Создание глобальной сети интернет в значительной степени способствовало появлению новых возможностей в сфере информационной войны. В настоящее время всемирная паутина включает в себя свыше 40 млн. компьютерных абонентов более чем в 154 странах мира и около 1 млрд. пользователей, в том числе примерно 845 миллионов – регулярных.

1. **Информационные войны**

|  |  |  |
| --- | --- | --- |
| 31 Янв 2008 | [Распечатать](http://www.rususa.com/news/print.asp-nid-30622) | В закладки В закладки [Закладки на RusUSA](http://www.rususa.com/bookmarks/add.asp?url=http%3A%2F%2Fwww%2Erususa%2Ecom%2Fnews%2Fnews%2Easp%3Fnid%3D30622%26catid%3D2&title=%C8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%FB%E5+%E2%EE%E9%ED%FB)[Добавить в StumbleUpon](http://www.stumbleupon.com/submit?url=http%3A%2F%2Fwww%2Erususa%2Ecom%2Fnews%2Fnews%2Easp%3Fnid%3D30622%26catid%3D2&title=%C8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%FB%E5+%E2%EE%E9%ED%FB)[Добавить в Technorati](http://technorati.com/faves?add=http%3A%2F%2Fwww%2Erususa%2Ecom%2Fnews%2Fnews%2Easp%3Fnid%3D30622%26catid%3D2)[Добавить в delicious](http://del.icio.us/post?url=http%3A%2F%2Fwww%2Erususa%2Ecom%2Fnews%2Fnews%2Easp%3Fnid%3D30622%26catid%3D2&title=%C8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%FB%E5+%E2%EE%E9%ED%FB)[Добавить в Facebook](http://www.facebook.com/share.php?u=http%3A%2F%2Fwww%2Erususa%2Ecom%2Fnews%2Fnews%2Easp%3Fnid%3D30622%26catid%3D2)[Добавить в MySpace](http://www.myspace.com/Modules/PostTo/Pages/?t=http%3A%2F%2Fwww%2Erususa%2Ecom%2Fnews%2Fnews%2Easp%3Fnid%3D30622%26catid%3D2&title=%C8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%FB%E5+%E2%EE%E9%ED%FB)[Добавить в Google](http://www.google.com/bookmarks/mark?op=edit&output=popup&bkmk=http%3A%2F%2Fwww%2Erususa%2Ecom%2Fnews%2Fnews%2Easp%3Fnid%3D30622%26catid%3D2&title=%C8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%FB%E5+%E2%EE%E9%ED%FB)[Digg it](http://digg.com/submit?phase=2&url=http%3A%2F%2Fwww%2Erususa%2Ecom%2Fnews%2Fnews%2Easp%3Fnid%3D30622%26catid%3D2&title=%C8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%FB%E5+%E2%EE%E9%ED%FB)[Reddit](http://reddit.com/submit?url=http%3A%2F%2Fwww%2Erususa%2Ecom%2Fnews%2Fnews%2Easp%3Fnid%3D30622%26catid%3D2&title=%C8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%FB%E5+%E2%EE%E9%ED%FB)[Добавить в Memori.ru](http://memori.ru/link/?sm=1&u_data%5burl%5d=http%3A%2F%2Fwww%2Erususa%2Ecom%2Fnews%2Fnews%2Easp%3Fnid%3D30622%26catid%3D2&u_data%5bname%5d=%C8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%FB%E5+%E2%EE%E9%ED%FB)  |

**просмотрено (1643)**   **рейтинг (2/2)**

Военные и ученые ряда развитых стран мира уже приступили к активной разработке и созданию "информационного оружия", а также заявили о подготовке к ведению информационных войн. Уже создаются спецподразделения в вооруженных силах и других силовых структурах ряда государств. Исходя из этого, вооруженные силы России также начали разработку концептуальных решений, элементов и способов ведения информационных операций, сообщил сегодня первый заместитель начальника Генштаба ВС РФ генерал Александр Бурутин на заседании Национального форума информационной безопасности "Инфофорум", сообщает РИА "Новости".

Цели войны теперь достигаются не за счет силы, а "за счет технологического и информационного превосходства", было заявлено на "Инфофоруме", который проводится под патронажем правительства РФ и рассматривает ключевые проблемы безопасности страны. Среди его участников - руководители ФСБ, ФСО, Мининформсвязи, Росинформтехнологий, а также члены Торгово-промышленной палаты, Российского союза промышленников и предпринимателей.

"Информационное оружие" сочетает невысокий уровень затрат и высокую эффективность применения. "Оно не уничтожает противника, для него не требуется создание сложных структур и при этом нет необходимости пересекать границы", - отметил генерал. Наряду с воздействием на средства телекоммуникаций, одним из главных объектов воздействия информационного оружия "остаются люди, их мировоззрение". И это воздействие, по данным Бурутина, уже "ведется по линии разрушения духовных ценностей, путем воздействия на индивидуальное, групповое и массовое сознание" населения России.

По словам военного, с помощью такого оружия рядом неправительственных организаций, поддерживаемых из-за рубежа, формируется негативный образ России, передает "Интерфакс". И Россия предпринимает действенные меры для противодействия информационному оружию, которое применяется извне.

"Уже ряд стран взяли курс на ведение информационных войн. Объемы финансирования на эти цели свидетельствуют о том, что превосходство в информационной сфере рассматривается как один из основных способов достижения национальных стратегий этих стран в 21 веке", - сказал первый замначальника Генштаба ВС РФ.

Потребители информации, к которым относится все население развитых стран и большинство жителей стран развивающихся, исследуются, как под микроскопом, тщательно изучаются их привычки и желания, а затем населению внедряются необходимые установки, желания и знания. Немаловажную роль в этом играет и "организационное оружие", среди методов которого - поиск общего врага, принцип "разделяй и властвуй", контрпропаганда.

И российские силовые структуры стремятся сохранить информационную независимость.

**Теория информационного оружия**

Американский военный аналитик, полковник ВВС США Ричард Шафрански в своей статье "Теории информационного оружия" отмечает, что "цель информационной войны - так повлиять на поведение противника, чтобы он не знал, что на него воздействовали. Успешная информационная кампания ведет к решениям (и действиям) противника, которые противоречат его намерениям или мешают их выполнению. Цель информационных атак на оперативном уровне – создание таких помех, которые не позволяют противнику действовать скоординированно и эффективно. Гармонизация действий на обоих уровнях заставляет противника принимать решения, которые помогают нам достигать наших целей и мешают противнику добиваться выполнения своих".

"Информационная технология в наше время делает возможным "управление" при минимальном насилии и кровопролитии", - пишет Шафрански, отмечая, что если открытое вооруженное столкновение - это ряд смертоносных процессов, то "победа в информационной войне - это подчинение врага и абсолютная власть над ним".

Информационная война может проводиться как часть большего и более полного набора военных действий - сетевой войны или кибервойны - или выступать в качестве единственной формы ведения военных действий.

"Противник" - это любой, чьи действия противоречат целям лидера. Вне государства это может быть "образ врага" или "не мы". Внутри, врагом может быть предатель или путешественник, любой, кто противостоит или недостаточно поддерживает лидера, который управляет средствами информационной войны. Если члены группы не поддерживают цели лидера в ходе боевых действий, внутренняя информационная война (включая такие вещи, как пропаганда, ложь, террористические акты и слухи) могут быть использованы в попытке заставить их быть более лояльными к целям лидеров.

Стратегические информационные системы в высокотехнологичных государствах часто дублируются на оперативном уровне. Информационная война не должна откладываться до тех пор, пока враждебность не станет открытой, заключает Шафрански.

**Подготовка ведущих стран к глобальной информационной войне**

Пару лет назад Центральное разведывательное управление (ЦРУ) упоминало только Россию и Китай в качестве основных источников угрозы из киберпространства. Сегодня американские эксперты отмечают, что уже более 20 стран планируют и осуществляют различные виды информационных операций, направленных против Соединенных Штатов. ЦРУ отмечает, что ряд противостоящих США государств, включают информационную войну как часть их новых военных доктрин.

Рассекреченная оценка угрозы, проведенная Военно-морским флотом США, выделяет Россию, Китай, Индию и Кубу в качестве стран, которые открыто подтвердили политику подготовки к информационной войне и которые быстро развивают их способности в этом направлении. Северная Корея, Ливия, Иран, Ирак и Сирия, по сообщениям, имеют некоторую способность к движению в этом направлении, а Франция, Япония и Германия уже весьма активны в этой области.

**Россия**

До последнего времени в России практически не существовало ясной государственной позиции по этой проблеме, что, собственно, и привело к поражению в холодной войне, отмечает научный работник, журналист Сергей Гриняев. Только в сентябре 2000 года президентом РФ была подписана Доктрина информационной безопасности России. В отличие от подхода, обозначенного США, в российской Доктрине на первое место ставится обеспечение информационной безопасности индивидуального, группового и общественного сознания.

Для реализации основных положений Доктрины и обеспечения информационной безопасности России было создано Управление информационной безопасности в Совете безопасности РФ.

Сегодня в работах по разработке отечественного представления информационной войны занимаются Министерство обороны, ФАПСИ, ФСБ и знаменитое Управление "Р" МВД, которое проводит расследования преступлений в высокотехнологической сфере информационных технологий.

**США**

Деятельность американской администрации в области защиты критической инфраструктуры берет свое начало с формирования Президентской комиссии по защите критической инфраструктуры в 1996 году.

На исполнение указаний президента, обозначенных в этом направлении, был разработан Национальный план защиты информационных систем США, подписанный президентом 7 января, 2000 года. На реализацию этого плана было затребовано 2,03 миллиарда долларов из федерального бюджета.

С целью улучшения способности активно защищать информационные системы и компьютеры была создана Объединенная оперативная группа по защите компьютерной сети Министерства обороны, а главнокомандующий космического командования принял полную ответственность за защиту сетей ЭВМ министерства c 1 октября 1999 года.

С 2000 года Министерством обороны начата работа с союзниками по вопросу обеспечения информационной безопасности: Канада имеет официального представителя, работающего в США, развивается система разделения информации между Министерствами обороны в соответствии с основными положениями Меморандума о понимании и Концепции действий подписанными с канадской стороной.

Тем не менее, отмечает эксперт, информация, доступная по каналам интернета, позволяет сделать вывод о том, что уровень информационной безопасности систем Минобороны США, несмотря на реализованные мероприятия, увеличился незначительно. Атаки китайских хакеров на системы Минобороны оказались достаточно эффективными.

**Китайская народная республика**

Китай уже давно включил термин "информационная война" в лексикон своих военных специалистов. Сегодня он неуклонно движется к формированию единой доктрины информационной войны. Фактически, если революция в военном деле определяется как существенное изменение в технологии, дающее преимущество в военном обучении, организации, стратегии и тактике военных действий, то, возможно Китай из всех стран сегодня испытывает истинную революцию в киберпространстве.

Китайская концепция информационной войны включает уникальные китайские представления о войне вообще, основанные на современной концепции "народной войны", 36 стратегем великого Сун Цзы, а также местных представлениях о том, как воевать на стратегическом, оперативном и тактическом уровне. Многое из его подхода имеет отношение к акценту на обмане, войне знаний и поиске асимметричных преимуществ над противником.

Информационная война определена как "переход от механизированной войны индустриального возраста к войне решений и стиля управления, войне за знания и войне интеллекта".

Китай развивает концепцию Сетевых сил (воинские подразделения численностью до батальона), которые состояли бы из высококлассных компьютерных экспертов, обученных в множестве государственных университетов, академий и учебных центров. Основной акцент делается на привлечение активной молодежи.

**Великобритания**

Британское представление об информационной войне схоже с американским. Это определение информационной войны как действий, воздействующих на информационные системы противника, при одновременной защите собственных систем.

Кроме того, Великобритания использует юридическую структуру, основанную на существующих законах, которая в значительной степени может применяться к действиям в киберпространстве - Regulation of Investigatory Powers Act (RIP), принятый в 2000 году.

Он предлагает, что нападения на информационные системы может рассматриваться как обычное уголовное преступление со всеми вытекающими последствиями. Данный акт позволяет британскому правительству перехватывать и читать электронную почту, а также требовать расшифровки личных файлов по требованию государственных чиновников.

**Франция**

Французы рассматривают концепцию информационной войны, состоящей из двух главных элементов: военной и экономической (или гражданской). Военная концепция предполагает несколько ограниченную роль информационных операций и направлена на миротворческие цели. В этом контексте, союзники не рассматриваются противниками.

Напротив, экономическая или гражданская концепция включает более широкий диапазон потенциального применения информационных операций. В этом случае французы не видят себя связанными рамками НАТО, ООН или согласием США. Их подход к экономическому конфликту позволяет быть и союзником и противником одновременно. Французы даже имеют экономическую школу для информационной войны.

Франция активно формирует структуры по контролю ее граждан в киберпространстве. Есть информация о том, что французы создали собственную версию системы "Эшелон" (по сообщениям американской прессы система направлена на перехват фактически всех частных глобальных коммуникаций). Frenchelon, так некоторые назвали эту систему, по сообщениям, используется для контроля и анализа французских коммуникаций особенно в районе Парижа.

**Информация стала для жителей Земли воздухом**

Информация пронизывает все сферы современной жизни и для молодой части населения Земли уже есть единственная реальность и коммуникация с миром: интернет, ТВ и печать - все что нужно, чтобы чувствовать себя обладателем информации, а значит, иметь власть.

Сфера применения информационного оружия настолько широка, что лишь им одним можно выигрывать и проигрывать войны. Методы применения информационного оружия хорошо зарекомендовали себя и во время цветных революций в Грузии и Украине.

Информационное "оружие" называли оружием будущего и нынешний американский президент Джордж Буш, и бывший президент Билл Клинтон, его давно применяют на практике Пентагон и ЦРУ. Главный поражающий фактор информационного "оружия" - манипуляция сознанием.

Огромную роль в глобализации информационных войн играет интернет. С ростом его популярности некоторые люди настолько увлекаются виртуальным пространством, что начинают предпочитать интернет реальности, проводя за компьютером до 18 часов в день. Это - наркотизирующий воображаемый мир, и мышление погруженного в него человека становится аутистическим. Вследствие чего и происходит манипуляция.

Отметим, что власти России неоднократно пытались контролировать интернет. При Владимире Путине этот вопрос остро не стоял. Сам Путин не особо пользуется интернетом и, по информации директора Института национальной стратегии Станислава Белковского, "воспринимает его как маргинальное явление, неспособное существенно влиять на умы людей". Между тем будущий президент России Дмитрий Медведев - активный пользователь интернета, который читает про себя в интернете и знает, что это - мощное информационное оружие.

Информационное пространство фактически стало театром военных действий, где каждая противоборствующая сторона стремится получить преимущество. Средствами реализации программно-технических методов являются компьютерные вирусы, логические бомбы и аппаратные закладки, а также специальные средства проникновения в информационные сети.

**Жертвы без жертв: страх терроризма как средство психологического воздействия**

Для России сегодня актуальным стал давно разработанный на Западе страх терроризма как эффективное средство манипуляции сознанием. Политические силы, борющиеся с государством или, напротив, с его противниками, стали использовать террор в "войне всех против всех", запугивая население, отмечает с воем исследовании историк, философ и политолог Сергей Кара-Мурза.

Главной целью подобного метода является не убийство конкретных личностей, а воздействие на чувства широкого круга людей. Согласно принятому в американской политологии понятию, терроризмом является "угроза или использование насилия в политических целях отдельными лицами или группами, которые действуют как на стороне, так и против существующего правительства, когда такие действия направлены на то, чтобы оказать влияние на большее число людей, чем непосредственные жертвы".

Деморализованные и запуганные люди делают сами, требуют от властей или хотя бы одобряют действия, которые этим людям вовсе не выгодны. Иногда самый большой выигрыш от этого получают политики, которые пользуются страхом населения перед терактом.

Как отмечает Кара-Мурза, терроризм возник вместе со СМИ и связан с ними неразрывно. Современный терроризм немыслим без СМИ, которые внедряют страх перед ним в каждый дом.

………….

1. Свободное распространение информации в Интернете не на шутку беспокоит спецслужбы, осознавшие свою слабость перед лавинообразно увеличивающимся потоком информации. Возможности всемирной паутины все чаще используются в целях различной пропаганды. Уже сегодня мировое сообщество стоит на пороге новой эпохи информационных противоборств, эпохи кибервойн.

**Интернет – оружие будущего**

С древних времен информация являлась важнейшей составляющей любых политически значимых действий. Чем более развитым становилось общество, тем более изощренными становились методы получения и распространения разнообразной политической информации и дезинформации, а также политической пропаганды. На современном этапе можно с уверенностью говорить об информационных баталиях и войнах, глобальных информационных противоборствах и локальных конфликтах, которые уже давно не ограничиваются вбрасыванием дезинформации. Стало очевидно, что современное общество зависимо от информационных систем, а наиболее современный способ воздействия на противника – воздействие на его граждан с помощью информации. Именно поэтому для достижения своих целей выгоднее использовать информационное оружие, нежели традиционное вооружения. В этом контексте Интернет является очень грозным средством.

Первоначально термин «информационная война» использовал 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. Публикация этого отчета послужила началом активной кампании в средствах массовой информации. Военные аналитики США начали активно исследовать данное направление. Пик изучения данной проблематики, пришелся на период распада СССР. Если вспомнить развал Советского Союза, то без сомнения можно сказать, что он стал результатом информационной открытости и беззащитности, которая пришла в страну вместе с перестройкой.

**Российские кибервойны**

Согласно одному направлению кибервойны исследуются как развитие и распространение информационных технологий, в военной области подразумевая под собой высокоточное оружие, технологии стелс, боевые и разведывательные радиоэлектронные средства и, даже, футуристические разработки в области роботизации и автоматизации. Другое направление исследований понимает кибервойны, как элемент информационных войн, осуществляемый по средствам всемирной паутины.

Интернет упростил жизнь многим традиционным СМИ. Большинство газет превратились в своего рода дайджест интернета. Появились даже специализированные газеты и журналы, публикующие исключительно материалы из всемирной паутины. Так или иначе, журналисты все больше работают с интернетом как с источником информации. В газетах и журналах появляются материалы из сети, на особенно популярные web-издания ссылаются центральные СМИ.

Интернет-СМИ отличаются от обычных средств массовой информации тем, что там можно публиковать новости не только дешево и оперативно, но и что самое примечательное анонимно. Это делает их идеальным инструментом для различного рода политических провокаций. Хронологию этих провокаций в российском интернете можно отсчитывать с ноября 1998 года, когда на российском сервере бесплатных web-страниц был размещён сайт "Коготь", содержащий список домашних адресов и телефонов многих известных чиновников, расшифровки телефонных переговоров, а также некоторые оперативные подробности. "Коготь" был прикрыт спецслужбами через пару часов после появления в сети. Но появилась его вторая версия - "Коготь-2", которая продержалась гораздо дольше, т.к. ресурс был зарегистрирован в США. Как утверждают специалисты, т.н. "Когти" оказались репетицией. Скорей всего, политтехнологи проверили, таким образом, эффективность использования Интернета для "раскрутки" скандала.

Наиболее распространенным приемом осуществления политических кибервойн может считаться выброс компромата по средствам специализированных интернет-сайтов. В сети функционируют целые порталы планомерно вбрасываемого компромата. С приближением выборов интернет становится похожим на систему для политических провокаций. Наглядный пример – история про сайты Ю. М. Лужкова в 99-м. В его день рождения - 21 сентября, к группе сайтов, так или иначе связанных с именем Мэра Москвы, добавился ещё один - www.lujkov.ru. По дизайну первой страницы он был почти идентичен личному сайту мэра www.luzhkov.ru. Но содержание для Лужкова было крайне неприятным. Спустя несколько часов после своего появления lujkov.ru был частично закрыт, - он перестал отзываться на свой URL. Через несколько дней после закрытия ответственность за его судьбу взял на себя - Фонд Эффективной Политики (ФЭП). И это далеко не единичный пример.

Незадолго до выборов в Государственную Думу третьего созыва в интернете, помимо официального веб-сайта Г. А. Зюганова www.zyuganov.ru появился “паразитический” сайт www.zuganov.ru, на котором образ лидера российских коммунистов выглядел совсем не престижно. Например, на главной странице сайта Г. А. Зюганов был изображен в бюстгальтере. Сайт содержал ненормативную лексику и пошлые карикатуры на Г.А. Зюганова. После выборов сайт перестал функционировать, очевидно, он был создан противниками КПРФ на предвыборный период с целью дискредитации имиджа руководителя партии.

**Террористы используют информационное оружие**

Существуют в сети и сайты, дискредитирующие не только политику партий или индивидов, но и политику целых государств, осуществляя тем самым информационные атаки не на те или иные политические институты, а на государственный суверенитет. Так, в сети на протяжении нескольких лет существовал сайт чеченских сепаратистов kavkaz.org, открыто выступавший не только против проведения контртеррористической операции в Чеченской Республике, но и призывающий бороться против федеральных властей.

Kavkaz.org неоднократно пытались ломать. В марте 2002 года группа хакеров, скрывающаяся под псевдонимом "Сибирская сетевая бригада", смогла частично ликвидировать сайт. При попытке открыть электронную страницу на экране появлялись сообщения антитеррористической направленности. На следующий день после теракта в ДК на Дубровке пропагандистский сайт был ликвидирован группой российских программистов, но вскоре он опять начал функционировать.

Исходя из мировой практики, создается впечатление, что действия программистов – возможно единственный адекватный ответ на акции сетевых провокаторов. Законодательные меры оказываются неэффективными. В сентябре 2003 года, суд Вильнюса признал незаконными действия литовского Департамента госбезопасности, который в июне 2003 года закрыл сайт «Кавказ-Центр». Тогда создателей интернет-ресурса обвинили в пропаганде терроризма, национальной и религиозной розни. Были проведены обыски в офисе фирмы, которая размещала электронную страницу на своем сервере. Закрыть «Кавказ Центр» требовали от Литвы и Российские власти. Однако уже в конце сентября 2003 года суд Вильнюса вынес решение в пользу создателей сайта.

Другой, не менее интересный пример: в апреле 2003 года руководство Эстонии ответило отказом на требование России запретить одной из коммерческих фирм этой прибалтийской страны сотрудничать с чеченскими террористами. Как сообщала телекомпания НТВ, данная структура предоставляла чеченским экстремистам услуги по размещению интернет-сайта боевиков. По словам эстонского премьер-министра, «сайт находится не на сервере правительства Эстонии, поэтому кабинет в его деятельность вмешиваться не станет, не смотря на то, что Россия требует его закрыть».

13 сентября 2004 года после ряда террористических актов Министерство иностранных дел России вновь потребовало прекращения работы сайта чеченских боевиков «Кавказ-Центр». Для этого в МИД был вызван посол Литвы в России Р. Шидлаускас. Как говорилось в сообщении ведомства, вопрос был поставлен перед ним "в жесткой форме" и 19 сентября власти Литвы временно заблокировали чеченский информационный сайт. Однако вскоре он опять был открыт, но уже в Финляндии, а после очередной ноты протеста российского правительства, вновь был закрыт.

Все чаще террористы берут на себя ответственность через интернет или вывешивают на своих сайтах фотографии жертв, взрывов и даже видеоролики отснятых терактов. Нередко посредством своих ресурсов боевики отчитываются о проделанной работе или обращаются с посланиями к определенной категории граждан. С помощью интернета террористы запугивают общественность, угрожая новыми террористическими атаками.

**Мировая угроза**

В настоящее время во Всемирной сети существует уже несколько сотен экстремистски настроенных информационных ресурсов. Если в 1998 г. примерно половина из 30 организаций, которых США причисляли к террористическим, обладали своими электронными страницами, то ныне в сети представлены абсолютно все известные своими радикальными взглядами группы. Причем материалы они переводят не менее чем на 40 различных языков.

Все более-менее серьезные представители экстремистских организаций располагают не только веб-сайтами, но и форумами, и досками объявлений, где могут пообщаться их сторонники. Террористы из группировки "Хамас", например, создали несколько сайтов, ориентированных на детей. А их «коллеги» из "Хезболлах" пошли еще дальше: ее поклонники могут скачать с сайта группировки видеоигру, сюжет которой - война с израильтянами в Ливане. В сети можно разыскать тексты выступлений Бен-Ладена, книги по идеологии джихада, информацию о проведенных терактах и ознакомиться с лучшими образцами джихадской поэзии.

Как сообщила газета The Washinfton Times за 29 июня 2004 года, наиболее активным пользователем всемирной паутины среди активным пользователем всемирной паутины среди террористов является Абу Мусаб аль-Заркави, возглавляющий ячейку "Аль-Каиды" в Ираке. Он использует сеть интернет для вербовки сторонников и сбора средств на проведения террористических актов, направленных против сил коалиции и нового иракского правительства.

Американцы пытаются оперативно закрывать сайты, на которых "засветился" известный террорист. Однако Аль-Заркави каждый раз ухитряется найти новый способ публиковать во всемирной сети факты своих деяний. Связь через всемирную компьютерную сеть идеально подходит для террористов. По некоторым данным, подготовка к терактам 11 сентября велась именно с помощью обмена зашифрованными посланиями по электронной почте. "Аль-Каида" поддерживает сейчас в Сети порядка 50 различных сайтов. "Интернет - это часть сегодняшнего поля битвы", - утверждает Брайан Дженкинс, специалист по антитеррору в мозговом центре "Рэнд корпорейшн".

Администрации многих стран в меру сил пытаются бороться с проявлением кибертеррора. В конце 2003 года США, впервые внесли в свой список иностранных террористических организаций несколько интернет-сайтов. Согласно американскому законодательству, эти ресурсы теперь вне закона, и запрещена любая материальная поддержка этих сайтов, их сотрудникам запрещен въезд на территорию США, а американские банки должны заморозить их счета. Однако, как сообщило агентство Reuters, даже сам, Госдепартамент пока не понимает, каким образом это будет сделано.

**Государство как гарант безопасности**

Единственный метод, которым можно, с точки зрения официальных лиц, остановить появление террористов-самоучек - это цензура. Нечто подобное после 11 сентября 2001 года практиковали США. Тогда из общего доступа были удалены многие ресурсы, представляющие хоть какую-то ценность для потенциальных террористов. Цензура введена и на территории Китая, где, помимо всего прочего, ограничен доступ к зарубежным СМИ.

Совсем не случайно Ю.М. Лужков опубликовал 16 мая 2004 года в газете «Известия» статью «О темной стороне Интернета». Основной смысл статьи сводился к тому, что необходим специальный закон об Интернете, каким-либо образом регламентирующий распространение информации.

Подобные меры, принимаемые в ряде стран, востребованы, хотя и не всегда являются популярными. Возможно, что с течением времени образуются учреждения, предсказываемые М. Кастельсом, так называемые «on-line полицейские патрули». Первый прототипы подобных организаций появились в августе 2004 во Вьетнаме, там было сформировано специальное полицейское подразделение, в задачи которого входит расследование онлайн-преступлений и слежка за распространением запрещенных публикаций в киберпространстве. Структуры, следящие за содержанием Интернета, безусловно, востребованы уже сегодня.

……………….

1. Именно    телевидение, интернет,   многочисленные печатные издания, активно участвуя в процессах управления жизнью общества, да пожалуй, и государства в целом, играют теперь основную роль в вопросах воспитания, образования, культурного развития, формирования общественно-политических взглядов, духовно-нравственных ценностей и взрослых, и подрастающего поколения.

Информация легковесная, часто недостоверная, современных СМИ стала «продуктом» индустрии сознания россиян. Рейтинговый фактор для большинства СМИ определяющий: чем выше он у той или иной программы или интернет-сайта, тем больше рекламных денег может привлечь. И для привлечения рекламодателей телеканалы, держатели «раскрученных» сайтов более всего озабочены привлечением аудитории любым путём, не заботясь об интересах общества.

Интернет — безконтрольный источник распространения часто негативной, агрессивной информации. Здесь вообще нет никаких сдерживающих центров. Например, ежедневно каждый абонент почтовой программы получает свыше 50 реклам явно деструктивного характера, содержащих информацию с указанием адресов сайтов, где с ней можно ознакомиться более подробно и посмотреть соответствующие «картинки».

Недавно электронными СМИ открыто развёрнута широкомасштабная рекламная кампания по продвижению цифровых наркотиков. Суть её в том, что на коммерческой основе каждому желающему несколькими зарубежными компаниями, серверы которых находятся в США, продают аудиофайлы, слушая которые можно достичь эффекта воздействия на мозг человека марихуаны, героина, LSD. Для этого пользователю, которым может оказаться любой человек и даже ребёнок, нужен обычный компьютер, стереонаушники, набор таких аудиофайлов и программа для их воспроизведения. И — «ловите кайф!» Десятки таких сайтов, устроенных по типу электронных музыкальных библиотек, предлагают выбрать «цифровой наркотик за 20 рублей. В основе его действия — бинауральные волны.

Слушать аудио-допинг надо только в наушниках. Объясню, почему: бинауральные волны — это один и тот же звуковой сигнал, подаваемый в уши человека с разной частотой, — в левое ухо поступает сигнал с частотой 120 Гц, в правое — 125 Гц. Разница между частотами — 5 Гц, и наш мозг вычисляет и воспринимает её автоматически, в виде т. н. бинауральных ритмов. В нормальной ситуации этот механизм служит для определения источника звука, но когда звук подается прямо в уши — через наушники — волны способствуют синхронизации работы обоих полушарий мозга, наблюдаемой в медитативных и гипнотических состояниях сознания.

Согласно экспериментальным данным, накладывая различные бинауральные ритмы друг на друга, можно заставить человека получать определённые ощущения. Бинауральные волны давно используются психотерапевтами и другими врачами, причём не только для лечения психических заболеваний. Однако в публичный доступ аудионаркотики поступили относительно недавно.

Организаторы одного из таких сайтов, рекламирующих цифровые наркотики, утверждают: «Самое главное в принципе действия цифрового наркотика то, что, создав определённый баланс звуковых волн, учёные добились воздействия бинауральных волн на центры удовольствия головного мозга человека, подобного действию реальных наркотиков. Кроме того, цифровой наркотик не вызывает привыкания и абсолютно безвреден. Мало того, он оказывает релаксирующий (расслабляющий) или стимулирующий эффект...».

Правда здесь лишь в том, что написаны цифровые наркотики, действительно, людьми. В иностранных, возможно даже военных, лабораториях... Видимо уже сейчас можно говорить о нейрозвуковом оружии, без стрельбы уничтожающем молодое поколение российских граждан.

Во время Первой мiровой войны многие разведки мра получили секретную информацию о том, что Германия ведёт разработки принципиально нового оружия, которое способно звуком убивать людей, сбивать аэропланы и даже разрушать укрепления противника. Тогда ни одна разведка так и не смогла достать ни опытных образцов, ни чертежей засекреченных немецких разработок. Только к концу 30-х годов удалось доказать, что опыты немцев по созданию звукового оружия идут полным ходом. Позже учёные нацистской Германии, сотни раз испытав звуковое оружие на узниках концентрационных лагерей, придут к выводу, что определённые звуковые волны способны вызывать у человека чувство страха и панику, а некоторые даже могут остановить сердце или разорвать внутренние органы...

В марте 1940 года один из немецких заводов выпустил партию грампластинок с записями одного из популярных английских исполнителей того времени. Все они предназначались для реализации на территории Англии. Интересно, что на каждой из них кроме песен записан не воспринимаемый человеческим ухом инфразвук, который должен был привести слушателей в безотчётный ужас, психическое расстройство, даже к смерти...

В течение месяца эти грампластинки была проданы на территории Англии, но ожидаемого эффекта не последовало. Немецкие учёные просчитались, проигрыватели того времени были технически несовершенны, поэтому не могли воспроизвести инфразвуки, которые должны были убить слушателей.

В апреле 1945 года в немецком городе Хиллерслебене американские военные обнаружили огромное сооружение странной формы, специальная комиссия установила, что там изготовлялось то самое секретное оружие Третьего рейха, работающее на основе звуковых волн.

И теперь уже американские специалисты начали опыты, первые результаты которых были ошеломляющими. Немецкая акустическая установка, если её направляли на предметы, разрывала их в клочья. В определённом режиме она «выдавала» звуковые частоты, которые сбивали дыхание, нарушали работу сердца.

Возможно, что незавершённый проект военных учёных фашистской Германии подтолкнул американцев к собственным исследованиям в этой области. В начале 1960-х NASA провело много опытов воздействия мощного инфразвука на человека. Необходимо было проверить, как повлияет на астронавтов низкочастотный рокот двигателей ракеты? Оказалось, что низкие звуковые частоты (почти от нуля и до 100 герц), а именно в этом диапазоне частот и работают цифровые наркотики, производят колебания грудной клетки, сбивающие дыхание, вызывают головную боль и кашель, искажают визуальное восприятие.

Последующие исследова ния показали, что частота 19 герц — резонансная для глазных яблок, и именно она способна не только вызывать расстройство зрения, но и видения, фантомы. Инженер Вик Тэнди из Ковентри мистифицировал коллег призраком в своей лаборатории. Видения серых проблесков сопровождались у них чувством неловкости.

Наш соотечественник Евгений Переверзев, доктор физико-математических наук, сотрудник кафедры акустического мониторинга и физической акустики МФТИ, подтверждая губительное воздействие цифровых наркотиков на организм человека, говорит: «В диапазоне 7—13 герц звучит природная волна страха, излучаемая тайфунами, землетрясениями и извержениями вулканов и побуждающая всё живое покидать очаги стихийных бедствий. При помощи инфразвука, например, запросто можно довести человека до самоубийства. Главное, чтоб он был в квартире один, а то получится не самоубийство, а массовое помешательство».

Найдутся люди, которые, ознакомившись с моей точкой зрения на цифровые наркотики, заявят о том, что я намеренно сгустил краски. Но судите по плодам: ведь несомненно, что эти самые «доступные, легальные и дешёвые» цифровые наркотики у молодёжи снижают порог чувствительности к наркотикам социальным.

Известный нейрохирург доктор Николас Теодор заявил, что употребление аудионарко-тиков является показателем готовности человека перейти на эксперименты с химическими веществами. Да и безопасность цифрового допинга для мозга не доказана. В интервью телеканалу ТВЦ научный сотрудник Института экспериментальной медицины РАН Дмитрий Мирошников сказал, что эффект от аудионаркотиков, наблюдаемый на электроэнцефалограмме, можно классифицировать как нарушение нормальной работы головного мозга.

Необъявленная война продолжается. Просто знай об этом, когда включаешь ТV или магнитофон. Выбери, на чьей стороне ты воюешь

***. Интернет: бесконтрольный прогресс информационных технологий или веление времени?***

* Значительная роль в воздействии на людей отводится мировой суперсети «Интернет». Сеть активно расширяется. В 2007 г. в России насчитывалось более 5 млн. пользователей, каждый день появляется более 3 млн. новых веб-страниц. В стране в целом 33% населения обладают персональным компьютером, в Москве - более 50%.
* Развитие информационных сетей формирует совершенно новый тип общечеловеческого сознания. Оно начинает функционировать независимо от национальной принадлежности и границ. Вполне возможно, что под влиянием этого сознания изменяется геополитическая карта мира и роль в нем отдельных государств.

Главной задачей психологических операций ранее была деморализация войск и населения противника с помощью пропаганды. Современное понятие информационного противоборства логично укладывается в рамках другого известного понятия - «стратегии непрямых действий». Все более важное место в американской концепции отводится борьбе с терроризмом.

 При наличии огромного количества ядерного оружия этнические конфликты могут превратиться в этноядерные. Дело в том, что экстремистские террористические организации могут использовать в своих целях экстремистски и радикально настроенных работников.

Используется также «искусственная разведка», т.е. математическое моделирование поведения пока только руководителей террористов. В 2002 году в ядерной лаборатории Лос-Аламос вошел в строй суперкомпьютер под кодовым название «Кью» (Q) с быстродействием 30 триллионов вычислений в секунду. В 2005 г. быстродействие превзошло 100 триллионов вычислений в секунду. Вот почему есть надежда обуздания ядерного терроризма средствами «цифровых» технологий.

 Интернет стал одним из главных средств коммуникации для членов «Аль-Каиды». Террористические группы используют веб-сайты, чтобы планировать свои атаки, агитировать за вступление в свои ряды и привлекать средства для финансирования своей деятельности, при этом риск быть схваченным ФБР или другой службой сводится к минимуму.

Большая часть данных на веб-сайтах написана на арабском и зашифрована. Зашифрованная информация помещается в цифровые фотографии, и это делает весьма затруднительным или даже невозможным ее расшифровку.

 Спецслужбы фактически никак не могут помешать террористам пользоваться Интернетом. Не существует законов, которые могли бы позволить закрыть сайты.

Экстремизм в Интернете

Сайт «Кавказ-центр» прославился оперативностью информации о ходе чеченской войны. Захват заложников в Москве 22-25 октября 2002 г. был дан под заголовком «Моджахеды вошли в Москву». Мовсар Бараев, руководитель банды, регулярно связывался с «Кавказом», снабжал журналистов новостей информацией.

Интернет стал идеальным местом и для начинающих террористов. В нем существует масса сайтов, на которых выложена детальная информация о том, как возможно изготовить оружие и взрывчатку из подручных материалов, как их использовать, как связаться с представителями террористических групп и т.д.