**Защита информации в глобальной сети Интернет в системе социально-политических отношений**

ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ В СИСТЕМЕ СОЦИАЛЬНО-ПОЛИТИЧЕСКИХ ОТНОШЕНИЙ

 Интернет находится в настоящее время в какой-то мере вне законодательного регулирования и контроля государственных органов, что порождает различные правонарушения и преступления под действием нескольких факторов, которые существенно влияют на криминогенную обстановку, сложившуюся вокруг Интернета: 1) возможность мошенничества при заключении сделок через Интернет, возможность хищения из виртуальных магазинов, а также создание виртуальных финансовых пирамид; 2) возможность совершения сделок и операций, скрытых от налоговых органов; 3) возможность нарушения авторских и патентных прав, а также использования различных информационных баз правоохранительных и контролирующих органов; 4) возможность совершения преступлений в сфере компьютерной информации (ст. 272 УК РФ - неправомерный доступ к компьютерной информации; ст. 273 УК РФ - создание, использование и распространение вредоносных программ для ЭВМ; ст. 274 УК РФ - нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети). Как известно, чем проще доступ в сеть, тем хуже ее информационная безопасность, поэтому с полным основанием можно сказать, что изначальная простота доступа в Интернет - хуже воровства, так как пользователь может даже и не узнать, что у него были скопированы файлы и программы, не говоря уже о возможности их порчи и корректировки. Что же определяет бурный рост Интернета, характеризующийся ежегодным удвоением числа пользователей? Ответ прост - дешевизна программного обеспечения; легкость и дешевизна доступа в Интернет (либо с помощью IP-адреса, либо с помощью провайдера) и ко всем мировым информационным ресурсам

Платой за пользование Интернетом является всеобщее снижение информационной безопасности, поэтому для предотвращения несанкционированного доступа к своим компьютерам все корпоративные и ведомственные сети, а также предприятия, использующие технологию Intranet, ставят фильтры (fire-wall) между внутренней сетью и Интернетом, что фактически означает выход из единого адресного пространства. Безопасность данных является одной из главных проблем в Интернете. Появляются все новые и новые истории о том, как компьютерные взломщики, использующие все более изощренные приемы, проникают в чужие базы данных. Разумеется, все это не способствует популярности Интернета в деловых кругах. Одна только мысль о том, что какие-нибудь хулиганы или, что еще хуже, конкуренты смогут получить доступ к архивам коммерческих данных, заставляет руководство корпораций отказываться от использования открытых информационных систем. Специалисты утверждают, что подобные опасения безосновательны, так как у компаний, имеющих доступ и к открытым, и к частным сетям, практически равные шансы стать жертвами компьютерного террора. Деятельность террористических групп в киберпространстве началась совсем недавно. В 1998 г. около половины из тридцати террористических организаций, внесенных США в список "Иностранные террористические организации", имели web-сайты, к 2000 г. практически все террористические группы обнаружили свое присутствие в сети Интернет. На данный момент существуют сотни сайтов, обслуживающих террористов и их сторонников. И все же, несмотря на все растущее присутствие террористов в сети Интернет, чиновники, журналисты и ученые при обсуждении комбинации терроризма и Интернета сосредоточились на переоцененной угрозе, называемой кибертерроризмом или кибервойной (атаки на компьютерные сети, включая Интернет). При этом многочисленные случаи ежедневного использования сети Интернет террористами в большинстве своем игнорировались. Терроризм в Интернете - очень динамичное явление, web-сайты внезапно появляются, часто меняют формат, а затем так же стремительно исчезают. Во многих случаях это лишь видимость исчезновения, меняется лишь адрес сайта, содержание остается прежним

Интернет может быть привлекателен для политических экстремистов, но он также символизирует и поддерживает свободу мысли и ее выражения - признак, по которому мы отличаем демократические государства от недемократических. Эффективные контртеррористические кампании не требуют введения драконовских мер по ограничению доступа в Интернет, подобными мерами они могут быть даже подорваны. Как ни парадоксально, децентрализованная сеть связи, созданная американскими спецслужбами для защиты от угрозы со стороны Советского Союза, теперь служит интересам самого большого противника служб безопасности Запада с конца холодной войны: международного терроризма. Начало сети Интернет было положено в ранние 1970-е годы, когда американское министерство обороны было обеспокоено уязвимостью его сетей связи перед ядерной атакой. Министерство решило децентрализовать единую систему путем создания связанных между собой участков компьютерных сетей. После 20 лет развития и использования для научных исследований характер Интернета в конце 1980-х годов быстро начал меняться в результате предоставления доступа коммерческим пользователям. К середине 1990-х годов Интернет соединил более 18 000 частных, общественных и национальных сетей, количество которых постоянно растет. В этих сетях было приблизительно 3,2 миллиона хостов и около 60 миллионов пользователей со всех континентов. Предполагаемое число пользователей в первые годы XXI столетия - более миллиарда человек.

Интернет был провозглашен интегратором культур и средством ведения различных видов коммерческой деятельности, средством связи правительств друг с другом. Казалось, это несет беспрецедентные возможности для создания форума, на котором global village сможет устраивать встречи и обмен идеями, стимулируя и поддерживая демократию во всем мире. Однако с быстрым ростом размера Сети и ее использования утопическому видению многообещающих возможностей Сети были противопоставлены сайты с порнографией и иной вредной информацией и использование Сети различными экстремистскими организациями. Группы, имеющие разные политические цели, но объединенные готовностью использовать террористические тактики, начали использовать Интернет для ведения пропаганды, связи со сторонниками, привлечения общественного внимания к своим действиям, поиска сочувствующих и даже поиска исполнителей своих действий. По своей природе Интернет во многих отношениях - идеальное поле деятельности террористических организаций. Особенно это привлекательно тем, что глобальная сеть предполагает: - свободный доступ; - отсутствие цензуры, других форм государственного контроля; - потенциально огромную аудиторию во всем мире; - анонимность связи; - быстрое движение информации; - невысокую стоимость создания сайта и обслуживания присутствия в сети; - мультимедийную среду: возможность комбинировать текст, графику, аудио и видео, возможность для пользователей загружать фильмы, песни, книги, постеры и т. д.; - возможность охватить также аудиторию традиционных СМИ, которые все чаще используют Интернет как источник сообщений. Указанные преимущества не остались незамеченными террористическими организациями, независимо от их политической ориентации. Интернет привлекает всех: исламистов и марксистов, националистов и сепаратистов, расистов и анархистов. На сегодняшний день почти все активные террористические организации (их больше 40) имеют веб-сайты, а многие поддерживают более одного сайта и используют несколько

Как показывает следующий список, эти организации находятся в разных точках земного шара (отметим, что географическая категоризация иллюстрирует географическое разнообразие, но затеняет тот факт, что многие группы являются в действительности межнациональными и даже трансрегиональными по характеру). - Ближний Восток: "Хамас" (Движение исламского сопротивления), ливанская "Хезболла" (партия Всевышнего), бригады мучеников Аль Аяксы, Фатх, Танзим, "Народный фронт освобождения Палестины", "Палестинский исламский джихад", "Кахане чаи", "Моджахедин-э Кхальк", Рабочая партия Курдистана, турецкая Революционная партия - фронт освобождения народа, "Восточный исламский фронт наступления". - Европа: Ирландская республиканская армия, "Родина и свобода басков", "Корсиканская армия". - Латинская Америка: "Тупак Амару" (Перу), "Сияющий путь", колумбийская "Национальная освободительная армия" и "Революционные вооруженные силы Колумбии". - Азия: "Аль-Каида", "Аум Синрике", "Ансар аль Ислам" в Ираке, японская "Красная армия", "Харакат аль-Муджахиддин", "Тигры освобождения Тамил-Илама", Исламская партия Туркестана - бывшее Исламское движение Узбекистана, "Исламский освободительный фронт" на Филиппинах, пакистанская "Лашкар-э-Тоиба", повстанцы в Чечне. Как правило, сайт содержит информацию об истории организации и ее действиях, детальный обзор ее социальных и политических истоков, отчет о наиболее заметных делах, биографии лидеров, основателей и героев, сведения о политических и идеологических целях, жесткую критику врагов и текущие новости. Националистические и сепаратистские сайты часто демонстрируют карты спорных областей: сайт "Хамас" содержит карту Палестины, РВСК - карту Колумбии, "Тигры освобождения Тамил-Илама" - карту Шри-Ланки и т. д. Несмотря на постоянное употребление слов "вооруженная борьба" и "сопротивление", то, чего создатели сайта не делают, - это детальное описание их насильственных действий. Даже если подробно разъясняется моральное и юридическое обоснование использования насилия, большинство сайтов воздерживаются от описания насильственных действий террористов и их фатальных последствий. Эта немногословность, вероятно, обусловлена пропагандистскими и направленными на создание имиджа целями. Из этого правила есть два исключения: "Хезболла" и "Хамас", на сайтах которых постоянно обновляются отчеты об их действиях ("ежедневные действия") и количестве "мертвых мучеников" и убитых "израильских врагов" и "сотрудников"

Анализ содержания этих сайтов позволяет выделить три группы, на которые направлены данные сайты: 1. Текущие и потенциальные сторонники. Террористические сайты используют лозунги и выставляют на продажу изделия, такие, как значки, футболки, флаги, видеозаписи, аудиокассеты, - вся эта продукция, очевидно, рассчитана на сочувствующих. Часто организация, заинтересованная в локальной поддержке в какой-либо местности, создает сайт на соответствующем языке, располагая на нем детальную информацию о действиях и внутренней политике организации, ее союзниках и врагах. 2. Мнение международного сообщества. На международную аудиторию, непосредственно не вовлеченную в конфликт, но в некоторой степени заинтересованную в проблеме, нацелены сайты на иных, кроме местного, языках. Большинство сайтов имеют версии на нескольких языках. Сайт баскского движения, например, содержит информацию на кастильском (испанском литературном) языке, а также немецком, французском и итальянском. Сайт организации "Тупак Амару" в дополнение к английской и испанской версии предлагает японскую и итальянскую, сайт Исламской партии Туркестана использует арабский, английский и русский языки. Для удобства иностранных посетителей сайты представляют основную информацию об организации с множеством второстепенных исторических обзорных материалов (материалов, с которыми сторонники организации, скорее всего, уже знакомы). Судя по содержанию многих сайтов, в потенциальную аудиторию включены также иностранные журналисты. Для озвучивания позиции организации в традиционных СМИ используются пресс-релизы на сайтах. Детальная второстепенная информация очень полезна для международных корреспондентов. Один из сайтов "Хезболлы" прямо обращается к журналистам, приглашая к сотрудничеству через электронную почту пресс-центра организации. 3. Аудитория "врага". Усилия по достижению аудитории "врага" (т. е. граждан государств, против которых борются террористы) не столь очевидно вытекают из содержания многих сайтов. Однако некоторые сайты, как кажется, направляют усилия на деморализацию противника, угрожая нападением и создавая чувство вины за мотивы и поведение неприятеля. Они также стремятся стимулировать общественные дебаты в государствах-врагах, повлиять на общественное мнение и ослабить поддержку обществом существующего режима. Мы выделили отдельные способы использования сети Интернет террористами. Некоторые из них похожи на те, которые использует каждый пользователь, - например, сбор информации. Другие напоминают использование средств популяризации традиционными политическими организациями - например, сбор средств и пропаганда. Третьи намного более необычны - например, отправка инструкций в закодированных сообщениях или зашифрованных файлах. Терроризм часто называют одной из форм психологической войны, и, конечно, террористы стремятся вести такую кампанию через Интернет. Для этого у террористов есть несколько путей. Например, они могут использовать Интернет для дезинформации, распространения угроз, направленных на то, чтобы посеять страх и ощущение беспомощности, распространять ужасающие изображения своих действий, как, например, видеозапись убийства американского журналиста Дэниэла Перла лицами, захватившими его в плен, которая распространялась через несколько веб-сайтов. Террористы могут также начать психологические атаки посредством кибертерроризма, а точнее, создания опасений угрозы совершения таких действий. Киберстрах возникает из беспокойства об угрозе компьютерных нападений (например, падения самолетов, вывода из строя систем управления воздушным движением, сбоев в системе национальной экономики путем нарушения компьютерных систем, регулирующих фондовые биржи, и т. п.), которое усиливается настолько, что общество начинает верить, что атака случится. Интернет - среда, не подверженная цензуре, которая распространяет информацию, изображения, угрозы или сообщения независимо от их законности или потенциального воздействия, - это идеально подходит даже небольшой группе лиц, чтобы усилить воздействие от передаваемой ею информации и преувеличить опасность угрозы, которую сведения несут

"Аль-Каида" комбинирует мультимедиапропаганду и передовые технологии связи, чтобы создать сложную модель ведения психологической войны. Усама бен Ладен и его последователи концентрируют усилия на пропаганде в Интернете, где посетители многочисленных сайтов "Аль-Каиды" и сайтов "сочувствующих" незапрещенных организаций могут получить доступ к аудио - и видеозаписям, фотографиям и объявлениям. Несмотря на постоянные преследования, которым в последние годы подверглась эта организация: аресты и смерть многих членов, разрушение ее операционных баз и тренировочных лагерей в Афганистане, "Аль-Каида" способна провести кампанию по внушению паники. С 11 сентября 2001 г. организация последовательно размещала на своих сайтах сообщения о планировании "большого нападения" на цели в Америке. Эти предупреждения получили широкое распространение в печати, что помогало сеять чувство страха и незащищенности во всем мире, и особенно в США

Интересно, что "Аль-Каида" последовательно утверждала на веб-сайтах, что разрушение Всемирного торгового центра причинило американской экономике не только конкретный экономический, но и "психологический" ущерб. Атака на башни-близнецы изображается как нападение на символ американской экономики, и доказательства этого видятся в ослаблении доллара, спаде после 11 сентября 2001 г. на американской фондовой бирже и предполагаемой потере веры в американскую экономику не только в пределах США, но и во всем мире. Проводятся параллели с развалом СССР. Одна из последних публикаций бен Ладена, распространенная в глобальной сети, объявляет, что "Америка отступает перед Святостью Всемогущего и ее экономическое истощение продолжается по сей день. Но требуются дальнейшие удары. Молодежь должна искать уязвимые места в американской экономике и атаковать эти узлы врага". Интернет значительно расширил возможности террористов по преданию гласности их деятельности. До появления Интернета надежды террористов на огласку их действий зависели от привлечения внимания телевидения, радио или печатных СМИ. Эти традиционные СМИ имеют многоступенчатую систему редакционного отбора, в результате террористы могут не достичь своей цели и потерять время. И конечно, подобных препятствий не существует на собственных веб-сайтах террористов. То, что многие террористические организации имеют непосредственный контроль над содержанием своих сообщений, предлагает возможности для подачи информации таким образом, чтобы с ее помощью манипулировать различными группами потенциальной аудитории. Террористические сайты в большинстве своем не восславляют свои насильственные действия. Вместо этого независимо от программы террористов, мотивов и местоположения большинство из них подчеркивают две проблемы: ограничения на свободу выражения своего мнения и тяжелое положение товарищей, являющихся политическими заключенными. Эти проблемы находят мощный отклик среди их сторонников и рассчитаны на то, чтобы вызвать симпатию у западной аудитории, лелеющей свободу выражения мнений и неодобрительно относящейся к действиям, направленным на то, чтобы заставить замолчать политическую оппозицию. Аудитория противника также может быть целью этих жалоб, поскольку террористы, подчеркивая антидемократический характер предпринимаемых против них действий, пытаются создать чувство неловкости и стыда в среде противника. Выражения протестов запрещенных террористических групп особенный эффект имеют в Интернете, который для многих пользователей является символом независимых, свободных, неподцензурных

Террористические сайты обычно используют три риторические конструкции для оправдания необходимости использования насилия. Первая: заявление о том, что террористы не имеют никакого выбора, кроме как обратиться к насилию. Насилие представляется потребностью, навязанной слабому как единственное средство ответа применяющему репрессии врагу. В то время как сайты забывают упомянуть о том, как террористы преследуют людей, силовые акции государства или режима, преследующего террористов, постоянно подчеркиваются и освещаются с такими характеристиками, как "кровопролитие", "убийство", "геноцид". Террористическая организация изображается как постоянно преследуемая: ее лидеры подвергаются попыткам убийства, последователи избиваются, свобода выражения ограничена, последователи арестовываются. Эта тактика, изображающая организацию маленькой, слабой и преследуемой мощью сильного государства, превращает террористов в слабую сторону. Вторая риторическая конструкция, связанная с оправданием применения насилия, - демонизация и делегитимизация врага. Члены движения или организации представляются борцами за свободу, использующими насилие против их желания, потому что безжалостный враг ущемляет права и достоинство людей. Враг движения или организации - настоящий террорист, множество сайтов настаивают: "Наше насилие ничтожно по сравнению с его агрессией". Это наиболее общий аргумент. Террористическая риторика перекладывает ответственность за насилие с террористов на противника, который обвиняется в демонстрации зверства, жестокости и безнравственности. Третий риторический прием - многочисленные заявления о ненасильственных действиях в противопоставление сложившемуся образу террористов. Несмотря на то что они являются сильными организациями, многие сайты утверждают, что их группы находятся в поиске мирных решений, что их окончательной целью является дипломатическое урегулирование, достигаемое посредством переговоров и международного давления на репрессивное правительство. Интернет можно рассматривать как огромную цифровую библиотеку. Всемирная паутина предлагает около миллиарда страниц информации, большей частью находящихся в свободном доступе, и многие из них представляют интерес для террористических организаций. Из Интернета террористы могут получать детальную информацию о целях - например, о транспортной инфраструктуре, атомных электростанциях, общественных зданиях, аэропортах, портах, и даже информацию о контртеррористических мерах. Известно, что ячейки "Аль-Каиды" сейчас работают с помощью больших баз данных, содержащих детальную информацию о потенциальных целях в США. Они используют Интернет, чтобы собрать сведения о мишенях, особенно критических экономических точках, а современное программное обеспечение позволяет им изучить структурные слабости в средствах обслуживания, так же как предсказать эффект от нападения на некоторые системы. Согласно докладу министра обороны США Д. Рамсфельда от 15 января 2003 г. пособие "Аль-Каиды", найденное в Афганистане, говорит читателям: "Используя общественные источники открыто без применения незаконных средств, можно собрать о враге как минимум 80% требуемой информации"

Веб-сайт, управляемый Мусульманским клубом хакеров (организация, целью которой, по мнению американских спецслужб, является разработка программного обеспечения для дальнейшего осуществления кибернападений), опубликовал ссылки на сайты, раскрывающие такую информацию, как кодовые названия или радиочастоты, используемые американскими разведслужбами. Тот же сайт предлагает программы, обучающие созданию и распространению вирусов, разработке хакерских стратегий, компьютерному саботажу, шифровке, а также дает ссылки на другие сайты исламских и иных террористических организаций. Цели, обсуждаемые на сайтах "Аль-Каиды" и родственных ей сайтах, центры контроля и предупреждения болезней в Атланте, система перевода фондов федерального резерва, средства обслуживания, управляющие потоком информации в Интернете. Как и многие другие пользователи Интернета, террористы имеют доступ не только к картам и схемам потенциальных целей, но и к данным относительно контртеррористических мер, принимаемых в этих целях. Один из обнаруженных компьютеров "Аль-Каиды" содержал информацию о проектных и структурных особенностях дамбы, полученную в Интернете и позволяющую инженерам "Аль-Каиды" моделировать последствия атаки. В других захваченных компьютерах американские исследователи нашли доказательства того, что операторы "Аль-Каиды" заходили на сайты, предлагающие программное обеспечение и инструкции по программированию электронных коммутаторов, управляющих энергией, водой, транспортом и сетевыми коммуникациями. Для сбора таких данных доступно множество инструментов, включая поисковые серверы, почтовые списки рассылки, чаты и форумы. Множество сайтов предлагают собственные инструменты поиска содержащейся в их базах данных информации. Изучение электронных версий газет и журналов также может дать террористам информацию для дальнейшего использования. Часть этой информации может быть доступна и в традиционных СМИ, но возможности электронного поиска позволяют террористам получать информацию анонимно и с очень небольшими усилиями и расходами. Как и другие политические организации, террористические группы используют Интернет для пополнения фондов. "Аль-Каида", например, всегда очень зависела от пожертвований, и ее глобальная сеть сбора денег построена, как и сети неправительственных организаций, благотворительных фондов и других финансовых учреждений, которые используют сайты, чаты и форумы. Суннитская группа экстремистов "Хизбут-Тахрир" использует взаимосвязанную сеть сайтов в различных странах - от Европы до Африки, на которых размещаются просьбы к сторонникам помочь усилиям джихада посредством пожертвования денег. Банковская информация, включающая номера счетов, на которые могут переводиться пожертвования, размещена на немецком сайте. Чеченские боевики также используют Интернет для информирования о банковских счетах, на которые сочувствующие могут перевести средства (один из этих счетов открыт в банке, расположенном в г. Сакраменто, штат Калифорния). Веб-сайт ИРА имеет страницу, на которой посетители могут делать пожертвования с помощью кредитных карт

Демографические данные интернет-пользователей (получаемые, например, из личной информации, введенной в онлайн-анкету или бланк заявки) позволяют террористам идентифицировать отношение аудитории к той или иной проблеме. Индивидуумов, сочувствующих террористам, после этого могут попросить о пожертвованиях посредством адресных рассылок по электронной почте, посланной от имени "фронт-групп", т. е. организаций, благосклонных к террористам, но действующих публично и легально и не имеющих никаких прямых связей с террористической организацией. Например, денежные средства для "Хамас" были собраны через веб-сайт основанного в Техасе Фонда милосердия. Американское правительство конфисковало активы этого фонда в декабре 2001 г. из-за его связей с "Хамас". Правительство США также заморозило активы трех с виду законных благотворительных организаций, которые использовали Интернет для сбора денег в пользу "Аль-Каиды". В январе 2004 г. федеральный суд присяжных в штате Айдахо признал саудовского аспиранта виновным в организации через Интернет заговора с целью оказания помощи террористическим организациям, в организации джихада путем сбора средств, вербовки новичков, определения местонахождения предполагаемых целей - американских вооруженных сил и гражданских лиц на Ближнем Востоке. Сами Омар Уссайен, соискатель докторской степени в университете штата Айдахо, по иронии спонсируемый Агентством национальной безопасности, был обвинен в создании веб-сайтов и почтовых рассылок, распространяющих сообщения от его имени и от имени двух радикальных клерикалов в Саудовской Аравии, поддерживающих джихад. Интернет может использоваться не только для просьб о пожертвованиях от сочувствующих, но также и для вербовки и мобилизации сторонников, играющих более активную роль в поддержке террористических действий. В дополнение к таким средствам поиска новобранцев, как технологии веб-сайта (звук, видео и т. п.), террористические организации собирают информацию о пользователях, просматривающих их сайты. С пользователями, которые кажутся наиболее заинтересованными в деятельности организации или хорошо подходящими для выполнения ее работы, входят в контакт. Вербовщики могут также использовать больше онлайн-технологий - перемещаться по чатам и форумам в поиске наиболее восприимчивых членов аудитории, особенно молодых людей. Электронные конференции, пользовательские сети (дискуссии по определенным проблемам) могут также служить средством для обращения к потенциальным новичкам

Можно отметить, что некоторые потенциальные новички сами используют Интернет для рекламирования себя террористическим организациям. Некто Зияд Халил, специализирующийся на изучении информатики в колледже Колумбия в штате Миссури, стал в кампусе мусульманским активистом и развивал связи с несколькими радикальными группами, создав сайт в поддержку "Хамас". Вследствие своих активных действий в сети Интернет он привлек внимание бен Ладена и его помощников. Халил стал офицером снабжения "Аль-Каиды" в США, занимался закупками спутниковых телефонов, компьютеров и других электронных средств наблюдения, помогая бен Ладену связываться с его последователями и агентами. Однако более типично для террористических организаций искать новичков вместо того, чтобы ждать, когда они представятся сами. Институт SITE в Вашингтоне, округ Колумбия, проводивший мониторинг интернет-коммуникаций "Аль-Каиды", обнаружил пугающие данные о высокотехнологичной вербовке, стартовавшей в 2003 г., чтобы рекрутировать бойцов для поездки в Ирак и последующего нападения там на силы США и коалиции. Потенциальные новички были засыпаны религиозными декретами и антиамериканской пропагандой, обучающими руководствами о том, как стать террористом "Аль-Каиды", а в секретных чатах они получали детальные инструкции о том, как совершить поездку в Ирак. В одном из типичных обменов сообщениями в секретном чате "Аль-Каиды" в начале сентября 2003 г. неизвестный исламский фанатик под именем "Искупление близко" пишет: "Братья, как мне поехать в Ирак для джихада? Есть ли там армейские лагеря или кто-то, кто там командует?" Четыре дня спустя он получает ответ от "Беспощадного террориста": "Дорогой брат, дорога для Вас там открыта, там много групп, ищите того, кому будете доверять, присоединяйтесь к нему, он будет защитником Ирака, и с помощью Аллаха Вы станете одним из воинов". "Искупление близко" начинает настаивать на получении более определенной информации относительно того, как он может совершить джихад в Ираке. "Беспощадный террорист" посылает ему видеоролики с пропагандой и инструктирует его по загрузке программного обеспечения "Pal Talk", позволяющего пользователям разговаривать в Интернете без опасения прослушивания. Многие террористические веб-сайты резко остановили вербовку новичков для совершения насильственных действий, но они поощряют новичков на иные действия поддержки. "Как я могу помочь борьбе: несколько предложений" - провозглашает заголовок на сайте "Кахане чаи". "Боевая готовность: что Вы можете сделать" - заголовок на сайте "Сендеро Люминосо". Возможности Интерне та по мобилизации активистов были проиллюстрированы ответом на арест лидера Рабочей партии Курдистана Оджалана. Когда турецкие власти арестовали его, десятки тысяч курдов во всем мире ответили демонстрациями в пределах считанных часов вследствие работы сочувствующих сайтов, убеждавших сторонников дать ответ

Многие террористические группы, среди которых "Хамас" и "Аль-Каида", подверглись преобразованию из строго иерархических организаций с определенными лидерами в сети из полуавтономных ячеек, не имеющих четко определенной иерархии. С помощью Интернета эти свободные независимые группы имеют возможность поддержания контакта друг с другом и с другими террористическими организациями. В будущем террористические организации, вероятно, будут еще более децентрализованными, состоящими из множества интернациональных групп, поддерживающих связь через Интернет и имеющих горизонтальную, а не вертикальную структуру. Современные коммуникационные технологии, особенно компьютерные, являются средством создания сетей и поддержания террористических сетей по нескольким причинам. Во-первых, новые технологии сильно сократили время передачи, позволяя рассеивать местонахождение действующих лиц, при этом есть возможность быстрой связи и эффективного координирования. Во-вторых, новые технологии значительно уменьшили стоимость связи. В-третьих, объединяя компьютеры с коммуникациями, террористы существенно повысили многообразие и сложность передаваемой информации. Интернет соединяет не только членов одной террористической организации, но также членов различных групп. Например, существует много сайтов, выражающих поддержку джихаду. Эти сайты и связанные с ними форумы позволяют террористам в различных местах типа Чечни, Палестины, Индонезии, Афганистана, Турции, Ирака, Малайзии, Филиппин, Ливана обмениваться не только идеями и предложениями, но также и практической информацией о том, как изготавливать взрывчатые вещества, создавать террористические ячейки, выполнять атаки. Всемирная паутина является домом многих сайтов, содержащих информацию о создании химического оружия и взрывчатых веществ. На многих из этих сайтов размещены книги "Руководство террориста" и "Поваренная книга анархиста", два известных учебника, посвященных детальному описанию создания различных видов взрывных устройств. Другое пособие - "Руководство моджахеда по ядам", написанное Абдель Азизом в 1996 г., "издано" на официальном сайте "Хамаса". На двадцати трех страницах оно детально рассказывает, как подготовить самодельные яды, ядовитые газы и другие смертоносные материалы для применения в террористических атаках. Намного большее по объему руководство под названием "Энциклопедия джихада", подготовленное "Аль-Каидой", - в нем более тысячи страниц, разбросанных по всей сети, - предлагает детальные инструкции по созданию подпольной организации и проведению атаки. Найденный в Афганистане ноутбук "Аль-Каиды" использовался для многократного посещения французского сайта "Анонимного сообщества", на котором было размещено "Руководство по саботажу" с такими разделами, как планирование убийства и методы избежания слежки. Эта информация используется не только террористическими организациями, но также разочаровавшимися индивидуумами, готовыми использовать террористическую тактику для выражения своих намерений. Например, в 1999 г. молодой человек по имени Дэвид Копелэнд установил самодельные бомбы в трех местах Лондона: многонациональном Брикстоне, в бангладешской общине в Брик Лэйне и в гей-части Сохо. В течение трех недель погибли 3 человека и были ранены 139. На судебном разбирательстве он заявил, что информацию о методах убийств людей почерпнул в Интернете из книг "Руководство террориста" и "Как делать бомбы: Книга 2". Оба названия легко доступны. Поиск в Google по ключевым словам "террорист" и "руководство" нашел почти четыре тысячи совпадений, включающих ссылки на пособия и руководства. Один из сайтов дает рекомендации о том, как приобрести взрывчатое вещество нитрат аммония. В 2002 г. в Финляндии блестящий студент-химик, называющий себя "RC", обсуждал методы изготовления бомб с другими энтузиастами на финском веб-сайте, посвященном взрывчатым веществам и взрывным устройствам. Иногда он задавал вопросы по таким темам, как производство нервно-паралитического газа в домашних условиях. Иногда он обменивался информацией с модератором сайта, все сообщения которого имели картинку: изображение его собственного лица на теле Осамы бен Ладена, в тюрбане и с бородой. Затем RC взрывает бомбу, убившую семь человек, в том числе и его, в переполненном торговом центре. Веб-сайт, часто посещаемый RC, известный как форум по домашней химии, был закрыт спонсором - компьютерным журналом. Но резервная копия, предназначенная только для чтения, была тут же вновь размещена в Сети. Террористы используют Интернет не только для того, чтобы узнать, как создавать взрывные устройства, но и для того, чтобы планировать и координировать определенные нападения. Активисты "Аль-Каиды" в большой степени использовали Интернет в планировании и координировании нападения 11 сентября. Тысячи зашифрованных сообщений в защищенной паролем части сайта были найдены позднее на компьютере арестованного террориста "Аль-Каиды" Абу Забейда, который, по сообщениям, был одним из руководителей нападавших. Первые сообщения, найденные на компьютере Забейда, были датированы маем 2001 г., последние - 9 сентября 2001-го. Наиболее высокая частота сообщений была в августе. Чтобы сохранить анонимность, террористы "Аль-Каиды" использовали Интернет в общественных местах доступа и посылали сообщения через публичную электронную почту. Некоторые угонщики самолетов поддерживали связь посредством почтовых аккаунтов на бесплатной почте. Активисты "Хамаса" на Ближнем Востоке используют чат-румы для планирования действий и электронную почту для обмена информацией между сектором Газа, западным берегом реки Иордан, Ливаном и Израилем. Инструкции в форме карт, фотографий, руководств, технических инструкций по использованию взрывчатых веществ маскируются посредством стенографии, сообщения скрываются внутри графических файлов. Однако иногда инструкции поступают в зашифрованном самыми простыми шифрами виде. Последнее послание Мохаммеда Атты восемнадцати террористам, участвующим в атаке 11 сентября, гласит: "Семестр начинается через три недели. Мы получили 19 подтверждений с факультета права, факультета градостроительного проектирования, факультета искусств, инженерного факультета (упоминание о факультетах, очевидно, было шифром для обозначения целей атак)"

На брифинге в конце сентября 2001 г. Рональд Дик, помощник главы ФБР, сообщил журналистам, что террористы 11 сентября использовали Интернет, и "использовали успешно". С тех пор они только совершенствуют свои навыки и увеличивают свое присутствие в глобальной сети. Сегодня террористы различных идеологических течений - исламисты, марксисты, националисты, сепаратисты, расисты - получили много уроков максимального использования Интернета. Большие достоинства Интернета - легкость доступа, минимум регулирования, огромная потенциальная аудитория, быстрый поток информации и пр. - были поставлены на службу группами, использующими для достижения своих целей террористические методы. Анализ приведенных фактов позволяет сделать следующие выводы. Сегодня необходимо стать более информированными о способах использования террористами Интернета и более приспособленными для контроля за их действиями. Журналистов, ученых, высших должностных лиц и даже правоохранительные органы до недавнего времени больше интересовала проблема кибертерроризма, являющаяся преувеличенной угрозой, из-за чего недостаточное внимание уделялось обычному использованию террористами Интернета. Эти случаи использования многочисленны и, с точки зрения террористов, неоценимы. Следовательно, всем субъектам противодействия терроризму необходимо продолжить изучение и контроль террористических действий в Интернете, а также поиск мер по ограничению использования этой среды современными террористами. В то же время в процессе защиты нашего общества от терроризма мы не должны разрушать те его качества и ценности, которые защищаем. Интернет является почти воплощением демократических идеалов свободы слова и связи. Это рынок идей, какого раньше не было. К сожалению, свобода, предлагаемая Интернетом, уязвима с точки зрения злоупотреблений со стороны групп, которые, как это ни парадоксально, зачастую сами враждебны к выражениям мысли, не прошедшим цензуру. Но если, напуганные угрозой терроризма, мы ограничим нашу собственную свободу использования Интернета, мы поможем террористам нанести удар по демократии.