Д.Г. Гаев

Электронный концлагерь

Ил. 1. «Прекратите нас прослушивать!»

Побег, ставший мировой сенсацией

Сейчас имя Эдварда Сноудена узнал весь мир. А до 2013 года оно не было известно никому, кроме его родных, знакомых — и узкого круга его непосредственных шефов из американских разведывательных ведомств. Последние, безусловно, много дали бы за то, чтобы Эдвард так и не стал никогда мировой знаменитостью. Но судьба распорядилась иначе.

Эдвард Сноуден (родившийся в 1983 году в непримечательном городке Элизабет-Сити, штат Северная Каролина) никогда не планировал становиться разоблачителем или диссидентом. Напротив, хорошо известно, что он даже пытался поучаствовать во второй иракской войне, чтобы, по его собственным словам, «бороться за права угнетенных народов». Однако перелом ног во время учений быстро поставил крест на его военной карьере. Как опытный специалист в IT-сфере, Сноуден решил строить свою карьеру в этой области. Работая сперва непосредственно в Агентстве национальной безопасности, а потом в формально гражданской (но имеющей весьма тесные связи с американской разведкой) компании “*Booz Allen Hamilton*”, — Сноуден увидел и узнал многое из того, что сильно повлияло на его мировоззрение. По-видимому, изнанка деятельности американских спецслужб оказалась совсем не такой романтичной, как ему ранее представлялось.

В начале 2013 года он окончательно решил рассказать прессе о том, что ему было известно, и связался с двумя известными журналистами: Гленном Гринвальдом (газета «Гардиан») и Бартоном Геллманом (газета «Вашингтон Пост»). Он переслал им ряд совершенно секретных материалов (например, закрытую электронную презентацию

возможностей программы **PRISM** — о ней подробнее впереди). В сопроводительной записке к первой партии документов Сноуден написал: «Я понимаю, что мне придётся страдать за свои поступки», но «я буду удовлетворён, если секретные законы, неравная безнаказанность и непреодолимая исполнительная власть, правящая тем миром, который я люблю, будут раскрыты хотя бы на мгновение...»

Ил. 2.

Хотя Сноуден принимал очень серьезные меры для защиты безопасности своей электронной переписки, он (как, вероятно, никто иной на нашей планете) еще лучше осознавал и возможности, которые американская разведка может задействовать для выслеживания ренегата. Поэтому еще до того, как в американской и британской прессе появились первые публикации о программе PRISM, он успел покинуть США. И когда в июне 2013 года рассекреченные им материалы увидели свет, он уже находился в Гонконге, в относительной безопасности (где, уже 9 июня, он дал свою первую открытую пресс-конференцию). Американские власти наблюдали за всем происходящим с плохо скрытой злобой — и ответили в весьма характерном для них стиле, специально приурочив предъявление Сноудену официальных обвинений (в «похищении государственной собственности» и в «разглашении государственной тайны») точно ко дню его 30-летия. Китайские власти выдавать его отказались — но и предоставлять ему политическое убежище тоже совсем не торопились. Поэтому 23 июня Сноуден перелетел в Москву, а 30 июня он обратился к российским властям с просьбой о политическом убежище. Ровно через месяц, 1 августа, он его получил, официально став политическим беженцем.

Почему же разоблачения Сноудена вызвали в мире такой шок? Как представляется, одним из факторов стало то, что они разрушили любимый миф многих: миф о свободном (и неподконтрольном кому-либо) Интернете. Парадоксальность ситуации многим виделась в том, что именно США когда-то создали глобальную (и неподцензурную) компьютерную сеть. Вместе с тем, как сейчас выяснилось, именно они и приложили огромные усилия, чтобы превратить Интернет в инструмент глобальной слежки! Причем, если про слежку за электронными коммуникациями (например, про систему «Echelon») было, в общем, известно и ранее; если тотальная поднадзорность линий телефонной связи (например, сотовой сети)

тоже, в общем, не была секретом — то Интернет, в силу традиции, всегда считался своеобразной «территорией свободы». Разоблачения Сноудена оказались болезненными в том числе и потому, что стали сильнейшим ударом по этому мифу. Тем более что многие помнят, как еще относительно недавно «свободный Интернет» все-таки был не мифом, а реальностью...

На заре Интернет-эпохи

Говорится совсем не в упрек, но сегодня многие имеют довольно туманное представление о «корнях» Интернета. Среди молодых пользователей Сети популярно убеждение, что Интернет появился если не во времена планшетных компьютеров и лэптопов, то, по крайней мере, во времена персональных компьютеров класса IBM PC. А «честь создания» Интернета приписывается если не Биллу Гейтсу, то Стивену Джобсу. При этом, узнав, что люди активно пользовались Интернетом как минимум десятилетием раньше, многие искренне удивляются. Между тем, даже само название «Internet» (если переводить дословно — «Межсеть») наводит на некоторые мысли. Ведь если вдруг появилась «Межсеть», значит, какие-то сети существовали и до этого?

Да, существовали. Интернет тоже возник не в полном вакууме, а как объединение группы научных, образовательных и коммерческих сетей, существовавших до этого. Впрочем, судьба ранних американских сетей оказалась разной: некоторые полностью влились в Интернет, некоторые вымерли как динозавры, а какие-то даже продолжают выживать параллельно (в какой-то степени, наперекор) Интернету.

Вот несколько наиболее примечательных компьютерных сетей («онлайн-сервисов») времен «до Интернета»:

- **AOL** (*America Online*, http://en.wikipedia.org/wiki/America_Online) в начале 1980-х выросла из небольшого и малозаметного предприятия под названием Control Video Corporation, специализировавшегося в основном на онлайн-доступе к видеоиграм. Превратилась в развитую компьютерную сеть, предоставлявшую пользователям широкий диапазон услуг: электронную почту, доступ к конференциям Usenet, свои собственные средства чатов/телеконференций. В настоящее время эта сеть «влилась» в Интернет (а AOL/TimeWarner – это мощный медиа-конгломерат, интересы которого вышли далеко за рамки компьютеров и сетей).

- **BITNET** (*Because It's Time Network*, http://en.wikipedia.org/wiki/Bitnet) – сеть изначально не коммерческая, а университетская (в 1981 году, объединила Нью-Йоркский и Йельский университеты, несколько позднее к ней присоединились другие образовательные учреждения, число которых к 1991 году достигло примерно пятисот). Действовала (как и Фидонет) довольно медленно и предоставляла пользователям такие базовые услуги, как

электронная почта, списки автоматической рассылки (LISTSERV), возможность файлообмена и (позднее) шлюзы в «большой» Интернет. Прекратила существовать как единое целое в 1996 году (хотя отдельные сегменты действовали и после).

- **CompuServe** (**CIS**, http://en.wikipedia.org/wiki/Compuserve) — одна из самых древних компьютерных сетей США: ее история отсчитывается с 1969 года! Вначале пользователи сети не имели даже нормальных регистрационных имен, представляясь системе номерами вида 71234, 567. Несмотря на это, ее популярность даже перешагнула границы США, достигнув Англии, Германии и Японии. Основными услугами были: электронная почта, собственные дискуссионные форумы и электронные доски объявлений (BBS), возможность обмениваться файлами, службы новостей и системы онлайн-торговли. Оригинальная сеть (**CompuServe Classic**) официально закрылась только 1 июля 2009 года (впрочем, **CompuServe 2000** работает до сих пор). Кстати, к наследию CompuServe относится и известный всем интернет-пользователям GIF-формат графических файлов.

- **Delphi Forums** (http://en.wikipedia.org/wiki/Delphi_%28online_service%29) — система дискуссионных онлайн-форумов на разнообразные темы, доступных пользователям через модемное подключение. В среде Интернета они существуют и сегодня (http://www.delphiforums.com/).

- **GEnie** (http://en.wikipedia.org/wiki/GEnie) — компьютерная сеть, созданная в 1985 году американским электронным гигантом **General Electric**. Помимо стандартных услуг (например, электронной почты), включала в себя популярные круглые столы (round tables), посвященные определенной тематике (от текущей политики до астрологии). Каждый круглый стол включал в себя форум, интерактивный чат и даже локальную библиотеку (т. е. файловое хранилище). К сожалению, с наступлением Интернета популярность GEnie стала падать. Датой окончательного закрытия сети считают 27 декабря 1999 года.

- **Prodigy** (http://en.wikipedia.org/wiki/Prodigy_%28online_service%29) существует с 1984 года. Создана как совместное предприятие IBM и американского гиганта розничной торговли Sears. Понятно, что коммерческая составляющая в проекте присутствовала с самого начала — но, помимо этого, имелись и электронная почта, и интересные дискуссионные форумы. Кстати, это была одна из первых сетей, реализовавших графический интерфейс для пользовательского доступа (за годы до первых web-страниц)! В настоящее время существует как Интернет-провайдер.

- **FidoNet** — полностью любительская компьютерная сеть, основанная в 1984 году и поддерживаемая самими пользователями Томом Дженнингсом и Джоном Мэдилом. («*Культура в современном мире*» уже подробно рассказывала о FidoNet в материале «*Из истории компьютерного андеграунда: эпоха BBS и Фидонет*», № 2011/03). Будучи

относительно медленной и лишенной средств общения в реальном времени (так как компьютеры сети Фидо обмениваются информацией лишь в выделенные «почтовые часы»), для очень многих пользователей Фидонет все-таки стал технологией прорыва и первым средством для общения друг с другом. Основные услуги Фидо — автоматическая передача электронной почты («нетмейл»), дискуссионные форумы («эхо-конференции») и удаленная пересылка запрашиваемых файлов («файл-реквесты»). Сама сеть состоит из поддерживаемых пользователями пронумерованных узлов (так наз. «нодов» и «хабов»), иерархия которых также определяется самим пользователями. Поэтому централизованное «начальство» у Фидонет отсутствует по определению: имеется лишь ряд документов, регламентирующих общепризнанную сетевую политику. Сеть Фидонет — международное явление, имеющее культовый статус в т.ч. и в нашей стране. И хотя пиком популярность Фидонет считается 1995 год, определенная активность в нем наблюдается даже сегодня.

Этот обзор был бы неполным без упоминания о UUCP (Unix-to-Unix Copy) — первой системе протоколов и технологий межкомпьютерной передачи данных. Будучи неким аналогом Фидонет для «больших» компьютеров (то есть обеспечивая относительно медленный и принципиально неинтерактивный обмен данными), именно технологии UUCP впервые подарили сотням пользователей и электронную почту, и телеконференции Usenet.

В завершение отметим некоторые общие проблемы «архаических» сетей:

1) взаимная *несовместимость*. Какие бы развитые информационные ресурсы каждая из этих сетей ни предоставляла *собственным* пользователям, для *чужих* пользователей эти ресурсы обычно будут недоступными (или, в лучшем случае, доступными с большим трудом). Даже пересылка простого почтового сообщения от пользователя одной сети пользователю другой может оказаться невозможной.

2) подверженность *устареванию* (как физическому, так и моральному). Средства, которые были удобны для начала 1980-х годов, быстро перестали устраивать пользователей 1990-х. Модернизации требовали не только сами сети, но и базовые принципы взаимодействия пользователей с ними: например, с начала 1990-х стали активно употребляться графические интерфейсы. А учитывая то, что программное обеспечение требовалось для всех популярных платформ (IBM PC, Apple Macintosh, разнообразные рабочие станции), его поддержка (и тем более дальнейшее развитие) даже для крупных компаний становилась неподъемной задачей.

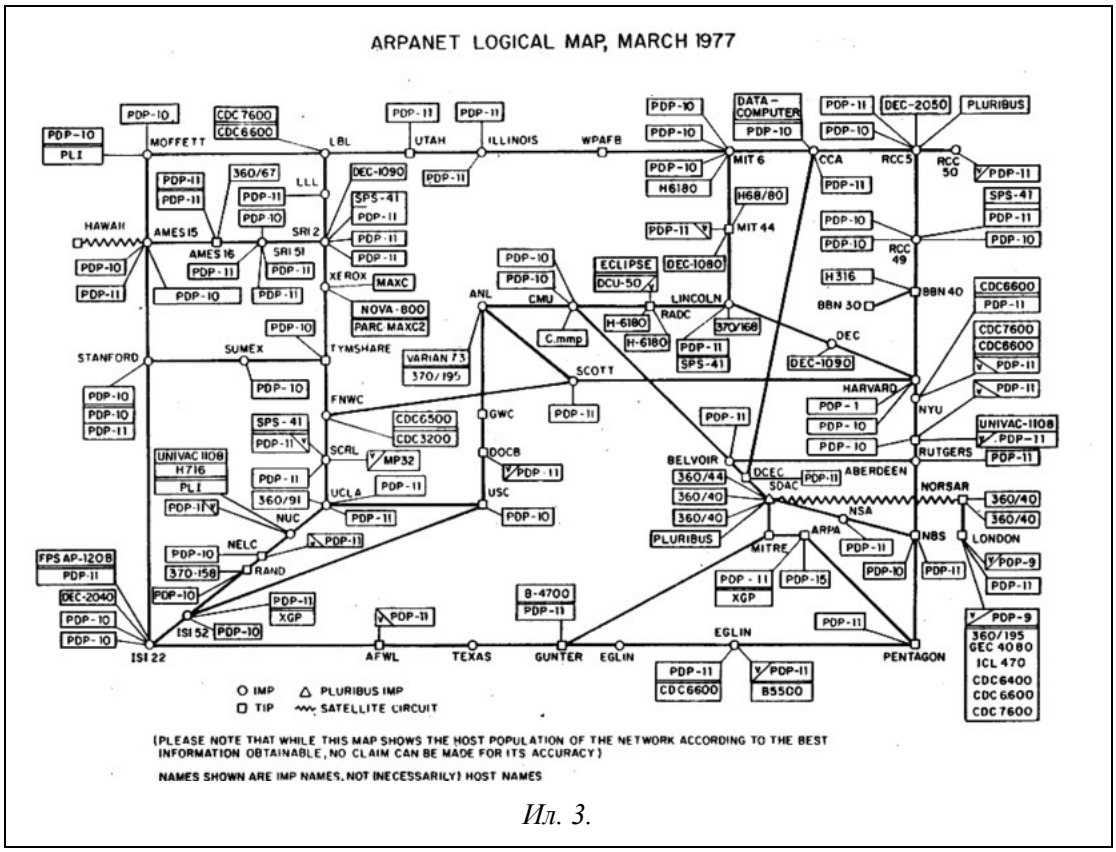
3) *закрытость* программного обеспечения и документации. Сосредоточенность всех технологий в одних руках мешало активно участвовать в развитии и продвижении сети сторонним разработчикам. Поэтому даже при наличии большой пользовательской базы, коммерческие сети начинали быстро умирать, когда их оригинальные разработчики теряли к

ним интерес.

Именно эти проблемы успешно сумел решить Интернет.

От ARPANET — к Интернету

Интернет тоже родился не на пустом месте. Сначала появился ARPANET: компьютерная сеть, созданная по заказу американских властей. ARPA – исследовательское агентство министерства обороны – ставило своей целью создание компьютерной сети, способной функционировать даже при выходе из строя большей части своих узлов, например из-за массированной ядерной атаки. В реальном мире до ядерной войны, к счастью, не дошло, но вот заложенный в сеть стратегический ресурс «выживаемости» оказался вполне востребованным и в сугубо мирное время. Удачной идеей военных было поручить разработку и отладку новых технологий гражданским специалистам, в основном из академической среды. Руководителем нового проекта стал профессор Леонард Клейнрок, один из признанных экспертов по компьютерным сетям и автор ряда ключевых работ в этой области. Первая сеть состояла из четырех компьютеров, расположенных в UCLA (Калифорнийском университете Лос-Анджелеса), SRI (Стэнфордском исследовательском институте), UCSB (Калифорнийском университете Санта-Барбары) и UofU (университете штата Юта), а первый сеанс передачи данных состоялся 29 октября 1969 года. Хотя начало оказалось не слишком обнадеживающим: оператор в Лос-Анджелесе попытался войти на удаленный компьютер в Стэнфорде, введя команду «login». Он успел ввести буквы «l» и «o», потом компьютер «завис» — и войти на удаленный сервер удалось лишь через час, после полной перезагрузки. Так или иначе, но начало ARPANET (а, следовательно, и Интернет) было положено. Динамику роста сети можно оценивать, исходя из того, что в марте 1972 года она насчитывала 29 узловых компьютеров, в июле 1975 — уже 57, а в марте 1977 года количество подключенных компьютеров перевалило за сотню (это можно видеть на следующей схеме).



Ил. 3.

Однако датой окончательного превращения ARPANET в то, что теперь называется Интернетом, обычно считают 1 января 1983 года. Именно тогда работа сети была полностью переведена на протоколы TCP/IP, разработанные Винтоном Серфом и Робертом Каном (до этого применялся более архаичный протокол NCP). Собственно, IP (то есть Internet Protocol) и дал название Сети. В том же 1983 году Интернет окончательно стал «гражданским»: от него был отключен MILNET — закрытая военная сеть, основанная на уже отработанных в ARPANET технологиях (но с того момента взаимодействующая с остальным Интернетом лишь ограниченно и через контролируемые шлюзы). Оценив возможности Интернета, к нему понемногу начали подключаться и коммерческие провайдеры сетевых услуг (в том числе и перечисленные выше). Таким образом, из явления сугубо научной среды Интернет стал превращаться в успешный коммерческий проект. К тому же международный: через спутники к глобальной сети начали подключаться Европа и Юго-Восточная Азия (а уже в 1990 году подключился и СССР).

В успехе Интернета сыграла роль совокупность следующих факторов:

1) *Пакетная коммутация*

Суть этого принципа (впервые сформулированного в своих работах Клейнроком) заключается в том, что данные по сети передаются дискретными фрагментами (*пакетами*). Термин не случайно напоминает о традиционной почтовой службе: как и обычное бумажное

письмо или бандероль, интернет-пакет содержит *заголовочную часть* (т.е. «конверт») и *сами данные* (его содержимое). Как и на конверте, в заголовке содержится только *мета-информация* (в основном, откуда был отправлен пакет и куда его следует доставить). Поэтому даже логически единые и непрерывные объекты данных (например, web-страницы) при передаче разбиваются на множество пакетов, которые объединяются в единое целое только на компьютере-получателе информации. Что было бы невозможным, если бы не следующий пункт.

2) *Единый стандарт адресации узлов сети*

Каждому компьютеру, подключенному к Интернету, приписывается уникальный адрес (так наз. *IP-адрес*), который обычно принято записывать в виде четырех чисел, разделенных точками (www.xxx.yyy.zzz). Внутренняя структура IP-адреса сложнее: в нем упакован *адрес подсети* и индекс компьютера в этой подсети. Сам способ кодирования этой информации меняется в зависимости от так наз. *ранга* подсети: от небольших локальных сетей (менее 256 компьютеров) до сетей-гигантов (десятки тысяч узлов). За счет этого к Интернету легко подключить не только отдельные компьютеры, но и «готовые» локальные сети: достаточно присвоить «внешний» IP-адрес компьютеру, через который происходит выход в подсеть («шлюз»), а уже «внутренние» адреса локальным компьютерам присваиваются администраторами подсети. Обычно на своем пути от отправителя к получателю интернет-пакет проходит множество промежуточных узлов, основная задача которых — доставить этот пакет к шлюзу (адрес которого автоматически вычисляется из IP-адреса назначения).

3) *Единая система символических имен*

IP-адреса узлов принципиально важны для работы Интернета, но не слишком удобны для запоминания человеком. Поэтому Интернет предоставляет большинству компьютеров систему *доменных имен*, позволяющих использовать символические имена (вида **infoculture.rsl.ru**) вместо IP-адресов (вида **195.74.82.79**). Заметим, что эти имена тоже структурированы в соответствии с иерархией *доменов*. Последние всегда «читаются» справа налево: например, в домене **ru** (весь Рунет) находится домен **rsl** (Российская государственная библиотека), а в нем домен — **infoculture** (НИЦ «Информкультура»). У каждого из промежуточных доменов есть своя *зона ответственности* (в том числе свой список имен и соответствующих им IP-адресов). Таким образом, хотя база данных доменных имен разбросана по множеству серверов Сети — при этом она работает как единое целое.

4) *Иерархия протоколов*

Работу Интернета обеспечивает множество *протоколов*. Они образуют *иерархию*: более сложные протоколы основываются на более простых. Классическая сетевая модель OSI (http://ru.wikipedia.org/wiki/%D1%E5%F2%E5%E2%E0%FF_%EC%EE%E4%E5%EB%FC_

OSI) насчитывает целых семь различных уровней! Мы проведем различие между тремя наиболее важными уровнями:

- *физический уровень* (нижний). Это уровень, на котором происходит физическая передача данных: модемный кабель, Ethernet-соединение, беспроводная связь по WiFi-каналу и так далее.

- *системный уровень* (средний). Уровень, на котором работают системные протоколы Интернета, как транспортные (IP, TCP, UDP), так и служебные (DNS, ICMP, ARP/RARP).

- *прикладной уровень* (верхний). Это уже уровень протоколов, фактически используемых большинством интернет-программ. В частности, web-браузерами (в основном известный всем протокол HTTP), программами скачивания файлов (FTP), почтовыми клиентами (POP и SMTP или IMAP), популярными интернет-пейджерами (OSCAR, XMPP) и т. д.

Основная идея, воплощенная в этой иерархии, или *стеке,* протоколов заключается в том, что интернет-программы *изолированы* от деталей физического подключения к нему: они общаются лишь со *средним* (системным) уровнем протоколов, избегая прямого общения с *нижним* (физическим). В практическом плане это означает, что если вы изменили способ своего подключения к глобальной сети (например, от древнего модема перешли к прямому подключению через Ethernet), то это довольно слабо повлияет на те программы, с которыми вы работаете. Ваше подключение станет намного быстрее, но при этом программы не потребуется переустанавливать (и даже в их настройке скорее всего ничего не потребуется менять)!

Наличие иерархии протоколов — один из важных факторов, который защитил Интернет от морального устаревания. Если бы Интернет был привязан к особенностям физического оборудования, он бы устарел вместе с ними: ведь сетевые технологии, которые использовались в начале 1980-х годов, в основном уже отправились на свалку истории. Скорость каналов между узлами Сети выросла многократно, все время появляются новые технологии связи (о которых на заре Сети и не мечталось), но фундаментальные принципы Интернета при этом менять не требуется.

5) *Открытость технологий и программного обеспечения*

Многие из ранних сетей страдали от закрытости документации и управляющего ими программного обеспечения. Ситуация с Интернетом с самого начала была диаметрально противоположной: подробная и обстоятельная документация по всем технологиям и коммуникационным протоколам была свободно доступна прежде всего из самого Интернета (в виде так наз. RFC-документов). Все (или почти все) программное обеспечение также было доступно бесплатно (или за весьма скромные деньги), и большая часть его была доступна в

исходных кодах (что открывало широкие возможности для участия посторонних разработчиков). В отличие от мира пользовательских компьютеров (таких, как PC или Macintosh) операционные системы интернет-серверов (BSD или Linux) в основном бесплатны и даже доступны в исходных текстах. Именно поэтому в создании и развитии Интернета мог принимать участие кто угодно, главное, чтобы он мог предложить интересные идеи.

6) *Отсутствие хозяина*

Последний (и, возможно, самый важный) фактор успеха Интернета.

С тех пор, как американские военные «отделились» от ARPANET, Интернет не имел какого-либо единого хозяина. Сперва он развивался усилиями американских научных учреждений (с их традиционно либеральными взглядами), а потом подключились коммерческие фирмы (которые принесли в него в общем конструктивный дух конкуренции). В Интернете всегда присутствовали центральные регулирующие организации: изначально InterNIC, затем ICANN (Internet Corporation for Assigned Names and Numbers). Но при этом их функции были жестко ограничены (в первую очередь, это управление интернет-доменами верхнего уровня, такими, как .**com**, .**org** или .**net**). В целом же Интернет не является их собственностью: он принадлежит всем — и никому конкретно.

Безусловно, простых пользователей Интернета это вполне устраивало. С американскими властями ситуация была сложнее.

Ключ в когтях

Об *Агентстве национальной безопасности США* (АНБ) известно не слишком много. Оно было (и остается) одной из самых секретных разведывательных организаций на нашей планете. В течение долгого времени американские власти вообще отказывались признавать его существование, что породило дежурную шутку про NSA — “No Such Agency” («Нет такого ведомства”). Символика агентства тоже не лишена намеков: американский орлан с гербовым щитом, сжимающий в своих когтях ключ (и явно не собирающийся его выпускать добровольно). До сих пор является закрытой информация как о бюджете, так и о численности сотрудников. Можно предполагать, что сотрудников в штате агентства от несколько десятков до сотни тысяч, что

Ил. 4.

же качается финансирования, возможно, это самая «дорогая» спецслужба мира. Правда, местонахождение штаб-квартиры агентства известно хорошо: знаменитый «Черный куб» в Форт-Миде, штат Мэриленд. Комплекс кубических зданий из черного стекла окружает целый мини-город площадью примерно в 250 га. В нем есть собственные жилые дома, рестораны и бары, службы сервиса, школы и детские сады: некоторые специалисты (например, шифровальщики) вынуждены проводить там практически всю свою жизнь. Вопреки популярным голливудским мифам, никаких «агентов АНБ» не существует: АНБ не занимается агентурной разведкой. Оно специализируется на разведке *электронной*: прежде всего на перехвате и анализе электронных коммуникаций (так наз. SIGINT, signal intelligence). Объемы собираемой АНБ информации колоссальны, а ее пользователями являются все основные «силовые» ведомства США (прежде всего Министерство обороны, ЦРУ и ФБР). До Сноудена известен только один случай перебежчиков из этого агентства: Уильям Мартин и Бернон Митчелл, штатные криптографы АНБ, которые бежали в СССР (по идейным соображениям) еще в сентябре 1960 года.

Ил. 5.

Когда появился Интернет, немедленно появились и мифы о тотальном контроле АНБ над ним (и они стали органичной частью мифологии, связанной с агентством). Некоторые из них вполне серьезны, а некоторые откровенно юмористические. Например, еще до Интернета появился миф о «строкоеде NSA» (“NSA line eater”), который был якобы ответственен за пропажу строк в ранних системах электронной почты. (В действительности, конечно, АНБ тут не при чем: это были просто «баги» ранних почтовых программ). Не без

влияния этих мифов, популярным развлечением стало включение во вполне невинные электронные письма «подозрительных» фраз (вроде «ЦРУ», «КГБ», «Моссад», «наркотрафик», «ядерный терроризм» и т. п.) — идея заключалась в том, чтобы гипотетические «шпионские компьютеры» АНБ, просматривающие электронную почту, «захлебнулись» в потоке мнимых угроз. (В некоторых популярных программах, например текстовом редакторе EMACS, был специальный модуль, добавляющий подобные «провокационные фразы» к каждому письму.) Удалось ли таким образом подпортить жизнь АНБ, достоверно неизвестно, но сама эта история наглядно иллюстрирует, как ранний либеральный (и даже анархичный) Интернет относился к идее тотального государственного контроля. На самом же деле пользователи «раннего» Интернета, которые были людьми технически продвинутыми, хорошо понимали невозможность полного контроля Интернета, ввиду того, что *тогда* он еще был сильно децентрализован.

В мифологизацию отношений Интернета с АНБ вносили свой вклад хакеры, журналисты, Голливуд, и даже популярные романисты. Здесь интересно вспомнить, что еще до сочинения своих наиболее известных бестселлеров (вроде «Ангелов и Демонов» или «Кода да Винчи») Дэн Браун стал автором романа «Цифровая крепость» («Digital fortress»). Где в центре сюжета не загадки криптоистории — а АНБ, и их колоссальный дешифровальный чудо-компьютер «ТРАНСТЕКСТ»:

...Это был «ТРАНСТЕКСТ», компьютер, равного которому не было в мире, — шифровальная машина, засекреченная агентством.

«ТРАНСТЕКСТ», подобно всем великим технологическим достижениям, появился на свет в силу необходимости. В 1980-е годы АНБ стало свидетелем революции в сфере телекоммуникаций, которой было суждено навсегда изменить весь мир разведывательной деятельности, — имеется в виду широкая доступность Интернета, а если говорить конкретнее — появление электронной почты.

Преступники, террористы и шпионы, которым надоело прослушивание их телефонов, с радостью встретили это новое средство глобальной коммуникации. Электронная почта соединила безопасность обычной почты со скоростью телефонной связи. С тех пор как сообщения стали передаваться по подземным волоконно-оптическим линиям, а не с помощью радиоволн, они оказались полностью защищенными от перехвата — таков, по крайней мере, был замысел.

В действительности перехват электронных писем, передвигаемых по Интернету, был детской забавой для технических гуру из АНБ. Интернет не был создан, как считали многие, в эру домашних персональных компьютеров. Он появился тремя десятилетиями

ранее благодаря усилиям специалистов из министерства обороны и представлял собой громадную сеть компьютеров, призванных обеспечить безопасность правительственной связи на случай ядерной войны. Профессионалы Интернета стали глазами и ушами АНБ. Люди, занимавшиеся нелегальной деятельностью с использованием электронной почты, быстро убедились в том, что их секреты больше не являются их частным достоянием. ФБР, Налоговое управление, Агентство по борьбе с наркотиками и другие правоохранительные агентства США — с помощью опытных штатных хакеров — сумели арестовать и предать суду гораздо больше преступников.

(*Дэн Браун, «Цифровая крепость», Москва, «АСТ», 2011*)

С технической точки зрения этот роман Брауна лучше не цитировать (тут в книге слишком много откровенных нелепостей). Но вот с идеологической, эта цитата очень интересна. Не правда ли, высказанные (еще в 1998 году) аргументы удивительно напоминают то, что мы слышим сегодня в связи с разоблачениями Сноудена? Их логика проста и незатейлива: тотальная и (тайная) интернет-слежка является, по сути, Хорошим Делом, ибо она позволяет эффективно бороться с Плохими Парнями. А если вы этим вдруг недовольны, то к вам надо внимательно присмотреться: вдруг вы тоже «преступник, террорист и шпион»?

Впрочем, возвращаясь от беллетристики к реальной жизни, следует признать: в ней мечты Дэна Брауна долгое время не хотели сбываться: Интернет оставался в основном децентрализованным, со слишком широко распределенной сетью коммуникаций. К тому же стремительное развитие эффективных алгоритмов шифрования делало почти бессмысленным перехват интернет-траффика. (Кстати, именно американские власти долго и в основном безуспешно пытались помешать распространению компьютерных криптографических технологий — но это уже тема для отдельного рассказа.) Новые технологии криптозащищенных интернет-соединений (например, SSL/TLS) позволяли неплохо скрывать информацию не только «шпионам и террористам», но и простым законопослушным пользователям. В АНБ понимали, что ключи от стратегически важных мировых информационных потоков уже почти выскользнули из их цепких когтей.

Концлагерь — дело добровольное

Как хорошо известно из богатого опыта репрессий двадцатого века, если вы хотите эффективно контролировать большую группу людей — достаточно согнать их в одно место, обнести его колючей проволокой и поставить по углам пулеметные вышки. Для такого места имеется и свое название — *концлагерь*. Казалось, что превратить в аналог концлагеря Интернет, исторически основанный на идеях свободы и бесконтрольности, будет непросто. В действительности это оказалось совсем не сложно. Достаточно убедить широкие массы,

что в нашем концлагере самые современные бараки, диетическое питание и очень приятная компания — и они охотно переедут туда сами.

К наиболее примечательным особенностям развития Интернета последнего десятилетия стоит отнести следующее: распространение централизованных серверов электронной почты, невероятный всплеск популярности социальных сетей, активное развитие интернет-торговли и удаленных («облачных») хранилищ пользовательских данных. Можно ли считать случайностью то, что все эти популярные новые услуги сильно *упрощают* массовый контроль над пользователями Сети? В результате у когда-то децентрализованного Интернета внезапно появилось несколько центров, в которых оказалось сосредоточено (по примерной оценке) около 80% пользовательского траффика.

Ил. 6.

Сперва появились централизованные *почтовые сервера*: Yahoo Mail, Hotmail (приобретенный Microsoft в 1997 году) и Google Mail (GMail). Нет ничего странного в том, что они сразу привлекли миллионы пользователей: удобно ведь, когда твой почтовый ящик доступен не только через специальную почтовую программу, но и через простой web-интерфейс, доступный пользователю из любого браузера. Удобно также и то, что ваш почтовый ящик не привязан к личному компьютеру или рабочему месту и легко доступен отовсюду: с работы или из дома, со стационарного компьютера или с мобильных устройств. Но у удобств есть своя цена: придется согласиться с тем, что *вся ваша переписка* теперь хранится на удаленном сервере Microsoft или Google. Впрочем, пользователям, которых это смущало, компании возмущенно отвечали: да как можно нам не доверять, мы всегда защищаем конфиденциальность своих пользователей! И пользователи охотно верили.

Следующий знаковый этап эволюции Интернета — это развитие массовых *социальных сетей*. Легендарный Facebook (более миллиарда пользователей по всему миру!), Twitter и Google Plus (обе примерно по полмиллиарда). Разумеется, есть и сети поменьше (в том числе, национальные) – но, как видим, основные игроки на этом поле *американские*. Для простого пользователя, конечно, социальная сеть является чудом прогресса: можно рассказать о себе всеми миру и приобрести виртуальных друзей из Австралии, Бразилии, и даже Гренландии, если повезет. А уж для любого шпионского ведомства социальная сеть — это чудо вдвойне! Одной из основных задач любого разведывательного ведомства всегда

была слежка за интересными людьми, и выявление их самых интимных секретов, из тех, про которые рассказывают только *друзьям*. А благодаря социальным сетям, у каждого появилась уйма друзей по всему миру — всегда найдется с кем пооткровенничать. Друзьям так и тянет подробно рассказать и о своих успехах, и о своих проблемах: трудностях на работе и в личной жизни, семейных неурядицах и супружеских изменах, проблемах с алкоголем или наркотиками, проблемах со здоровьем, неприятностях с законом... А если вы более-менее значимый человек (политик, высокопоставленный чиновник, крупный бизнесмен...), то вся эта информация о вас крайне интересна не только вашим друзьям, но и любой разведке (не только американской). Даже если вы своим сетевым друзьям ничего такого не рассказываете, сам их круг — это тоже предмет пристального интереса (установление круга близкого общения человека — это тоже одна из ключевых разведывательных задач). А тут заходим на личную страницу этого человека и сразу видим, кто у него в друзьях, а кто нет.

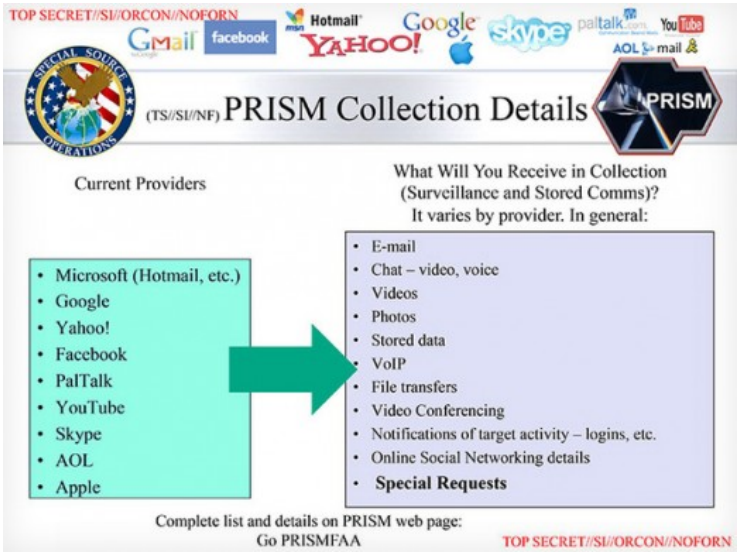
Все сказанное, конечно, не ново, и говорилось многократно. Но все подозрения пользователей социальных сетей относительно конфиденциальности обычно сталкивались с хором негодования со стороны их владельцев: ну как же, мы тщательно охраняем секреты наших пользователей! И у нас их хранить даже безопаснее, чем на вашем собственном компьютере!

Ну и третья, относительно недавняя тенденция — массовое внедрение технологий *удаленного («облачного») хранения* документов и удаленной работы с ними. Здесь, в первую очередь, вспоминаются Google Docs (но можно вспомнить и конкурирующие сервисы: Microsoft SkyDrive, и ICloud от Apple). Как-то внезапно практически все гиганты Интернета озаботились сохранностью персональных документов своих пользователей. Зачем их хранить у вас на жестком диске, когда их можно держать на нашем сервере? Это ведь удобнее: они будут доступны из любого места, и с любого из ваших компьютеров (или мобильных устройств)! Ваш компьютер вы можете потерять, его даже могут украсть — но вот на наших серверах ваши документы в безопасности всегда. Правда, некоторые пользователи считали, что им важна не только безопасность, но и конфиденциальность (ну, вы уже знаете, что им на это отвечали.)

Впрочем, пользователи всему этому охотно верили. Им слишком часто и старательно объясняли, что пристальная слежка за Интернетом — это специфическая особенность нехороших диктаторских режимов, таких, как Иран, Северная Корея, Китай и Россия. В свободной Америке такого быть не может! США не шпионят за пользователями глобальной Сети!

А если и шпионят, то только за очень нехорошими пользователям, и лишь самую-самую чуточку...

Под «Призмой» у АНБ



Ил. 7.

Теперь пора вернуться к Эдварду Сноудену и к тому, что он решился рассказать всему миру. Даже для людей, знающих про американский аппетит к чужим секретам, его разоблачения стали шокирующими.

Прежде всего, это та самая программа *PRISM* (т. е. “Призма”) — основной инструмент контроля над большинством базирующихся в США глобальных компьютерных служб. В частности, в рамках этой программы АНБ прямо доступны базы данных Microsoft (включая, разумеется, и почтовую службу Hotmail), Facebook, Google (вместе с видеохостингом YouTube и почту Gmail), Yahoo (с Yahoo mail), Twitter, Apple (в том числе и “облачное” хранилище данных ICloud), а также такие популярные средства голосовой связи и видеосвязи, как Skype и PalTalk. Контроль над большей частью этих служб АНБ способно осуществлять *напрямую* (то есть агентству доступны *непосредственно* базы данных перечисленных компаний, и для получения информации оттуда не требуется никаких разрешений или согласований). Эта программа действует с 2007 года.

Не менее важны системы *NarusInsight и Carnivore*. С их помощью обеспечивается динамическое слежение за интернет-траффиком, включая и его «глубинный» (т.е. на уровне отдельных пакетов) анализ. Суперкомпьютеры NSA позволяют эффективно отслеживать многое, в том числе web-траффик, электронную почту и даже потоки голосовой информации (включая сюда и протокол VoIP, используемый Skype). В США в эту программу вовлечены и большинство провайдеров сетевых услуг (т. е. все потоки данных без особого труда отслеживаются непосредственно вплоть до конкретного пользователя).

Ил. 8.

Система *Tempora*: британский аналог вышеперечисленных технологий отслеживания

сетевого трафика, функционирующий в тесном контакте с АНБ.

Системы *Boundless Informant* и *X-Keyscore* ориентированы на слежку за информационными потоками *за пределами* США (т. е. там, куда не могут дотянуться вышеперечисленные средства слежки). Насколько можно судить по публикациям, даже в «дружественных» странах (например, Германии) перехват и сбор пользовательской информации в рамках этой программы осуществляется *нелегально* (про «недружественные», разумеется, не приходится и говорить). Многие технические детали этой программы не раскрываются, но известно, что ее обслуживает около 500 серверов по всему миру, так что можно предположить, что масштабы «нелегального» перехвата информации вполне сравнимы с «легальным», если не превосходят его.

Ил. 9. «АНБ. Единственная часть правительства, которая всегда готова вас слушать».

Программа с красивым названием «*Stellar Wind*» («*Звездный ветер*») — еще одна программа динамического анализа как телефонных разговоров, так и email-трафика.

Программа *MUSCULAR*: она обеспечивает нелегальный перехват информационных потоков крупнейших американских компаний (в основном, тех же Yahoo и Google), осуществляемый уже без их ведома.

Наконец, АНБ занимается *хакерской деятельностью* в чистом виде (т.е. взломами «чужих» серверов с целью получения конфиденциальной информации об их пользователях). Понятно, об этих действиях АНБ известно немного, но всплывшие факты также шокируют. Например, успешно были подвергнуты взлому сервера службы резервирования компании «Аэрофлот» (http://lenta.ru/news/2013/09/01/crack/) и катарской телекомпании «Аль-Джазира». Нужно заметить, что подобные действия обычно являются уже *прямым и непосредственным* нарушением законодательства тех стран, в которых расположены сервера (в России, например, автоматически попадая под статью 272 УК РФ).

Впрочем, заметим, что и разглашение конфиденциальных данных пользователей (или, что то же самое, предоставление «тайного» доступа к ним) тоже граничит с нарушением закона. От того, что личные данные пользователя находятся на сервере некой американской компании, они не становятся ее собственностью. То есть предоставление доступа к ним третьей стороне без разрешения их владельцев — это, фактически, уже их *кража*.

Хотя разглашена лишь очень небольшая часть информации о деятельности АНБ, даже ее вполне достаточно, чтобы констатировать *беспримерное лицемерие* американских властей. Вспомним, что именно из их уст в адрес нелюбимых ими стран и правительств очень часто звучат обвинения в «слежке над Интернетом» — но теперь стало очевидно, что не чья-нибудь, а именно американская слежка над пользователями Интернета приобрела масштабы, вообще не имеющие аналогов в мире! *Любой* пользователь из *любой* страны мира, заходя на (практически) любой популярный американский сайт (включая, разумеется, Google, Hotmail, Facebook, YouTube, Yahoo...), должен осознавать, что оказывается «под колпаком» у американских спецслужб (точнее говоря — под их «Призмой»).

Сами масштабы американской интернет-слежки таковы, что вызывают ощущение театра абсурда. Действительно, какой смысл следить одновременно за *миллионами* пользователей во всем мире? Невозможно поверить, что большинство из них является террористами или наркоторговцами. На самом деле, все разглагольствования о «борьбе с преступностью и/или терроризмом» — явная и очевидная ложь. (Тем более нелепая, что как раз преступники и террористы прекрасно понимают: Интернет всегда находится под жестким присмотром заинтересованных ведомств. А потому какой-нибудь очередной Бен Ладен вряд ли будет обсуждать планы следующего теракта на своей странице в Facebook.) Целью американской глобальной слежки является, прежде всего, сбор информации о простых (и в большинстве своем законопослушных) пользователях глобальной сети. Политический сыск, слежка за потенциальными диссидентами, сбор компромата на важных лиц для последующего шантажа или давления — в общем, все что угодно, но только не декларированная «борьба с терроризмом».

В связи с разоблачениями Сноудена АНБ и американские власти подвергаются жесткой международной критике, в том числе и со стороны своих традиционных союзников по НАТО. Впрочем, это их нисколько не смущает. Никаких извинений с их стороны мир не дождался: наоборот, инфраструктура глобального шпионажа расширяется. «Васька слушает, да ест»: из последних новостей — строительство новых центров обработки данных в штате Юта (http://telecombloger.ru/16160):

АНБ опубликовало первый пресс-релиз о строительстве массивного ЦОД в штате Юта в январе 2011 года, назвав его крупнейшим дата-центром в ведении Пентагона в стране. Согласно тексту пресс-релиза, проект позволит создать от 5 000 до 10 000 временных рабочих мест на этапе строительства, а также от 100 до 200 постоянных рабочих мест после ввода ЦОД в эксплуатацию. Строительство дата-центра ведется инженерными войсками США. Пресс-секретарь АНБ Вани Вайнс сказал, что возведение

ЦОД должно быть завершено в сентябре. Помимо АНБ, объектом смогут воспользоваться и другие учреждения, в том числе Департамент национальной безопасности США.

Объемы информации, которые будут там храниться, впечатляют: примерно *пять зеттабайт* (а один зеттабайт — это *триллион* гигабайт). Во всем мире невозможно отыскать достаточно террористов, чтобы оправдать подобные затраты! Только уже понятно, что речь идет совсем не о террористах, а обо всех подряд. Включая, возможно, и вас: даже если сегодня вы совершенно не интересны американским властям — вдруг завтра они возьмут и вами заинтересуются?

Можно ли вернуться к суверенному Интернету?

Из разоблачений Эдуарда Сноудена и весь мир, и Россия должны извлечь определенные уроки. Самый важный из них таков: избыточно централизованный Интернет (главные центры которого находятся в США) — это *несомненное зло* для пользователей (хотя, конечно, и бесценный подарок для американских властей). Единственный эффективный способ борьбы с этим злом — постепенное возвращение к децентрализованной и распределенной модели Интернета.

По традиции, понятие «государственный суверенитет» включает в себя немало: возможность проводить суверенную политику, свой внутренний рынок, свою валюту и финансовую систему, свои собственные вооруженные силы, собственные законы и суды. Сейчас, в наше время, появился еще один важнейший вид национального суверенитета: *электронный* или *цифровой*. Цифровой суверенитет — это не просто собственная доменная зона в Интернете, но и собственные ключевые интернет-ресурсы. То есть, свои поисковые системы, свои социальные сети, свой национальный сервис электронной почты, свои «облачные» хранилища данных и система онлайн-торговли. Это, конечно, довольно дорогое удовольствие, доступное отнюдь не каждой стране. Однако стремиться к этому надо. Полезно помнить крылатые слова Наполеона: «Народ, который не хочет кормить свою армию, будет кормить чужую». А народ, не имеющий суверенного Интернета, — будет поддерживать Google, Facebook и Twitter, не только помогая зарабатывать миллиарды американским интернет-гигантам, но и вдобавок еще и предоставляя им неограниченные возможности для скрытного надзора над собственной интернет-жизнью.

Строительство суверенного Интернета — это непростая задача. Китай занимается его созданием давно и целенаправленно: у него уже есть собственный аналог Google – Baidu, свой локальный Facebook – Renren, есть собственный сервис микроблогов Weibo и свой портал интернет-торговли Taobao. К собственным электронным ресурсам стремятся и другие страны, находящиеся в натянутых отношениях с США (например, в Иране основным и

весьма популярным социальным сервисом является Cloob).

В последние дни, в связи с фактами, раскрытыми Сноуденом, вопрос о создании «собственного Интернета» *очень серьезно* поднят и в Германии:

И вот, германская телекоммуникационная компания Deutsche Telekom (32% акций государственные, остальные на свободных биржевых торгах) предложила создать национальную коммуникационную сеть. Для начала – только в Германии. Но если она проявит эффективность и приобретёт популярность у пользователей, в дальнейшем она может быть распространена на все страны шенгенской зоны. От Deutsche Telekom уже поступило официальное предложение властям Германии – запретить переправку интернет-трафика через узлы, расположенные за пределами страны. Как пояснил один из руководителей концерна Филипп Бланк, сначала речь пойдёт об электронной почте, а потом и обо всём трафике. Официально объявленная цель проекта в этом и заключается – защитить немецких пользователей Интернета от прослушки иностранными спецслужбами. Фактически же речь идёт о создании первой национальной системы Интернета, полностью независимой от американских сервисов.

Пока не известно, насколько создаваемая в Германии локальная сеть сможет обеспечить безопасность от американских спецслужб. Но информационная безопасность отнюдь не сводится только к защите от прослушки. Речь идёт в целом о возможности самостоятельно обеспечить функционирование Интернета на своей территории. Что бывает с теми, кто самостоятельное функционирование обеспечить не может – можно наблюдать на примере Ливии, где с началом западных бомбардировок Интернет был просто отключён. А на сегодняшний день и Германия находится в таком же положении, как Ливия. Вот о чём идёт речь в предложении Deutsche Telekom.

(http://newsland.com/news/detail/id/1270639/)

В России же *исторически* получилось так, что национальные интернет-сервисы заняли рыночные нищи, во многих других странах прочно занятые глобальными компаниями. У нас уже есть собственные поисковые системы (Yandex и Rambler), несколько собственных почтовых сервисов (например, Mail.Ru и почта Yandex), собственные социальные сети (прежде всего, «Одноклассники» и «ВКонтакте»). То есть, в России уже есть практически все, что способно эффективно обеспечить свой электронный суверенитет. А в свете того, что рассказал миру Эдвард Сноуден, все это — не роскошь, а насущная необходимость. И электронный суверенитет мало обрести — его надо быть готовым отстаивать так же последовательно, как и любые другие формы государственного

суверенитета.

Список литературы:

1. [Электронный ресурс]. – Режим доступа: URL: http://en.wikipedia.org/wiki/Leonard_Kleinrock (дата обращения: 07.11.2013).
2. [Электронный ресурс]. – Режим доступа: URL: http://www.ehow.com/facts_7266921_did-offer-internet-online-services.html (дата обращения: 07.11.2013).
3. [Электронный ресурс]. – Режим доступа: URL: http://en.wikipedia.org/wiki/History_of_the_Internet (дата обращения: 07.11.2013).
4. [Электронный ресурс]. – Режим доступа: URL: http://www.12min.ru/it/vozniknovenie-interneta-xronologiya-sobytij.html (дата обращения: 07.11.2013).
5. [Электронный ресурс]. – Режим доступа: URL: http://www.teachervision.fen.com/computers/jargon/N/NSA-line-eater.html (дата обращения: 07.11.2013).
6. [Электронный ресурс]. – Режим доступа: URL: http://en.wikipedia.org/wiki/Martin_and_Mitchell_defection (дата обращения: 07.11.2013).
7. [Электронный ресурс]. – Режим доступа: URL: http://www.inopressa.ru/article/31Oct2013/wp/nsa2.html (дата обращения: 07.11.2013).

Сведения об использованных иллюстрациях:

Иллюстрация содержания. [Электронный ресурс]. – Режим доступа: URL: http://teecraze.com/wp-content/uploads/bsapeepingeagle.jpg (дата обращения: 07.11.2013).

Ил. 1. «Прекратите нас прослушивать!» [Электронный ресурс]. – Режим доступа: URL: http://ahlibeyt.ru/wp-content/uploads/2013/08/5753.jpeg (дата обращения: 07.11.2013).

Ил. 2. [Электронный ресурс]. – Режим доступа: URL: http://www.unionjalisco.mx/articulo/2013/07/12/politica/las-10-de-un1on-12-de-julio (дата обращения: 07.11.2013).

Ил. 3. [Электронный ресурс]. – Режим доступа: URL: http://en.wikipedia.org/wiki/File:Arpanet_logical_map,_march_1977.png (дата обращения: 07.11.2013).

Ил. 4. [Электронный ресурс]. – Режим доступа: URL: http://www.democracynow.org/images/blog_posts/68/23068/w320/NSA-Logo.jpg?20130724 (дата обращения: 07.11.2013).

Ил. 5. [Электронный ресурс]. – Режим доступа: URL:

http://news.dphotographer.co.uk/wp-content/uploads/2012/nsa-headquarters-building (дата обращения: 07.11.2013).

Ил. 6. [Электронный ресурс]. – Режим доступа: URL: http://image.zn.ua/media/images/original/Nov2011/38945.jpg (дата обращения: 07.11.2013).

Ил. 7. [Электронный ресурс]. – Режим доступа: URL: http://siliconangle.com/files/2013/07/nsa-eagle1.jpg (дата обращения: 07.11.2013).

Ил. 8. [Электронный ресурс]. – Режим доступа: URL: http://clashdaily.com/wp-content/uploads/2013/06/Political-memes-nsa.jpg (дата обращения: 07.11.2013).

Ил. 9. «АНБ. Единственная часть правительства, которая всегда готова вас слушать». [Электронный ресурс]. – Режим доступа: URL: http://teecraze.com/wp-content/uploads/bsapeepingeagle.jpg (дата обращения: 07.11.2013).

Источник: ***Культура в современном мире. — 2013. — № 4. — [Электронный ресурс].*** — Режим доступа: ***URL:*** http://infoculture.rsl.ru