ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

ГОУ ВПО «САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ

УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА»

ИНСТИТУТ ПЕЧАТИ

**РЕФЕРАТ**

**ПО ДИСЦИПЛИНЕ «ИНФОРМАТИКА»**

**на тему: «ИНФОРМАЦИОННЫЕ ВОЙНЫ. ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО»**

Выполнила: студентка группы 41114

Сафина Е.О.

Проверила: Кузьмишина Т.М.

Оценка:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Самара

2007

**Содержание**

Введение

Информационные ресурсы современного общества

Проблема информационной безопасности личности, общества и государства

Информационное противоборство

Информационные войны

Заключение

Список используемой литературы

**Введение**

Развитие новых информационных технологий и их быстрое проникновение во все сферы жизни породило новое направление в современной информатике – **социальная информатика**, включающее в себя следующую проблематику:

* + - * Информационные ресурсы как фактор социально-экономического и культурного развития общества;
      * Закономерности и проблемы становления информационного общества;
      * Развитие личности в информационном обществе;
      * Информационная культура;
      * Информационная безопасность, а также другие проблемы, близкие к данным.

В данном реферате я рассматриваю проблему информационной безопасности, а именно подробнее описываю такие понятия как информационные войны и информационное противоборство.

# Информационные ресурсы современного общества

Обсудим вначале само понятие «информационный ресурс». **Ресурс** – это запас или источник некоторых средств. Всякое общество, государство, фирма и частное лицо имеют определенные ресурсы, необходимые для их жизнедеятельности. Традиционно различают следующие виды общественных ресурсов: материальные, сырьевые (природные), энергетические, трудовые, финансовые.

Одним из важнейших видов ресурсов современного общества являются **информационные ресурсы**. Значимость информационных ресурсов постоянно растет; одним из свидетельств этого является то, что уже на нынешней фазе продвижения к информационному обществу информационные ресурсы **становятся товаром, совокупная стоимость которого на рынке сопоставима со стоимостью традиционных ресурсов**.

Информационные ресурсы общества в настоящее время рассматриваются как стратегические ресурсы, аналогичные по значимости ресурсам материальным, сырьевым, энергетическим, трудовым и финансовым. Однако между информационными и другими ресурсами существует одно важнейшее различие: всякий ресурс после использования исчезает (сожженное топливо, израсходованные финансы и т.п.), а информационный ресурс остается, им можно пользоваться многократно, он копируется без ограничений. Более того, по мере использования информационный ресурс имеет тенденцию увеличиваться, так как использование информации редко носит совершенно пассивный характер, чаще при этом генерируется дополнительная информация. Вместе с тем необходимость понимать, что информационный ресурс несамостоятелен и сам по себе имеет лишь потенциальное значение. Только соединяясь с другими ресурсами – техникой, энергией, сырьем и т.д., информационный ресурс реализуется как нечто материальное.

Любая попытка дать классификацию информационных ресурсов общества оказывается неполной. В основу классификации можно положить:

* + - * Отраслевой принцип (по виду науки, промышленности, социальной сферы, по тому, к чему относится информация);
      * Форму представления (по виду носителей, степени формализованности, наличию дополнительного описания и пр.) и другие принципы.

Внутри каждого класса можно проводить дополнительное, более детальное разделение. Например, ресурсы сети Интернет можно разделять по их назначению и формам представления: сервисная информация, библиографическая информация, материалы телеконференций, программное обеспечение, видео и т.д.

Крупнейшей категорией информационных ресурсов являются **национальные информационные ресурсы**. Это понятие сформировалось не так давно, в начале 1980-х гг., в ответ на растущую зависимость развитых стран от объемов информации, уровня развития средств ее передачи и обработки. Классификацию национальных информационных ресурсов можно посмотреть в Таблице классификации информационных ресурсов.

# Проблема информационной безопасности личности, общества и государства

Информационное общество отнюдь не есть общество всеобщего благоденствия. Те же технологические факторы, которые порождают его позитивные черты и новые, специфические опасности. Рассмотрим некоторые из них.

По мере продвижения к информационному обществу все более острой становится проблема защиты права личности, общества и государства на конфиденциальность, т.е. секретность определенных видов информации. Уже сегодня в странах, в которых в массовом порядке используются компьютерные сет, предпринимаются огромные усилия по охране информации. Каждый человек, доверяющий информацию о себе государственному органу или фирме, вправе рассчитывать на то, что она не будет разглашена или использована ему во вред.

Проблемы нарушения информационной безопасности актуальны и для отдельных граждан, и для всевозможных фирм и организаций, и для страны в целом.

В последние годы мы имели возможность видеть, сколь тяжкими могут быть последствия нарушения информационной безопасности личности, связанные с использованием современных технологий.

Перечислим более конкретно некоторые опасности и проблемы, возникшие на пути к информационному обществу:

* + - * Реальная возможность разрушения информационными технологиями частной жизни людей или организаций;
      * Возможность все большего влияния на общество со стороны средств массовой информации и тех, кто эти средства контролирует;
      * Сложность отбора качественной и достоверной информации при большом ее объеме;
      * Сложность адаптации многих людей к среде информационного общества и необходимости постоянно повышать свой профессиональный уровень;
      * Появление у некоторых людей (особенно молодых) при столкновении с виртуальной реальностью, в которой трудно различимы иллюзия и действительность, мало изученных, но явно неблагоприятных психологических отклонений;
      * Сохранение социального расслоения людей при переходе к информационному обществу; более того, информационное неравенство, добавившись к существующим видам неравенства, может усилить социальную напряженность;
      * Сокращение числа рабочих мест в экономике развитых стран, которое, если его не компенсировать полностью созданием новых рабочих мест в информационной сфере, может привести к опасному социальному недугу – массовой безработице.

Государственную политику России в обсуждаемой сфере отражает *Доктрина информационной безопасности Российской Федерации*, принятая в 2000 г. Рассмотрим основные ее положения.

К объектам информационной безопасности РФ относятся:

* + - * Все виды информационных ресурсов;
      * Права граждан, юридических лиц и государства на получение, распространение и использование информации, защиту информации и интеллектуальной собственности;
      * Система формирования, распространения и использования информационных ресурсов, включающая в себя информационные системы различного класса и назначения, библиотеки, архивы, базы и банки данных, информационные технологии и т.д.
      * Информационная инфраструктура, включающая в себя центры обработки и анализа информации, каналы информационного обмена и телекоммуникации, механизмы обеспечения функционирования телекоммуникационных систем и сетей;
      * Система формирования общественного сознания (мировоззрения, моральных ценностей, нравственных оценок, социально допустимых стереотипов поведения и взаимоотношений между людьми), базирующаяся на средствах массовой информации и пропаганды.
      * В сферу национальных информационных интересов РФ входят:
      * Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и ее использования, обеспечения духовного становления России, сохранение и укрепление ценностей общества;
      * Информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности достоверной информации о государственной политике;
      * Развитие современных информационных технологий отечественной индустрии информации;
      * Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

В доктрине формулируются **методы обеспечения информационной безопасности** страны, включая правовые, организационно-технические и экономические, а также **особенности обеспечения информационной безопасности РФ** в различных сферах общественной жизни: экономической, политической, обороны, науки и техники и др.

Особенно актуальной для современной России является проблема обеспечения информационной безопасности в области науки и техники, в частности проблема «утечки мозгов». Дело в том, что многие отечественные (в основном молодые) ученые эмигрируют за границу, имея перспективу хорошо оплачиваемой научной деятельности. Часть этих ученых являются носителями важной научно-технической, экономической, оборонной информации. Ряд государств (в том числе и недружественных России) прилагают специальные усилия для привлечения научных работников из стран, входивших ранее в состав СССР. В связи с этим возникает проблема защиты научного потенциала нашей страны.

Доктрина информационной безопасности одной из важнейших объявляет проблему информационного неравенства, которое вносит раскол в общество и отчуждение между составляющими его группами населения, т.е. данная проблема имеет прямое отношение к национальной безопасности. Особенно важно преодоление проявлений информационного неравенства в образовании, поскольку:

* + - * Появилась тенденция разделения образовательных учреждений на элитные и массовые с соответствующей разницей в ресурсном обеспечении;
      * Велико различие уровней доходов семей учащихся;
      * Значителен разрыв в размерах финансового обеспечения образовательных учреждений в различных регионах страны.

Преодоление информационного неравенства в России является задачей первостепенной государственной важности.

# Информационное противоборство

Многочисленные межгосударственные, межрелигиозные, межнациональные противоречия сопутствуют человечеству с первых моментов его истории. Их прообразы проявлялись даже на том еще начальном этапе, когда еще не оформились государства, религии и нации. К сожалению, от этих противоречий не может уйти и современное общество. Более того, к традиционным видам противоборства добавился новый вид, порожденный информационными технологиями.

Успех в экономике, политике, науке, военном деле в решающей степени обусловлен тем, насколько быстро можно получить нужную и достоверную информацию, а также не менее важно не дать воспользоваться этой информацией конкуренту, неприятелю или противнику.

События последнего времени показывают, что победа даже в боевых действиях зависит не только от того, у кого больше солдат и танков, а определяется тем, чье оружие “умнее” и насколько оно аккумулирует последние достижения науки, техники и особенно информатики. Подтверждение этому – война в Ираке.

Обострение информационного противоборства в мире, последние проявления международного терроризма, диктатуры и авторитарности ряда государств повышают актуальность проблем технической защиты информации в Российской Федерации.

**Информационное противоборство** – это открытое и\или скрытое целенаправленное информационное воздействие систем друг на друга с целью получения определенного выигрыша в материальной сфере.

Под информационным противоборством следует понимать комплексное информационное воздействие на систему государственного и военного управления противостоящей стороны, на ее военно-политическое руководство.

Интенсивное внедрение информационных технологий, рост удельного веса безопасности информации в обеспечении национальной безопасности государства привели к тому, что информационный ресурс становится сегодня таким же богатством страны, как ее полезные ископаемые, производственные и людские ресурсы.

Сейчас экономическое могущество общества напрямую связывается с наличием в его распоряжении высоких технологий, и в первую очередь, в информационной сфере.

Превращение информации в товар привело к резкому обострению международной конкуренции за обладание информационными рынками, технологиями и ресурсами, а информационная сфера в значительной мере определяет и эффективно 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, которое представляет чрезвычайную угрозу национальной безопасности, в том числе и России, 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. При этом можно утверждать, что 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. Ими могут быть отдельные страны и их органы разведки, преступные, террористические и наркобизнесные группировки, коммерческие фирмы и даже лица, действующие без преступных намерений.

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

Концепция «Соперничество», сформулированная в США в 1986 году, констатирует: «Посредством правдивой и ложной информации об экономике, управлении, о вооруженной борьбе можно достичь целенаправленного регулирования процессов принятия необходимых для нас решений руководством другого государства».

Одним из основных элементов информационной войны являются психологические операции.

США вырабатывали и испытывали в Ираке стратегию и тактику применения информационного оружия. Накануне боевых действий против Ирака в марте 2003 года в Катаре был создан центр информационного обеспечения представителей мировых средств массовой информации, оснащенный самой современной техникой общей стоимостью 1 млн. долларов. Однако он использовался в интересах коалиционной группировки, которая давала очень дозированную информацию и только в выгодном для себя виде. В целях обеспечения доведения нужной информации до широких масс, США выбросили перед началом боевых действий на территорию Ирака 150 тысяч дешевых радиоприемников. Это прямое доказательство того, что психологические операции – боевое оружие. Одним из видов такого оружия является спутниковая система ТЕЛЕДЕЗИС (создана в США, насчитывает до 300 спутников), которая может применяться в тайных спецоперациях. Речь идет о программированном облучении человека. Специфическое «зомбирование» может проводиться по всей российской территории – от западной границы России до регионов Дальнего Востока. При этом плотность мощности излучения на поверхности Земли достигает десяти в минус восьмой-девятой степени Ватт на квадратный сантиметр.

При этом американские эксперты исходят из того, что в ближайшие годы в США возможно дополнение национальной доктрины «ядерного сдерживания» доктриной «направленной силы», одним из элементов которой, как ожидается, будет информационное оружие.

На совете национальной безопасности, состоявшемся в феврале 2003 года, Президент США утвердил «Положение о концепции и принципах ведения компьютерных информационных войн на территории других государств». Данная концепция определяет, когда и при каких обстоятельствах Президент США, директора агентства национальной безопасности и ЦРУ, министр обороны США и другие должностные лица могут принять коллективное или индивидуальное решение на проведение специальной операции по нейтрализации или полному разрушению информационного пространства чужого государства, выводу из строя или нейтрализации линий связи и управления, как с территории США, так и сопредельных к противнику территорий.

В последние три-четыре года в министерстве обороны США активизируются работы по созданию информационного оружия как одного из компонентов ведения информационной войны. Эксперты определяют это оружие как совокупность средств и методов, позволяющих похищать, искажать или уничтожать информацию; ограничивать или прекращать доступ к ней законных пользователей; нарушать работу или выводить из строя телекоммуникационные сети и компьютерные системы, используемые в обеспечении жизнедеятельности общества и государства. Так, в ходе ведущейся войны в Ираке вооруженные силы коалиции применили против иракских радиоэлектронных средств свою новейшую электромагнитную бомбу. Это устройство преобразует химическую энергию взрывчатого вещества в электромагнитный импульс высокой мощности (до 10 Гигаватт), что соответствует мощности крупной ГРЭС. При этом поражаются компоненты радиоэлектронной техники в радиусе более 250 метров и тем самым выводятся из строя системы связи, информатики и управления.

Широкие возможности по применению информационного оружия против России представляет использование в российских информационных системах программного обеспечения зарубежного производства, в которые могут быть вмонтированы фрагменты, активизирующие свою работу по специальному сигналу или при наступлении установленного времени. Эти фрагменты, называемые логическими бомбами или логическими закладками, могут вызывать сбои в работе информационных систем, искажение или полное уничтожение информационных ресурсов и, в конечном счете, привести к полной потере управляемости транспортными структурами, военными объектами, системами государственного управления, что может иметь катастрофические последствия для любой страны. Ярким примером логической закладки является «Чернобыльский вирус», ежегодно активизирующий свою работу 26 апреля в тех системах, куда был внедрен случайно или умышленно. Поиск и выявление логических бомб и закладок в программном обеспечении практически невозможен, так как фирмы-разработчики программного обеспечения практически никогда не продают исходных текстов, мотивируя это нежеланием раскрыть «ноу-хау» своих разработок.

Элементом информационного оружия могут считаться компьютерные вирусы, разработки которых не требуют больших материальных и финансовых затрат, а применение которых может быть высокоэффективным. Так, распространенный в конце января 2004 года в сети Интернет вирус практически парализовал работу этой сети на сутки в азиатских странах и снизил пропускную способность сети практически в два раза в странах Европы.

Помимо применения информационного оружия для нарушения работы систем командования и управления войсками и боевыми средствами специалисты также выделяют экономическую, банковскую, социальную и иные сферы его потенциального использования. При этом возможно достижение цели по дезорганизации деятельности управленческих структур, транспортных потоков и средств коммуникации. Только представьте себе последствия, которые могут возникнуть от нарушений в работе автоматизированных систем управления железнодорожным транспортом. В результате неудовлетворительной защиты информации от ее искажения возможна ситуация, когда грузопотоки пойдут не по назначению. К примеру, взрывчатка, предназначенная для шахтеров, может быть отправлена за рубеж и перехвачена террористическими организациями. Кроме того, с помощью информационного оружия возможно блокирование деятельности отдельных предприятий и банков, а также целых отраслей промышленности путем нарушения технологических связей, систем взаиморасчетов, проведения валютно-финансовых махинаций. Только высокий профессионализм лиц, ответственных за защиту информации, позволил предотвратить попытку преступников внедрить в банковскую компьютерную систему Москвы поддельные векселя с реквизитами Московского сберегательного банка с тем, чтобы похитить 375 млрд. руб. и 80 млн. долларов США.

Стратеги применения информационного оружия рассчитывают на массовое распространение и внедрение в сознание людей определенных представлений, привычек и поведенческих стереотипов. Получая информацию из СМИ, мы имеем возможность наблюдать широкомасштабные операции по информационному и морально-психологическому воздействию на население, государственные институты и руководство страны. Конечным же результатом использования информационного оружия в социальной сфере предполагается вызов недовольства или паники среди населения, а также провоцирование деструктивных действий различных социальных групп.

Наконец, целью применения информационного оружия является инициирование крупных техногенных катастроф на территории противника в результате нарушения штатного управления технологическими процессами и объектами, имеющими дело с большими количествами опасных веществ и высокими концентрациями энергии. Например, если произойдет одновременное открытие всех шлюзов Зейской ГЭС, то по расчету специалистов, на пятые сутки уровень воды в реке Амур будет таким, что затопит г. Хабаровск, а через сутки – г. Комсомольск-на-Амуре и г. Николаевск-на-Амуре.

В качестве основных объектов применения информационного оружия, как в мирное, так и в военное время выступают:

* + - * компьютерные системы и системы связи, используемые государственными и правительственными организациями;
      * информационные и управленческие структуры банков, транспортных и промышленных предприятий;
      * средства массовой информации и, в первую очередь, электронные.

Достижение успеха в любой войне, а тем более в информационной, невозможно без наличия достоверных сведений и разведывательных данных. В этих целях иностранные спецслужбы используют самые разнообразные способы и методы: от мониторинга открытых средств массовой информации до самых изощренных, включая промышленный шпионаж и техническую разведку. Иностранные технические разведки развернули глобальную систему разведки с применением технических средств. Многофункциональные разведывательные космические системы, наземные центры радио-, радиотехнической и радиолокационной разведки, стратегические самолеты-разведчики, морские системы и комплексы технической разведки действуют в настоящее время против России непрерывно. При этом расходы на разведывательную деятельность иностранных государств не сокращаются (например, в США они составляют ежегодно около 30 млрд. долларов). ЦРУ продолжает закупку новых технических средств для сбора развединформации, в том числе космических «спутников-шпионов», беспилотных летательных аппаратов «Предэтор», хорошо зарекомендовавших себя в ходе военной кампании в Афганистане и в Ираке. Пентагон делает ставку на «умное» оружие, управляемое со спутников, микроволновые бомбы и беспилотные самолеты. В 2000 году челночный корабль Шаттл произвел подробнейшие снимки 80% поверхности Земли. Эти материалы есть не что иное, как топогеодезическое обеспечение применения высокоточного оружия и полетов беспилотных самолетов-разведчиков. Используя эту информацию, высокоточные бомбы и крылатые ракеты могут направляться на объект военнослужащими спецподразделений, находящихся на территории противника и оснащенных специальными компьютерами, и это не зависит от метеоусловий.

Наиболее эффективным способом получения необходимой информации является использование технических разведок, на долю которых приходится до 80% добываемых сведений. В качестве примера можно привести Систему глобального контроля международных линий связи «Эшелон». Работу Системы «Эшелон» обеспечивает наземная сеть центров обработки информации, на которых размещены 96 комплексов радиоэлектронной разведки, она способна перехватить до 2 млн. сообщений в минуту. Две тысячи специалистов-лингвистов анализируют и расшифровывают информацию со 100 языков мира. Космическая группировка системы насчитывает от 20 до 40 летательных аппаратов. Периодичность их пролета над территорией Дальнего Востока составляет не менее 1-2 раза в час. Система позволяет перехватывать информацию, передаваемую в системах кабельной и радиосвязи, включая спутниковые каналы, циркулирующую в телефонных и компьютерных сетях, в том числе и «Интернет», а также обрабатывать полученную информацию в соответствии с заявками пользователей системы. Возможности Системы «Эшелон» позволяют осуществлять контроль за деятельностью, прежде всего, должностных лиц высшего эшелона власти, министерств, ведомств, отдельных организаций и граждан, а также использовать «Интернет» с целью несанкционированного доступа к закрытой информации.

Имеются и другие способы несанкционированного доступа к информации. Так, ученые Кембриджского университета в марте 2002 года опубликовали работу, в которой показали, что имеется принципиальная возможность с расстояния в несколько сотен метров восстанавливать картинку экрана просто по мерцанию света в окне комнаты, где установлен монитор. Также доказано, что с расстояния до полутора километров можно снимать данные с постоянно мигающих индикационных лампочек компьютерного оборудования. Не испытывая затруднений, можно практически в любом крупном городе купить спецаппаратуру и, например, тотально контролировать всю пейджинговую связь. С таким же успехом прослушиваются и сотовые телефоны даже тогда, когда они находятся в отключенном состоянии. Аналогичные примеры можно продолжать. Необходимо также отметить, что опасность в последнее время для ряда структур стали представлять и криминальные группировки, использующие в своей преступной деятельности самые изощренные способы негласного получения информации.

В наше время, когда ни одна уважающая себя фирма не может обойтись без компьютера, без доступа в «Интернет», проблемы защиты информации приобретают особое значение. Число пользователей «Интернет» в России составляет 6 млн., а к 2010 году достигнет 30-40 млн. Как известно, основные узлы сети «Интернет» расположены на американской территории и постоянно находятся под пристальным контролем спецслужб США, добывающих из них необходимую информацию. Таким образом, даже сообщение, отправленное электронной почтой из г. Владивостока в г. Хабаровск, сначала побывает в США, обработается специалистами разведки, а затем попадет к адресату.

Из средств массовой информации известно, что за две недели войны в Ираке зарегистрировано до тысячи попыток проникновения хакеров к базам данных только американской группировки войск. Поэтому в США уделяется большое внимание защите информационных ресурсов, особенно специального и военного назначения. Так, на ведение политики информационного противодействия американцы ежегодно тратят более 2 млрд. долларов. Общие расходы правительства США на реализацию концепции «Информационной войны» до 2005 года составят более 18 млрд. долларов.

По данным МВД России, за три года (2000-2002 г.г.) общее количество зарегистрированных преступлений в сфере высоких технологий возросло более чем в 63 раза, почти в 30 раз возросло количество преступлений, связанных с неправомерным доступом к компьютерной информации, в 137 раз – с созданием, использованием и распространением вредоносных программ для ЭВМ, в 75 раз – с незаконным производством, сбытом или приобретением специальных технических средств, предназначенных для негласного получения информации, в 41 раз – с нарушением правил эксплуатации ЭВМ, систем ЭВМ или их сетей. Не остаются «без внимания» хакеров и российские информационные центры. К примеру, только за 6 месяцев 2002 года ими было предпринято свыше 400 тысяч попыток атак на официальный сервер ФСБ России. В администрациях краев и областей Дальнего Востока еженедельно регистрируются до десяти попыток проникновения в базы данных.

В настоящее время задача обеспечения информационной безопасности Российской Федерации как неотъемлемого элемента ее национальной безопасности является важной составной частью ее национальных интересов. Невыполнение требований по защите информации может привести к существенным потерям в информационной сфере и, в конечном итоге, в экономике, политике и обороноспособности страны. Здесь необходимо отметить, что за нарушение правил защиты информации, приведшее к утечке сведений ограниченного распространения, у нас в стране предусмотрена ответственность по статьям Уголовного Кодекса Российской Федерации и Кодекса об административных правонарушениях Российской Федерации. В тоже время следует ясно осознать, что нейтрализовать угрозу информационного воздействия можно только, создав эффективно действующую государственную систему защиты информации. Нормативная правовая база определяет структуру системы технической защиты информации, которую образуют на территории субъекта Российской Федерации:

* + - * Советы по защите информации при руководителях органов исполнительной власти субъектов Российской Федерации;
      * постоянно действующие технические комиссии по защите государственной тайны на предприятиях, в учреждениях и организациях;
      * подразделения по защите информации;
      * территориальные органы федеральных органов исполнительной власти: управления ФСБ, МВД, Минюста, Государственного таможенного комитета, МЧС и другие;
      * предприятия, работающие со сведениями, составляющими государственную и служебную тайну, выполняющие свои основные функции на территории субъектов Российской Федерации;
      * научно-исследовательские, проектные и конструкторские организации по защите информации региональных органов власти;
      * региональные аттестационные центры;
      * предприятия, имеющие соответствующие лицензии и аккредитацию на оказание услуг в области защиты информации;
      * предприятия, имеющие соответствующие лицензии по противодействию иностранным техническим разведкам;
      * высшие учебные заведения и институты, занимающиеся подготовкой и повышением квалификации специалистов в области защиты информации.

В органах исполнительной власти субъектов Российской Федерации создаются:

* + - * Советы по защите информации от иностранных технических разведок и от её утечки по техническим каналам при руководителях органов исполнительной власти субъектов Российской Федерации;
      * постоянно действующие технические комиссии (ПДТК) по защите государственной тайны в органах исполнительной власти субъектов Российской Федерации (коллегиальный орган);
      * подразделения по защите информации (штатные специалисты).

Систему защиты информации в органах местного самоуправления и организациях образуют:

* + - * подразделения по защите информации;
      * постоянно действующие технические комиссии;
      * режимно-секретные органы;
      * экспертные комиссии.
      * Главными направлениями в работе по защите информации являются:
      * обеспечение эффективного создания и управления системой защиты информации;
      * определение сведений, охраняемых от технических средств разведки, и демаскирующих признаков, раскрывающих эти сведения;
      * анализ и оценка реальной опасности перехвата информации техническими средствами разведки;
      * выявление возможных технических каналов утечки сведений, подлежащих защите и др.

# Информационные войны

Информационная война не есть детище сегодняшнего дня. Многие приемы информационного воздействия возникли тысячи лет назад вместе с появлением информационных самообучающихся систем – история обучения человечества – это и есть своего рода постоянные информационные войны.

При этом вполне естественно, что с повышением способности информационных систем в части их обучения акцент все более и более будет смещаться в сторону применения не огнестрельного оружия, а информационного: если систему дешевле уничтожить и создать заново в нужном виде, чем переучить, то ее уничтожают; если же проще переучить, то ее переучивают. И чем лучше развиты информационные технологии, позволяющие переучивать (перепрограммировать), тем дешевле и эффективнее их применение.

Под системой могут приниматься: человек, компьютер, природный ландшафт и т. д. Разница между этими системами в том, что если у тех из них, которые принято называть информационными, модификация внутренних управ­ляющих структур связана с получением новой информации, с обучением, то модификации механических или природных геообразований, с нашей, человеческой точки зрения, носят несколько иной характер. Горный обвал может изменить течение реки, засыпав ее камнем и песком, а для того чтобы изменить поведение человека или животного, достаточно показать этот обвал; чтобы откорректировать горную цепь, требуется землетрясение, а для изменения поведения жителей достаточно информации о предстоящем землетрясении.

Чем полнее система воспринимает внешний мир, тем более «тонкими» энергиями можно воздействовать на ее поведение.

Под **информационной системой**будем понимать систему, осуществляющую: получение входных данных, обработку этих данных и (или) изменение собственного внутреннего состояния (внутренних связей – отношений); выдачу результатов либо изменение своего внешнего состояния (внешних связей – отношений).

**Простой информационной системой**называется система, элементы которой функционируют в соответствии с правилами, порожденными одним и тем же взаимно непротиворечивым множеством аксиом.

**Сложной информационной системой**наловим систему, которая содержит элементы, функционирующие в соответствии с правилами, порожденными отличными друг от друга множествами аксиом. При этом допускается, что среди правил функционирования различных элементов могут быть взаимно противоречивые правила и цели.

Взаимодействие элементов (в том числе и информационное противодействие) осуществляется через протоколы информационно-логического сопряжения между ними, средства и технологии их практической реализации. Протокол информационно-логического взаимодействия для элементов социального пространства нашел свое воплощение в естественном языке каждого народа. Использование того или иного языкового подмножества во многом определяет ин­формационные возможности различных групп населения.

Основными средствами корректировки протоколов информационно-логического взаимодействия для социального пространства сегодня стали средства массовой информации (СМИ).

Протокол информационно-логического взаимодействия для элементов кибернетического пространства отражен во множестве языков программирования, в сетевых протоколах. Основным средством корректировки этих протоколов являются компьютерные вирусы, а также всевозможные технические средства и технологии воздействия на каналы телекоммуникаций.

В зависимости от того, какие происходят изменения во внутреннем состоянии информационных систем, предлагается осуществить следующую классификацию этих систем:

* + - * класс А – системы с неизменным внутренним состоянием;
      * класс В – системы с изменившимся внутренним состоянием.
      * В свою очередь в классе В можно выделить следующие подклассы:
      * подкласс 1 – системы с неизменным алгоритмом обработки, но с изменяющимися данными (базы данных, отдельные массивы и т. д.), которые используются в процессе обработки входной информации;
      * подкласс 2 – системы с адаптивным алгоритмом обработки, т. е. алгоритм настраивается на условия применения; настройка осуществляется путем либо изменения управляющих коэффициентов, либо автоматического выбора алгоритма из множества равносильных алгоритмов;
      * подкласс 3 – системы с самомодифицирующийся целью и, соответственно, с полностью самомодифицирующимся алгоритмом, выходящим за пределы множества равносильных алгоритмов.

В частности, старинный классический телеграфный аппарат является в большей мере механической системой, осуществляющей обработку входных данных и возвращающейся в исходное состояние по окончании обработки (класс А), но, будучи оснащен процессором с памятью и алгоритмом для восстановления искаженных данных, поддерживающим несколько уровней протоколов информационно-логического взаимодействия, он вместе с подобными аппаратами уже переходит и разряд систем передачи данных (класс В).

То же можно сказать и про автоматизированные информационно-поисковые системы; в зависимости от реализации они могут быть отнесены к системам как первого подкласса, так и второго.

Системы управления также различаются не только по своим функциональным и потенциальным возможностям, но и по способам реализации.

Между указанными информационными системами могут вестись войны. Информационная война между двумя информационными системами — это открытые и скрытые информационные воздействия систем друг на друга в целях получения определенного выигрыша в материальной сфере.

**Информационное воздействие**предполагает применение информационного оружия, т. е. таких средств, которые позволяют осуществлять с передаваемой, обрабатываемой, создаваемой, уничтожаемой и воспринимаемой информацией задуманные действия.

Для систем подкласса 3 можно сформулировать определение информационной войны более конкретно.

**Информационная война**— это война в целях захвата сырьевых, энергетических, людских ресурсов другой страны с использованием высших уровней (идеологического, хронологического, методологического) обобщенных средств управления обществом.

При ведении информационной войны в общественное сознание народа страны-жертвы агрессии целенаправленно внедряются такие ложные представления об окружающем мире, которые позволяют агрессору в дальнейшем свободно манипулировать как правительством, так и народом этой страны и осуществлять захват необходимых ресурсов, практически не встречая никакого сопротивления, т. е. без вооруженного столкновения обычного типа.

Информационные войны ведутся между центрами концентрации управления информационными столкновениями, лишь иногда переходя в войны с применением оружия.

Агрессия осуществляется методом «культурного сотрудничества», через управляющую «элиту» страны – жертвы агрессии, которая в меру своего понимания думает, может быть даже искренне, что работает на свой народ, а в силу непонимания общего хода вещей является, по сути, марионеткой в руках агрессора, выполняя его планы.

В результате такой агрессии у народа-жертвы:

* + - * разрушается целостное восприятие окружающего мира, разрывается связь с окружающей природой и идет формирование фрагментарного, частичного, калейдоскопического сознания, легко поддающегося манипулированию извне, через подсознание;
      * рушится историческое самосознание, реальная история народа подменяется ложными мифами, целостный исторический процесс разрывается на части, которые противопоставляются друг другу;
      * связь с природой подменяется верой в идеалистические и материалистические «священные писания», которые сталкиваются между собой и ведут непримиримую вековую борьбу, исполняя принцип «разделяй и властвуй!»;
      * нормальные потребности человека в пище, одежде, жилище и прочем подменяются потребностью в деньгах, которая культивируется и доводится до страсти, тем самым обеспечивая зависимость населения от тех, кто владеет финансовой системой;
      * культивируются низменные инстинкты, подрывающие физическое, психологическое здоровье человека и разрушающие генофонд нации.
      * Что же касается кибернетического пространства, то его возникновение и ознаменовало собой начало эпохи информационных войн. Именно для кибернетических систем наработаны соответствующие средства, именуемые информационным оружием. Именно в кибернетическом пространстве, используя это оружие, можно добиваться определенных побед.

Поэтому если быть точным, то, говоря о современной информационной войне технических систем, следует употреблять термины **кибернетическая война**и **кибернетическое оружие***.*

Для технических систем самый простой пример выглядит следующим образом. Компьютерная программа получает на вход значения двух переменных и делит первое на второе. Понятно, что если злоумышленник или сама жизнь подсунет в качестве значения второй переменной ноль, то результат может быть самым неожиданным, что при определенных условиях приведет к гибели всей ранее накопленной информации.

Системы целенаправленного сбора информации и контроля за объектами в режиме реального времени выводятся из строя путем создания перегрузок; например, космическая техника, особенно базирующаяся на геостационарной орбите, совершенно неремонтнопригодна, не может быть оперативно заменена и очень уязвима перед воздействием современных средств радиоэлектронного подавления (РЭП). Дело в том, что приемное устройство связных и разведывательных спутников выполнено очень чувствительным (детекторы «Магнум» засекают сигналы начиная с 10-14 Вт) и защищено только от помех или перегрузок, сравнимых по длительности с продолжительностью полезных сигналов. Мегаваттное воздействие с поверхности Земли, произведенное самодельными средствами РЭБ на нужной частоте, неизбежно приведет к потере приемного устройства спутника, а следовательно, к выводу из строя всего канала сняли.

В основе приемов информационного воздействия лежит перепрограммирование информационных систем. Перепро­граммировать информационную систему – значит подобрать для нее такие входные данные, которые соответствуют цели программирования.

Определить **цель перепрограммирования –** значит найти в окружающем мире или специально создать информационную систему (эталон), на которую данная система должна стать похожей. При этом перепрограммируемая система и «эталон» должны «понимать» друг друга.

Как формировалась цель перепрограммирования в мире программного обеспечения для «народа», описывает А.П. Кулаичев: «Многие были свидетелями, но уже мало кто вспоминает о том, что заря Windows занялась во второй половине 1992 г. с беспрецедентного кру­госветного пропагандистского турне руководства Microsoft с массой речей и выступлений на сотнях бизнес-встреч, семинаров и международных выставок. Главной целью этой акции было всколыхнуть мировую общественность, увлечь за собой и привязать к себе ведущих мировых производителей, которые после переориентации своих перспективных разработок (и связанных с этим капиталовложений) уже не смогут уклониться от магистрального пути. А уж за ними поплетутся массы пользователей, быстро привыкающие считать такой мир единственным. Этот замечательный пример показал всем сообразительным, что затраты на рекламу значительно эффективнее, чем затраты на корпоративное «долизывание» продуктов. Поэтому с приходом Windows начались резкая деградация качества программного обеспечения и его усложнение. Тем самым несомненной заслугой Б. Гейтса является открытие и наглядная демонстрация сверхмощных механизмов массового порабощения в эру информационной цивилизации».

Подобрать входные данные для системы в соответствии с заданной целью перепрограммирования – значит заставить информационную систему «смотреть на мир чужими глазами», глазами той информационной системы, на которую данная система должна стать похожей, т. е. «глазами» эталона.

Способна ли информационная система защититься, если враг применит против нее описанный способ перепрограммирования информационных систем? Безусловно. Для этого достаточно «закрыть глаза» на те входные данные, которые подаются на вход противной стороной. Причем, что характерно, во многих странах данный способ защиты населения и страны закреплен законодательно.

«Даже в 70-е годы, когда Америка увязла в войне во Вьетнаме, американские СМИ, критикуя эту войну, «торпедируя» ее, не позволяли себе использовать съемки телеоператоров, работающих со стороны Вьетнама. Более того, в той же Америке, а также Англии, Франции и еще десятке стран существует строжайший законодательный запрет на использование любых кино-, фото-, видео- и печатных материалов, снятых или написанных на стороне тех, кто ведет боевые действия против армий этих стран, и даже просто имеющих сочувственные «врагам» интонации или же идеи» (В. Шурыгин).

В. Шурыгин, анализируя информационный аспект военных действий в Чечне, подробно описывает, как был реализован способ перепрограммирования информационной системы на практике:

«В среднем чеченская тематика занимала в программах НТВ от 10 до 18 минут на информационный выпуск, в «Вестях» (информационная программа российского телевидения) – от 3 до 7 минут. Так вот у НТВ до 80 % всех видеосъемок непосредственно боевых действий велось со стороны чеченских боевиков или использовались пленки, снятые со стороны сепаратистов. В «Вестях» это соотношение достигало 60 %. Оставшиеся 20 % НТВ обычно делило между съемками разрушений, обычно приписываемых армии, интервьюированием местных жителей-чеченцев, «страдающих от русской агрессии», или же комментариями своих тележурнал истов, в лучшем случае на фоне российских позиций, но чаще у сгоревшей российской техники. Так же примерно делили оставшийся эфир и «Вести».

Анализ публикаций таких газет, как «Московский Комсомолец» и «Известия», выявил следующее: лишь в одной из четырех статей упоминалась или раскрывалась точка зрения на происходящие события федерального командования. Три же из четырех публикаций или носили откровенно прочеченский характер, героизируя боевиков, преувеличивал их возможности, или жестко критиковали армию и ее действия в Чечне».

Опросы общественного мнения, проводимые НТВ, возможно, в целях проверки эффективности данного способа перепрограммирования, подтверждали, что для среднестатистического гражданина, регулярно смотрящего телевизор, отношение к собственной армии изменяется в худшую сторону, а цели боевиков становятся «ближе и понятнее».

Как грустно шутил Л. Шебаршин, в прошлом один из первых руководителей КГБ СССР: «Телевидение – средство общения мошенников с простаками».

Все виды информационного воздействия на информационную систему можно классифицировать еще и следующим образом:

* + - * входные данные – «сухие» факты;
      * входные данные – логически обоснованные выводы;
      * входные данные – эмоционально окрашенные утверждения.

Ощущении, являясь критерием субъективной достоверности в процессе познания, могут быть присущи только самообучающейся информационной системе класса В, для которой они выступают как рычаг управления субъектом и массами людей. При этом эмоциональный заряд для любой входной последовательности повышает скорость ее обработки информационной системой, порой минуя даже обязательные логические проверки. Например, эмоционально насыщенный крик о помощи или об опасности заставляет сразу же совершать определенные действия и уже только потом, если будет возможность, проверять логикой справедливость тех или иных утверждений.

Например, диктор телевидения монотонно сообщает о поездках по стране кандидатов в президенты. При этом без искажения фактов, говоря об одном из них, он подкрепляет слова мимикой, выражающей презрение, а в случае упоминания другого кандидата, наоборот, сияет от счастья. В результате у зрителей незаметно для них самих начинает формироваться соответствующее отношение к кандидатам. Видно, что в данном случае сама возможность сказать что-то (даже нейтральное) о том или ином кандидате может использоваться для перепрограммирования слушателей. Аналогичным образом формируются информационные материалы и прессе. Текст сообщения содержит «голые» факты, "к которым не может быть претензий, а название заметки, особенно если речь идет о конкурентах, имеет обязательную эмоциональную окраску. Сообщение прочитают не все, но на заголовок обязательно обратят внимание, а тем самым неявно свяжут возникшее эмоциональное ощущение с объектом газетного материала.

Сложившиеся стереотипы поведения – это то пространство действий, в котором конкретная система наиболее эффективно способна противостоять внешним, известным системе угрозам. Естественно, что для каждой системы именно собственные привычки и являются ее достоинством. Они во многом определяют данную систему, так как обеспечивали и обеспечивают ее существование. Навязывание собственных стереотипов поведения окружающим системам, особенно уже сформированным, неизбежно будет ослаблять последние. Это объяснимо – всегда тяжело играть на чужом поле, да еще по неизвестным правилам.

Из вышеизложенного можно предложить общую схему стратегии информационной войны.

Приведенная схема, безусловно, не отражает всех возможных подходов и приемов к организации и проведению операций по информационному воздействию. Ум человеческий более изощрен, чем любая возможная проекция генерируемых им мыслей в плоскость практических алгоритмов.

В типовую стратегию включено лишь то, что вытекает из доказанных ранее теорем, утверждений и следствий. Отсюда следует: если информационная система обнаруживает воздействие против себя комплекса приемов схемы, то это означает, скорее всего, что данная информационная система находится в состоянии информационной войны.

Причем, что интересно, подобный алгоритм целенаправ­ленного информационного воздействия, можно сказать, в зачаточном прообразе сегодняшней информационной войны был изложен почти сто лет назад в документе под названием «Протоколы собраний Сионских мудрецов». Не вдаваясь в споры о причинах и источнике данного документа, необходимо отметить, что его автора бесспорно следует назвать первым серьезным теоретиком в области построения типовых тактик и стратегий ведения информационных войн.

В названном документе можно прочитать следующее: «Чтобы привести наш план к такому результату, мы будем подстраивать выборы таких президентов, у которых в прошлом есть какое-нибудь нераскрытой темное дело, какая-нибудь «панама» – тогда они будут норными исполнителями наших предписаний из боязни разоблачений и из свойственного всякому человеку, достигшему власти, стремления удержать за собою привилегии, преимущества и почет, связанный со званием президента» (протокол 10).

«В руках современных государств имеется великая сила, создающая движение мысли в народе – это пресса» (протокол 2).

«Ни одно оповещение не будет проникать в общество без нашего контроля. Это и теперь уже нами достигается тем, что все новости получаются несколькими агентствами, в которых они централизуются со всех концов света. Эти агентства будут тогда уже всецело нашими учреждениями и будут оглашать только то, что мы им предпишем.

...Каждый, пожелавший быть издателем, библиотекарем или типографщиком, будет вынужден добыть на это дело установленный диплом, который, в случае провинности, немедленно же будет отобран» (протокол 12).

«Вы говорите, что на нас поднимутся с оружием в руках, если раскусят, в чем дело, раньше времени; но для этого у нас в запасе есть такой терроризующий маневр, что самые храбрые души дрогнут: метрополитеновые подземные ходы-коридоры будут к тому времени проведены во всех столицах, откуда они будут взорваны со всеми своими организациями и документами стран» (протокол 9).

Кратко и точно в «Протоколах» сказано практически обо всех аспектах информационной войны:

* + - * система управления (контроль властных структур);
      * средства перепрограммирования населения (средства массовой информации);
      * терроризм;
      * экономические войны;
      * средства экономического управления;
      * финансовая программа (протокол 20);
      * всеобщее голосование и т. д.

Данные протоколы носят методический характер. Они составлены так, что их может использовать любой, понимающий значимость тайной войны, – и их применение отнюдь не ограничивается тем далеким временем. С точки зрения значимости для теории информационной войны, данные протоколы, наверное, в чем-то аналогичны первым робким исследованиям по теории ядерного оружия, кстати, относящимся примерно к тому же времени.

Описанный алгоритм существовал века. В настоящее время изменились многие методы и приемы, они получили научное обоснование. Возникли целые научные дисциплины по управлению поведением человека, коллектива, общества. К ним относятся: социология, психоанализ, теория рекламы и т. п. Получил теоретическое обоснование гипноз, и были сделаны попытки перенесения методов гипнотического воздействия с отдельного индивидуума на коллективы и на целые человеческие общества.

Даже в прошлом веке не было достаточно эффективных средств массовой информации, научно обоснованных алгоритмов управления социумом; а возникнуть эти алгоритмы могли только с появлением теории программирования применительно к сегодняшним средствам вычислительной техники.

Потому что, еще раз повторим, **информационное оружие** – это, прежде всего, алгоритм. Применить информационное оружие – значит так подобрать входные данные для системы, чтобы активизировать в ней определенные алгоритмы, а в случае их отсутствия активизировать алгоритмы генерации нужных алгоритмов.

Имеющаяся на сегодняшний день теория алгоритмов позволяет объяснить, каким образом может осуществляться автоматическое написание программ для определенных предметных областей.

В настоящее время в США созданы и приняты на вооружение различные системы информационного оружия (ИНФОР), которые по предназначению и сферам (объектам) воздействия можно условно подразделить на три вида (класса):

* + - * ИНФОР-1 – нарушает и парализует информационные системы и сети, обеспечивающие функционирование органов управления государственных и военных объектов, промышленности, транспорта, связи, энергетики, банков и других учреждений.

К этому классу ИНФОР относятся «компьютерные вирусы», логические бомбы и другие средства. По оценкам западных специалистов вероятность восстановления нарушенных функций таких систем, и частности систем раннего предупреждения, СПРН (систем предупреждения о ракетном нападении), систем управления ПРО, довольно низкая. Целенаправленное вторжение в их работу может иметь особо тяжелые последствия, сопоставимые с последствиями применения оружия массового поражения.

* + - * ИНФОР-2 – оказывает влияние на психику людей, что позволяет управлять их поведением.

Имеются сообщения о так называемом «вирусе №666», который обладает способностью губительно воздействовать на психофизиологическое состояние оператора ЭВМ. Этот вирус-убийца выдаст на экран особую цветовую композицию, погружающую человека в своеобразный гипнотический транс и вызывающий у него такое подсознательное восприятие, которое меняет функционирование сердечно-сосудистой системы вплоть до блокировки сосудов головного мозга.

* + - * ИНФОР-3 – новое поколение оружия, возможности которого держатся в секрете; однако можно предположить, что по результатам своего воздействия оно будет более эффективно и разрушительно.

Информационное оружие, созданное к США в результате крупного технологического прорыва, вполне способствует его материализации в обозримом будущем. Экономичность информационного оружия позволяет, с одной стороны, сокращать в определенной мере военный бюджет, а с другой – создать высокоэффективное оружие XXI века, применение которого сулит многообещающие результаты.

Процессы, проходящие в последнее время в общественной жизни России, явно свидетельствуют о ведении целенаправленного информационного воздействия на общество в целом.

Зная алгоритмы воздействия на индивидуум, можно достаточно точно описать алгоритм информационного воздействия на общество в целом. Для этого возьмем за основу работу Ч. Тарта «Состояния сознания» и попробуем по аналогии перенести методы гипнотического внушения с индивидуума на коллектив. Наведение гипнотического состояния на отдельного индивидуума у Ч. Тарта описывается в виде алгоритма так:

* + - * расслабить тело (цель данного действия: организм как целое должен исчезнуть в качестве объекта сознания);
      * слушать только гипнотизера, отбросив иные мысли или ощущения (цель: процесс нагружения сознания и действие формирующих сил ослабляются);
      * не размышлять над тем, что говорит гипнотизер (цель: торможение непрерывного потока мыслей);
      * сосредоточить внимание на каком-то предмете помимо голоса самого гипнотизера цель: подсистема сознания, ответственная за обработку чувственной информации, оказывается не в состоянии выполнять свою функцию и как бы расстраивается);
      * гипнотизер внушает, что вы спите или засыпаете (цель: внушение сна ослабляет память и чувство самоотождествленности, которыми характеризуется состояние бодрствования);
      * гипнотизер убеждает человека, что это не совсем настоящий сон (цель: создание пассивного состояния созна­ния, в котором сохраняется возможность контакта с гипнотизером).
      * по аналогии процесс наведения гипнотического состояния на отдельное общество мог бы, наверное, выглядеть следующим образом:
      * расслабить общество – внушать через средства массовой информации, что врагов нет, при этом обсуждать отдельные исторические периоды и интересы отдельных народностей (цель: общество как целое должно исчезнуть в качестве объекта сознания);
      * заставить общество слушать только противника, не обращая внимания на какие-то иные мысли или ощущения, например: акцентировать средства массовой информации на некой одной парадигме общественного развития, скажем западной, исключив любой другой опыт: Китай, Японию, мусульманский мир (цель: процесс нагружения общественного сознания и действие формирующих сил ослабляются);
      * заставить общество не размышлять над тем, что говорит противник, для этого исключить из средств массовой информации серьезные аналитические исследования проблем (цель: способствовать торможению непрерывного потока мыслей);
      * сосредоточить внимание общества на каком-то предмете, помимо входного информационного потока, например на внутренних катаклизмах, войнах, атаках террора (цель: подсистема защиты, ответственная за обработку входной информации, оказывается не в состоянии выполнять свою функцию и как бы расстраивается);
      * постоянно внушать, что и само общество, и отношение к нему окружающего мира становиться лучше и лучше (цель: подобное внушение ослабляет историческую память и чувство самоотождествленности, которыми характеризуется нормальное состояние общества);
      * средства массовой информации одновременно должны убеждать членов общества, что возникшее состояние – это не совсем то, что должно быть (цель: создание пассивного состояния сознания, в котором сохраняется возможность зависимости от информационного воздействия противника).

Приведенный алгоритм в общих чертах отражает работу средств массовой информации в России периода 1990 – 1997 гг.

В заключение можно сказать, что сегодняшнему миру уже не свойствен дефицит информации и промышленных товаров, наоборот, его отличает именно их избыток. А это значит, что цель информационной войны не защита информации, а защита от информации и продвижение своего видения мира, а в условиях экономической войны речь идет о защите от чужих товаров и навязывании своих.

# Заключение

Массовое внедрение информационных технологий во все сферы жизни общества привело часть человечества в конце XX века в начальную стадию новой общественной формации, получившую собирательное название – информационное общество. Резкое увеличение объемов информации, с которым столкнулся современный человек, привело не только к новым упрощающим это информационное разнообразие параметрам, таким, как имидж, но и к новым положительным и отрицательным тенденциям в этой области. Информационная война лежит в рамках подобных изменений. Цивилизация резко усилила эту свою составляющую, в какой-то мере выпустив ее из-под контроля. По этой причине возможно возникновение даже такого варианта, как информационная война против своего собственного народа. Ведь, наверное, так можно рассматривать идущее повсюду засилье массовой культуры. Пол Кеннеди пишет: «Упрощенность» американской культуры, которая проявляется в чрезмерном внимании к удовлетворению потребительского спроса, поп-культуре, комиксам, громкости, яркости красок и развлечений в ущерб серьезному размышлению, воспринимается как удар, нанесенный Америкой самой себе. В среднем американский ребенок проводит у телевизора пять тысяч часов еще до поступления в школу, а ко времени ее окончания эта цифра приближается к двадцати тысячам. Распространению этой антиинтеллектуальной культуры – проявляющейся в дальнейшем в увлечении спортивными программами и «мыльными операми» – способствуют и такие факторы, как распад семьи.

За исключением некоторых групп населения, уделяющих особое внимание образованию (евреи, американцы азиатского происхождения), средний американский ребенок, как утверждается, усваивает систему ценностей массовой индустрии развлечений, а отнюдь не моральные установки, воспитывающие дисциплину и любознательность ума, желание учиться» (Кеннеди П. Вступая в двадцать первый век. - М., 1997. - С. 362).

Как видим, перед нами общие проблемы, поскольку массовая культура как раз носит транснациональный характер, нигде не являясь естественным продуктом с точки зрения общества.

Информационные войны становятся реалией сегодняшнего дня, поэтому противодействие им также должно стать приметой нашего времени.

# Список используемой литературы

1. Володихин, Дмитрий. [Рецензия] [Текст] / Дмитрий Володихин // .-2005.-№12.-С.263;
2. Маньков, Виктор Дмитриевич. Безопасность общества и человека в современном мире [Текст]: [учеб. пособие для техн. вузов] / В.Д. Маньков, 2005.-551с.;
3. Могилев, Александр Владимирович. Информатика [Текст] / А.В. Могилев, Н.И. Пак, Е.К. Хеннер; под ред. Е.К. Хеннера, 2004.-841с.;
4. Почепцов, Георгий. Информационные войны [Текст] / Георгий Почепцов, 2000.-576с.;
5. Фролов, Дмитрий Борисович. Информационная война: эволюция форм, средств и методов [Текст] / Д.Б. Фролов // Социология власти.-2005.-№5.-С.121-143.

Национальные информационные ресурсы

|  |
| --- |
| Библиотечные ресурсы |
|  |
| Архивные ресурсы |
|  |
| Научно-техническая информация |
|  |
| Правовая информация |
|  |
| Информация государственных (властных) структур |
|  |
| Отраслевая информация |
|  |
| Финансовая и экономическая информация |
|  |
| Информация о природных ресурсах |
|  |
| Информация предприятий и учреждений |

Таблица. Классификация национальных информационных ресурсов