против подобных действий; и использованию наших собственных военных информационных функций.

Это определение является основой для следующих утверждений.

Информационная война - это комплексное совместное применение сил и средств информационной и вооруженной борьбы.

Информационная война - это коммуникативная технология по воздействию на информацию и информационные системы противника с целью достижения информационного превосходства в интересах национальной стратегии, при одновременной защите собственной информации и своих информационных систем.

Информационная война - только средство, а не конечная цель, аналогично тому как бомбардировка - средство, а не цель. Информационную войну можно использовать как средство для проведения стратегической атаки или противодействия.

Первым использовал термин "информационная война" американский эксперт Томас Рона в отчете, подготовленным им в 1976 году для компании Boeing, и названный "Системы оружия и информационная война". Т. Рона указал, что информационная инфраструктура становится ключевым компонентом американской экономики. В то же самое время, она становится и уязвимой целью, как в военное, так и в мирное время. Этот отчет и можно считать первым упоминанием термина «информационная война».

Публикация отчета Т. Рона послужила началом активной кампании в средствах массовой информации. Сама постановка проблемы весьма заинтересовала американских военных, которым свойственно заниматься «секретными материалами». Военно-воздушные силы США начали активно обсуждать этот предмет уже с 1980 года.

С военной точки зрения термин «информационная война» в наше время был употреблен в середине 80-х годов XX в. в связи с новыми задачами Вооруженных сил США после окончания «холодной» войны. Это явилось результатом работы группы американских военных теоретиков в составе Г.Е. Экклз, Г.Г. Саммерз и др. В дальнейшем термин начал активно употребляться после проведения операции «Буря в пустыне» в 1991 г. в Ираке, где новые информационные технологии впервые были использованы как средство ведения боевых действий. Официально же этот термин впервые введен в директиве министра обороны США DODD 3600 от 21 декабря 1992 года.

Спустя несколько лет, в феврале 1996 года, Министерство обороны США ввело в действие «Доктрину борьбы с системами контроля и управления». Публикация определяет борьбу с системами контроля и управления как «объединенное использование приемов и методов безопасности, военного обмана, психологических операций, радиоэлектронной борьбы и физического разрушения объектов системы управления, поддержанных разведкой, для недопущения сбора информации, оказания влияния или уничтожения способностей противника по контролю и управлению над полем боя, при одновременной защите своих сил и сил союзников, а также препятствование противнику делать тоже самое».

Наиболее важным является то, что эта публикация определила понятие войны с системами контроля и управления. И это было впервые, когда Министерство обороны США определило возможности и доктрину ИВ.

В конце 1996 г. Роберт Банкер, эксперт Пентагона, на одном из симпозиумов представил доклад, посвященный новой военной доктрине вооруженных сил США XXI столетия (концепции "Force XXI"). В ее основу было положено разделение всего театра военных действий на две составляющих - традиционное пространство и киберпространство, причем последнее имеет даже более важное значение. Р. Банкер предложил доктрину "кибермaневра", которая должна явиться естественным дополнением

традиционных военных концепций, преследующих цель нейтрализации или подавления вооруженных сил противника.

Таким образом, в число сфер ведения боевых действий, помимо земли, моря, воздуха и космоса теперь включается и инфосфера. Как подчеркивают военные эксперты, основными объектами поражения в новых войнах будут информационная инфраструктура и психика противника (появился даже термин "human network").

В октябре 1998 года, Министерство обороны США вводит в действие «Объединенную доктрину информационных операций». Первоначально эта публикация называлась «Объединенная доктрина информационной войны». Позже она была переименована в «Объединенную доктрину информационных операций». Причина изменения состояла в том, чтобы разъяснить отношения понятий информационных операций и информационной войны. Они были определены, следующим образом:

– информационная операция: действия, предпринимаемые с целью затруднить сбор, обработку передачу и хранение информации информационными системами противника при защите собственной информации и информационных систем;

– информационная война: комплексное воздействие (совокупность информационных операций) на систему государственного и военного управления противостоящей стороны, на ее военно-политическое руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны-инициатора информационного воздействия решений, а в ходе конфликта полностью парализовало бы функционирование инфраструктуры управления противника.

Сейчас существует довольно много разных определений ИВ и с технико-технологической точки зрения. В коридорах Пентагона ходит, например, такое шутливое определение «Информационная война - это компьютерная безопасность плюс деньги».

А если серьезно, то военные подходят к ИВ так, как это было сформулировано еще в Меморандуме N30 (1993 г) заместителей Министра Обороны и Комитета начальников штабов Вооруженных Сил США.

Под информационной войной здесь понимаются действия, предпринимаемые для достижения информационного превосходства в поддержке национальной военной стратегии посредством воздействия на информацию и информационные системы противника при одновременном обеспечении безопасности и защиты собственной информации и информационных систем.

В гуманитарном смысле «информационная война» понимается как те или иные активные методы трансформации информационного пространства. В информационных войнах этого типа речь идет об определенной системе (концепции) навязывания модели мира, которая призвана обеспечить желаемые типы поведения, об атаках на структуры порождения информации, процессы рассуждений.

Основными формами ведения технической ИВ являются радиоэлектронная борьба, война с использованием средств электронной разведки и наведения, нанесения удаленных точечных ударов с воздуха, психотропная война, борьба с хакерами, кибернетическая война.

Прежде чем всерьез анализировать различные определения информационной войны с технической точки зрения отметим присущее ей важное свойство: ведение информационной войны никогда не бывает случайным или обособленным, а подразумевает согласованную деятельность по использованию информации как оружия для ведения боевых действий - будь то на реальном поле боя, либо в экономической, политической, социальной сферах.

Поэтому в качестве основного и наиболее общего определения ИВ используется следующее:

Информационная война - это всеобъемлющая целостная стратегия, обусловленная все возрастающей значимостью и ценностью информации в вопросах командования, управления и политики.

Поле действия информационных войн при таком определении оказывается достаточно широким и охватывает следующие области:

1) инфраструктуру систем жизнеобеспечения государства - телекоммуникации, транспортные сети, электростанции, банковские системы и т.д.;

2) промышленный шпионаж - хищение патентованной информации, искажение или уничтожение особо важных данных, услуг; сбор информации разведывательного характера о конкурентах и т.п.;

3) взлом и использование личных паролей VIP-персон, идентификационных номеров, банковских счетов, данных конфиденциального плана, производство дезинформации;

4) электронное вмешательство в процессы командования и управления военными объектами и системами, "штабная война", вывод из строя сетей военных коммуникаций;

5) всемирная компьютерная сеть Интернет, в которой, по некоторым оценкам, действуют 150.000 военных компьютеров, и 95% военных линий связи проходят по открытым телефонным линиям.

Какой бы смысл в понятие "информационная война" ни вкладывался, оно родилось в среде военных и обозначает, прежде всего, жесткую, решительную и опасную деятельность, сопоставимую с реальными боевыми действиями. Военные эксперты, сформулировавшие доктрину информационной войны, отчетливо представляют себе отдельные ее грани: это штабная война, электронная война, психотронная война, информационно-психологическая война, кибернетическая война и т.

Итак, информационная война - это такая форма конфликта, в которой происходят прямые атаки на информационные системы для воздействия на знания или предположения противника.

Информационная война может проводиться как часть большего и более полного набора военных действий.

Таким образом, под угрозой информационной войны понимается намерение определенных сил воспользоваться поразительными возможностями, скрытыми в компьютерах, на необозримом кибер-пространстве, чтобы вести «бесконтактную» войну, в которой количество жертв (в прямом значении слова) сведено до минимума. Гражданская информационная война может быть развязана террористами, наркотическими картелями, подпольными торговцами оружием массового поражения.

Военные всегда пытались воздействовать на информацию, требующуюся врагу для эффективного управления своими силами. Обычно это делалось с помощью маневров и отвлекающих действий. Так как эти стратегии воздействовали на информацию, получаемую врагом, косвенно путем восприятия, они атаковали информацию врага косвенно. То есть, для того чтобы хитрость была эффективной, враг должен был сделать три вещи:

1. наблюдать обманные действия
2. посчитать обман правдой
3. действовать после обмана в соответствии с целями обманывающего.

Тем не менее, современные средства выполнения информационных функций сделали информацию уязвимой к прямому доступу и манипуляции с ней. Современные технологии позволяют противнику изменить или создать информацию без предварительного получения фактов и их интерпретации. Вот краткий список характеристик современных информационных систем, приводящим к появлению подобной уязвимости: концентрированное хранение информации, скорость доступа, повсеместная передача информации, и большие возможности информационных систем выполнять свои функции автономно. Механизмы защиты могут уменьшить, но не до нуля эту уязвимость.

3.3.1. Составные части информационной войны

К составным частям информационной войны относятся:

1) психологические операции - использование информации для воздействия на аргументацию солдат врага.

2) электронная война - не позволяет врагу получить точную информацию

3) дезинформация - предоставляет врагу ложную информацию о наших силах и намерениях

4) физическое разрушение - может быть частью информационной войны, если имеет целью воздействие на элементы информационных систем.

5) меры безопасности - стремятся избежать того, чтобы враг узнал о наших возможностях и намерениях.

6) прямые информационные атаки - прямое искажение информации без видимого изменения сущности, в которой она находится.

Как ранее говорилось, существует два способа повлиять на информационные функции врага - косвенно или напрямую. Проиллюстрируем разницу между ними на примере.

Пусть нашей целью является заставить врага думать, что авиаполк находится там, где он совсем не находится, и действовать на основании этой информации таким образом, чтобы это было выгодно нам.

Косвенная информационная атака: используя инженерные средства, мы можем построить макеты самолетов и ложные аэродромные сооружения, и противник будет наблюдать ложный аэродром и считать его настоящим. Только тогда эта информация станет той, которую должен иметь противник по нашему мнению.

Прямая информационная атака: если мы создаем информацию о ложном авиаполке в хранилище информации у противника, то результат будет точно такой же. Но средства, задействованные для получения этого результата, будут разительно отличаться.

Другим примером прямой информационной атаки может быть изменение информации во вражеской базе данных об имеющихся коммуникациях в ходе боевых действий (внесение ложной информации о том, что мосты разрушены) для изоляции отдельных вражеских частей. Этого же можно добиться бомбардировкой мостов. И в том, и в другом случае вражеские аналитики, принимая решение на основе имеющейся у них информации, примут одно и то же решение - производить переброску войск через другие коммуникации.

Оборонительной стороной информационной войны являются меры безопасности, имеющие своей целью защитить информацию - не позволить противнику провести успешную информационную атаку на наши информационные функции. Современные меры защиты, такие как операционная безопасность и коммуникационная безопасность - типичные средства по предотвращению и обнаружению косвенных действий врага, направленных на наши военные информационные функции. Напротив, такие меры защиты, как компьютерная безопасность включают в себя действия по предотвращению, обнаружению прямых информационных действий врага и организации контрдействий.

3.3.2. Цели информационной войны

Существуют три цели информационной войны:

– контролировать информационное пространство, чтобы мы могли использовать его, защищая при этом наши военные информационные функции от вражеских действий (контринформация).

– использовать контроль за информацией для ведения информационных атак на врага

– повысить общую эффективность вооруженных сил с помощью повсеместного использования военных информационных функций.

Следует отличать информационную войну от компьютерной преступности. Любое компьютерное преступление представляет собой факт нарушения того или иного закона. Оно может быть случайным, а может быть специально спланированным; может быть обособленным, а может быть составной частью обширного плана атаки. Напротив, ведение информационной войны никогда не бывает случайным или обособленным (и может даже не являться нарушением закона), а подразумевает согласованную деятельность по использованию информации как оружия для ведения боевых действий - будь то на реальном поле брани, либо в экономической, политической или социальной сферах. Театр информационных боевых действий простирается от секретного кабинета до домашнего персонального компьютера и ведется на различных фронтах.

Электронное поле боя представлено постоянно растущим арсеналом электронных вооружений, преимущественно засекреченных. Говоря военным языком, они предназначены для боевых действий в области командования и управления войсками, или «штабной войны». Последние конфликты уже продемонстрировали всю мощь и поражающую силу информационных боевых действий - война в Персидском заливе и вторжение на Гаити. Во время войны в Персидском заливе силы союзников на информационном фронте провели комплекс операций в диапазоне от старомодной тактики разбрасывания пропагандистских листовок до вывода из строя сети военных коммуникаций Ирака с помощью компьютерного вируса.

Атаки инфраструктуры наносят удары по жизненно важным элементам, таким как телекоммуникации или транспортные системы. Подобные действия могут быть предприняты геополитическими или экономическими противниками или террористическими группами. Примером служит вывод из строя междугородной телефонной станции компании AT&T в 1990 году. В наши дни любой банк, любая электростанция, любая транспортная сеть и любая телевизионная студия представляют собой потенциальную мишень для воздействия из киберпространства.

Промышленный шпионаж и другие виды разведки грозят великим множеством тайных операций, осуществляемых корпорациями или государствами в отношении других корпораций или государств; например, сбор информации разведывательного характера о конкурентах, хищение патентованной информации и даже акты саботажа в форме искажения или уничтожения данных. Иллюстрацией этой угрозы служит документально доказанная деятельность французских и японских агентов на протяжении восьмидесятых годов.

Сбор разведывательной информации также выходит на новые рубежи. Лаборатория Линкольна в Массачусетском технологическом институте разрабатывает аппарат для воздушной разведки размером с пачку сигарет. Другая лаборатория работает над химическими веществами, которые можно ввести в провизию неприятельских войск, чтобы позволить датчикам отслеживать их перемещение по дыханию или выделению пота. Помимо этого уже имеются спутниковые системы слежения, имеющие разрешающую способность в несколько сантиметров.

Конфиденциальность все более уязвима по мере появления возможности доступа к постоянно растущим объемам информации в постоянно растущем числе абонентских пунктов. Важные персоны, таким образом могут стать объектом шантажа или злобной клеветы, и никто не гарантирован от подложного использования личных идентификационных номеров.

Как бы то ни было, термин "информационная война" обязан своим происхождением военным и обозначает жестокую и опасную деятельность, связанную с реальными, кровопролитными и разрушительными боевыми действиями. Военные эксперты, сформулировавшие доктрину информационной войны, отчетливо представляют себе отдельные ее грани: это штабная война, электронная война, психологические операции и так далее.

Информационная война представляет собой всеобъемлющую, целостную стратегию, призванную отдать должное значимости и ценности информации в вопросах командования, управления и выполнения приказов вооруженными силами и реализации национальной политики. Информационная война нацелена на все возможности и факторы уязвимости, неизбежно возникающие при возрастающей зависимости от информации, а также на использование информации во всевозможных конфликтах. Объектом внимания становятся информационные системы (включая соответствующие линии передач, обрабатывающие центры и человеческие факторы этих систем), а также информационные технологии, используемые в системах вооружений. Информационная война имеет наступательные и оборонительные составляющие.

Многие ведущие стратеги полагают, что противостояние армий, погибающих на полях генеральных сражений, очень скоро займет свое место на свалке истории рядом со шпорами и арбалетами. Высшая форма победы теперь состоит в том, чтобы выигрывать без крови. В то же время довольно трудно представить боевые действия как игру на видеоприставке без страха и боли.

Таким образом, под угрозой информационной войны понимается намерение определенных сил воспользоваться поразительными возможностями, скрытыми в компьютерах, на необозримом киберпространстве, чтобы вести "бесконтактную" войну, в которой количество жертв (в прямом значении слова) сведено до минимума. "Мы приближаемся к такой ступени развития, когда уже никто не является солдатом, но все являются участниками боевых действий, - сказал один из руководителей Пентагона. - Задача теперь состоит не в уничтожении живой силы, но в подрыве целей, взглядов и мировоззрения населения, в разрушении социума".

Гражданская информационная война может быть развязана террористами, наркотическими картелями, подпольными торговцами

оружием массового поражения. Крупномасштабное информационное противостояние между общественными группами или государствами имеет целью изменить расстановку сил в обществе.

Поскольку такая война связана с вопросами информации и коммуникаций, то если смотреть в корень, это есть война за знания - за то, кому известны ответы на вопросы: что, когда, где и почему и насколько надежными считает отдельно взятое общество или армия свои знания о себе и своих противниках.

Исследователи выделили характерную особенность человеческого восприятия, заключающуюся в том, что человек лучше усваивает ту информацию, которая похожа на уже существующие у него представления.

Основные средства ИВ ориентированы на этот феномен. Любые манипуляции и пропагандистские компании основаны на «эффекте резонанса», когда «имплантируемая» информация, направленная на изменение поведения общности, маскируется под знания и стереотипы, уже существующие в конкретной социальной общности на которую направлена пропагандистская компания.

Целью манипуляции является асинхронизации представлений группы-адресата с помощью «эффекта резонанса» и перевод ее на другие модели поведения, ориентированные на совершенно иную систему ценностей.

«Эффект резонанса» достигается, когда тому или иному факту, проблеме или психологической установке придается искусственно преувеличенное значение, которое по мере продвижения в культурное ядро, диссонирует и разрушает существующую в обществе систему ценностей. Диссонанс достигается при раздувании одной из уже существующих моральных норм, которые в определённых рамках сами по себе помогают обществу.

Крупномасштабное информационное противостояние между общественными группами или государствами имеет целью изменить расстановку сил в обществе.

Как указывают американские военные эксперты, ИВ состоит из действий, предпринимаемых с целью достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой собственной информации и информационных систем и инфраструктуры.

Информационное превосходство определяется как способность собирать, обрабатывать и распределять непрерывный поток информации о ситуации, препятствуя противнику делать то же самое. Оно может быть также определено и как способность назначить и поддерживать такой темп проведения операции, который превосходит любой возможный темп противника, позволяя доминировать во все время ее проведения, оставаясь непредсказуемым, и действовать, опережая противника в его ответных акциях.

Информационное превосходство позволяет иметь реальное представление о боевой обстановке и дает интерактивную и высокоточную картину действий противника и своих войск в реальном масштабе времени. Информационное превосходство является инструментом, позволяющим командованию в решающих операциях применять широко рассредоточенные построения разнородных сил, обеспечивать защиту войск и ввод в сражение группировок, состав которых в максимальной степени соответствует задачам, а также осуществлять гибкое и целенаправленное материально-техническое обеспечение.

Информационное противоборство осуществляется путем проведения мероприятий направленных против систем управления и принятия решений (Command & Control Warfare, C2W), а также против компьютерных и информационных сетей и систем (Computer Network Attack, CNA).

Деструктивное воздействие на системы управления и принятия решений достигается путем проведения психологических операций (Psychological Operations, PSYOP), направленных против персонала и лиц,

принимающих решения и оказывающих влияние на их моральную устойчивость, эмоции и мотивы принятия решений; выполнения мероприятий по оперативной и стратегической маскировке (OPSEC), дезинформации и физическому разрушению объектов инфраструктуры.

Вообще, по словам некоторых экспертов, попытки в полной мере осознать все грани понятия информационной войны напоминают усилия слепых, пытающихся понять природу слона: тот, кто ощупывает его ногу, называет его деревом; тот, кто ощупывает хвост, называет его канатом и так далее. Можно ли так получить более верное представление? Возможно, слона-то и нет, а есть только деревья и канаты. Одни готовы подвести под это понятие слишком много, другие трактуют какой-то один аспект информационной войны как понятие в целом [4].

Однако проблема поиска надлежащего определения этому явлению весьма серьезная и требует детальнейшей и серьезной проработки.

3.3.3. Последствия информационной войны.

Взрыв нескольких гранат нельзя назвать войной, кто бы их не бросал. Взрыв нескольких водородных бомб - это уже и начатая и завершенная война.

Информационную пропаганду 50-ых, 60-ых годов, которой занимались СССР и США, можно сравнить именно с несколькими гранатами. Поэтому никто не называет прошлое противостояние информационной войной, в лучшем случае оно заслуживает термина "холодная война".

День сегодняшний, с его телекоммуникационными вычислительными системами, психотехнологиями кардинально изменил окружающее пространство. Отдельные информационные ручейки превратились в сплошной поток. Если ранее было возможно "запрудить" конкретные информационные каналы, то сегодня все окружающее пространство информационно коллапсировалось. Время на информационное взаимодействие между самыми отдаленными точками приблизилось к нулю.

В результате проблема защиты информации, которая ранее была как никогда актуальна, перевернулась подобно монете, что вызвало к жизни ее противоположность - защиту от информации.

Почему надо защищать информационную систему от информации? Потому что любая поступающая на вход системы информация неизбежно изменяет систему. Целенаправленное же, умышленное информационное воздействие может привести систему к необратимым изменениям и к самоуничтожению.

Поэтому информационная война - это не что иное, как явные и скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной сфере.

Исходя из приведенного определения информационной войны, применение информационного оружия означает подачу на вход информационной самообучающейся системы такой последовательности входных данных, которая активизирует в системе определенные алгоритмы, а в случае их отсутствия - алгоритмы генерации алгоритмов.

Создание универсального защитного алгоритма, позволяющего выявить системе-жертве факт начала информационной войны, является алгоритмически неразрешимой проблемой. К таким же неразрешимым проблемам относится выявление факта завершения информационной войны. Однако, несмотря на неразрешимость проблем начала и окончания информационной войны, факт поражения в ней характеризуется рядом признаков, присущих поражению в обычной войне. К ним относятся:

1) включение части структуры пораженной системы в структуру системы победителя (эмиграция из побежденной страны и в первую очередь вывоз наиболее ценного человеческого материала, наукоемкого производства, полезных ископаемых);

2) полное разрушение той части структуры, которая отвечает за безопасность системы от внешних угроз (разрушение армии побежденной страны);

3) полное разрушение той части структуры, которая ответственна за восстановление элементов и структур подсистемы безопасности /разрушение производства, в первую очередь, наукоемкого производства, а также научных центров и всей системы образования; прекращение и запрещение разработок и производств наиболее перспективных видов вооружения);

4) разрушение и уничтожение той части структуры, которая не может быть использована победителем в собственных целях;

5) сокращение функциональных возможностей побежденной системы за счет сокращения ее информационной емкости (в случае страны: отделение части территории, уничтожение части населения).

Обобщив перечисленные признаки, можно ввести понятие "степень поражения информационным оружием", оценив ее через информационную емкость той части структуры пораженной системы, которая либо погибла, либо работает на цели, чуждые для собственной системы.

Информационное оружие даст максимальный эффект только тогда, когда оно применяется по наиболее уязвимым от него частям ИСС. Наибольшей информационной уязвимостью обладают те подсистемы, которые наиболее чувствительны к входной информации - это системы принятия решения, управления. На основании сказанного можно ввести понятие информационной мишени. Информационная мишень - множество элементов информационной системы, принадлежащих или способных принадлежать сфере управления, и имеющих потенциальные ресурсы для перепрограммирования на достижение целей, чуждых данной системе.

Исходя из определения информационной мишени, намечаются основные направления работ, как по обеспечению се безопасности, так и по повышению ее уязвимости. Например, для того, чтобы повысить уязвимость противника, следует максимально расширить его информационную мишень, т.е. подтолкнуть его на включение в мишень как можно больше равноправных элементов, причем желательно открыть доступ в сферу

управления таким элементам, которые легко поддаются перепрограммированию и внешнему управлению.

Заставить противника изменить свое поведения можно с помощью явных и скрытых, внешних и внутренних информационных угроз.

Причины внешних угроз в случае целенаправленного информационного воздействия (в случае информационной войны) скрыты в борьбе конкурирующих информационных систем за общие ресурсы обеспечивающие системе допустимый режим существования.

Причины внутренних угроз - в появлении внутри система множества элементов, подструктур, для которых привычный режим функционирования стал в силу ряда обстоятельств недопустимым.

Скрытая угроза - это неосознаваемые системой в режиме реального времени входные данные, угрожающие ее безопасности.

Связи с общественностью играют важную роль в жизни общества. Изначально созданные для информирования общественности о ключевых событиях в жизни страны и властных структур, они постепенно стали выполнять еще одну не менее важную функцию - воздействие на сознание своей аудитории с целью формирования определенного отношения к сообщаемым фактам, явлениям действительности. Это воздействие осуществлялось при помощи методов пропаганды и агитации, разрабатываемых на протяжении не одной тысячи лет.

В скором времени связи с общественностью заняли важное место в жизни государств, а с развитием техники и технологии стали активно использоваться и на международном уровне с целью приобретения каких-либо преимуществ контролируемым им государством. В наши дни особое внимание следует уделить роли связей с общественностью в международных конфликтах, в том числе и геополитического характера, поскольку в последние годы наряду с классическими видами оружия все чаще применяется информационно-пропагандистское, в основе которого - работа с различными средствами массовой информации.

Таким образом, на основе ранее сказанного, можно сформулировать следующие утверждения:

1. Наступление информационной эры привело к тому, что информационное воздействие, существовавшее испокон веков во взаимоотношениях между людьми, в наши дни все более очевидно приобретает характер военных действий.

2. В настоящее время накоплен значительный опыт научных исследований в области информационного противоборства и информационно-психологических войн. Какой бы смысл в понятие "информационная война" ни вкладывался, оно родилось в среде военных и обозначает, прежде всего, жесткую, решительную и опасную деятельность, сопоставимую с реальными боевыми действиями. Военные эксперты, сформулировавшие доктрину ИВ, отчетливо представляют себе отдельные ее грани и виды. Гражданское же население пока не готово в силу причин социального и психологического характера в полной мере ощутить всю опасность неконтролируемого применения НКТ в информационной войне.

3. Информация действительно стала реальным оружием. Пример с февральской атакой китайцев, затронувшей корневые серверы Интернет, стала чем-то большим, чем забавы нескольких хакеров. Этот инцидент мог стать "первым залпом" в глобальной информационной войне.

Информационная война идет уже в третьем поколении. Сергей Гриняев, доктор технических наук даёт следующую классификацию:

1-е поколение информационной войны - это РЭБ (радиоэлектронная борьба). Проводная, частотная, сотовая связь, подслушки, глушилки, блокировки, помехи и т.д.;

2-е поколение информационной войны - это РЭБ плюс партизанская и контрпартизанская пропаганда. Так было в Чечне в 90-х. У сепаратистов-боевиков были свои пропагандистские сайты в Интернете, они распространяли газеты и боевые листки, организовывали интервью для сочувствующих им западных журналистов. Контрпропаганда велась

доступными федеральному центру средствами как на территории конфликта и смежных территориях, так и на более широкую общественность.

3-е поколение информационной войны - это глобальная информационная война, специалисты называют её так же "войной на эффектах". Информационная войны вокруг событий в Южной Осетии - именно война третьего поколения.

Формирование вокруг России "санитарного пояса" из стран-соседей происходит политическими средствами - проведением цветных революций, формированием органов власти и парламентского большинства из проамериканских сил, и экономическими средствами - скупкой национальных бирж, наращиванием американского капитала в ключевых государственных отраслях и компаниях. Но в эпоху информационного общества ключевое значение приобрели СМИ, Интернет-каналы и контроль над информпотоками. Из представленного материала очевидно, что Россия в этом отношении значительно отстает от США. Для формирования нового многополярного мирового порядка России необходимо предпринимать решительные действия для прорыва в информационной сфере [36].

3.4. Информационная безопасность государства

Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации определяется в «Доктрине информационной безопасности Российской Федерации» (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895).

Под **информационной безопасностью Российской Федерации** понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

3.4.1.Виды угроз информационной безопасности Российской Федерации.

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

– угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

– угрозы информационному обеспечению государственной политики Российской Федерации;

– угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

– угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

В сфере внутренней политики.

Наиболее важными объектами обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются:

– конституционные права и свободы человека и гражданина;

– конституционный строй, национальное согласие, стабильность государственной власти, суверенитет и территориальная целостность Российской Федерации;

– открытые информационные ресурсы федеральных органов исполнительной власти и средств массовой информации.

Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Российской Федерации:

– нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;

– недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей;

– распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;

– деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации.

Основными мероприятиями в области обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются:

– создание системы противодействия монополизации отечественными и зарубежными структурами составляющих информационной инфраструктуры, включая рынок информационных услуг и средства массовой информации;

– активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России.

В сфере внешней политики.

К наиболее важным объектам обеспечения информационной безопасности Российской Федерации в сфере внешней политики относятся:

– информационные ресурсы федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;

– информационные ресурсы представительств федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, на территориях субъектов Российской Федерации;

– информационные ресурсы российских предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, реализующим внешнюю политику Российской Федерации;

– блокирование деятельности российских средств массовой информации по разъяснению зарубежной аудитории целей и основных

направлений государственной политики Российской Федерации, ее мнения по социально значимым событиям российской и международной жизни.

Из внешних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

– информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики Российской Федерации;

– распространение за рубежом дезинформации о внешней политике Российской Федерации;

– нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;

– попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях.

Система обеспечения информационной безопасности Российской Федерации является частью системы обеспечения национальной безопасности страны.

Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

3.4.2. Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются:

– Президент Российской Федерации,

– Совет Федерации Федерального Собрания Российской Федерации,

– Государственная Дума Федерального Собрания Российской Федерации,

– Правительство Российской Федерации,

– Совет Безопасности Российской Федерации,

– федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации,

– органы исполнительной власти субъектов Российской Федерации,

– органы местного самоуправления,

– органы судебной власти,

– общественные объединения,

– граждане, принимающие в соответствии с законодательством Российской Федерации участие в решении задач обеспечения информационной безопасности Российской Федерации [37].

Контрольные вопросы

1. Что такое информационное воздействие? Какие виды информационного воздействия существуют?

2. Перечислите пять признаков воздействия посредством СМИ, которые, на Ваш взгляд, встречаются чаще остальных? Приведите примеры.

3. Дайте определение понятию «специальные информационные операции». На какие виды они подразделяются?

4. Дайте определение понятию «информационная война». Кто впервые его использовал и при каких обстоятельствах?

5. Перечислите составные части информационной войны.

6. Каковы цели информационной войны?

7. В чем состоит отличие информационной войны от компьютерной атаки?