А.И.Смирнов
Президент НИИГлоБ, советник РКСС,
Чрезвычайный и Полномочный
Посланник РФ в отставке,
д.и.н. профессор

«Snowdengate»: анализ «цифрового фашизма» спецслужб США и их союзников

Начало XXI в. может войти в скрижали человечества как один из самых драматичных периодов. Планета вошла в зону геополитической турбулентности: сполохи войны цивилизаций, международного терроризма, угроза рецессии, рецидивы холодной войны и пиратства, всплеск локальных и региональных конфликтов, техногенные, природогенные, социогенные катастрофы, эпидемии и пандемии, голод.

Беспрецедентная информационная революция, наряду с несомненным позитивом, на первый план выдвинула и инфогенные угрозы.

Данный феномен принципиально изменил геополитический код цивилизации: с одной стороны – локомотив пятого технологического уклада, с другой – новые вызовы и угрозы международной безопасности.

В Послании Президента России Федеральному Собранию от 12 декабря 2013 года подчеркнуто: «Накал военно-политической, экономической, информационной конкуренции в мире не снижается, а только усиливается. И другие центры влияния внимательно следят за усилением России.»[1]

Ведущие страны мира разработали и реализовали концептуальные и доктринальные стратагемы[2] использования ИКТ в геополитической конкуренции и обеспечения информационного суверенитета.

---

[1] http://www.kremlin.ru/news/19825

[2] Стратагема, или стратегема (древнегреч. στρατήγημα — военная хитрость, кит. 計 палл. цзи) - хитроумный план, оригинальный путь к достижению военных, гражданских, политических, экономических или личных целей

Важную роль в этом процессе сыграло обнародование в ряде СМИ экс-сотрудником ЦРУ и Агентства национальной безопасности (АНБ) США[3] Эдвардом Сноуденом секретных документов американских спецслужб. Документы разоблачают многочисленные факты незаконной деятельности[4] США и их союзников в глобальном информационном пространстве.

Анализ публикаций показывает, что США, грубо попирая права граждан, создали глобальную систему электронного шпионажа, перехвата и обработки личных данных пользователей разных стран мира: телефонных разговоров, смс-сообщений, переписки в социальных сетях и по электронной почте.

АНБ взламывало операционные системы смартфонов практически всех ведущих производителей: «iPhone» компании «Apple», «BlackBerry», «Android», перехватывая личные данные пользователей.

В 2010-2011 гг. спецслужбы разработали программу по сбору геолокационных сведений об абонентах сотовых сетей. Так, АНБ ежедневно собирает и сохраняет около пяти миллиардов записей о местонахождении и передвижениях владельцев мобильных телефонов по всему миру, а затем при

---

[3] Разведывательное сообщество США (United States Intelligence Community, IC) - собирательный термин для обозначения 16-и отдельных правительственных учреждений Общее руководство с 2005 года осуществляет директор Национальной разведки. С образованием министерства внутренней безопасности и отделением ЦРУ от руководства разведсообщества данные всех разведсообществ аккумулирует директор Национальной разведки, а ЦРУ работает с так называемой human intelligence — агентурой. Это совпало с общим трендом последнего времени, когда все большую роль играет SIGINT — signal intelligence, то есть массив электронной информации. Кроме того, за последние 15–20 лет за счет спутников и других средств мощное развитие получила геопространственная разведка. АНБ (National Security Agency/Central Security Service, NSA/CSS) — отвечает за сбор и анализ зарубежных трафиков, их координат, направлений, криптоанализ, а также за защиту государственных коммуникационных каналов от действий аналогичных служб других государств http://ru.wikipedia.org/wiki/ 17.12.2013

[4] Программы АНБ США по сбору данных о телефонных переговорах американцев противоречат конституционным нормам. Таково предварительное определение, вынесенное 16.12.2013 г. в Вашингтоне федеральным окружным судьей Ричардом Леоном. Ранее АНБ на основании судебного решения от 1979 г. оправдывалось, что метаданные о звонках не подпадают под действие четвертой поправки, однако судья счел, что "спустя 34 года использование телефонов вышло на совсем другой уровень, и сегодня подобная информация по мере накопления позволяет выстраивать подробную картину о личной жизни каждого". Скандалы вокруг разоблачений в отношении АНБ привели к отставке его главы. В октябре 2013 г. комитет по разведке сената США одобрил законопроект, накладывающий ограничения на деятельность АНБ. Будут ограничены возможность для массового сбора телефонных и электронных данных, сроки их хранения, введена уголовная ответственность за умышленный несанкционированный доступ к подобным сведениям. Администрация Б. Обамы изучает возможность внесения серьезных корректив в работу спецслужб. http://www.rg.ru/2013/12/17/sud-site.html 17.12.2013

помощи специальной программы CO-TRAVELER проводит контент, ивент и коннект-анализ, а также мониторинг передвижения людей.

С 2010 г. АНБ обрабатывает информацию о социальных контактах граждан США, их персональных данных, в том числе телефонных звонках, интернет-активности, банковских кодах, страховых сведениях, регистрационных списках избирателей.

АНБ было способно хранить собранные данные о жителях США вплоть до 5 лет без получения специального разрешения. Единственным формальным ограничением является то, что собранная информация должна способствовать предотвращению угроз национальной безопасности или проведению расследований. Она может быть передана союзным государствам или иностранным организациям, при условии сохранения анонимности пользователей.

В рамках проекта «Boundless Informant» АНБ только в марте 2013 г. собрало около 97 млрд. файлов информации о звонках иностранных граждан по всему миру[5], в том числе об Иране (14 млрд. файлов), Пакистане (13,5 млрд.), Иордании (12,7 млрд.), Египте (7,6 млрд.), Индии (6,3 млрд.).

Вторая молодость «Эшелона»

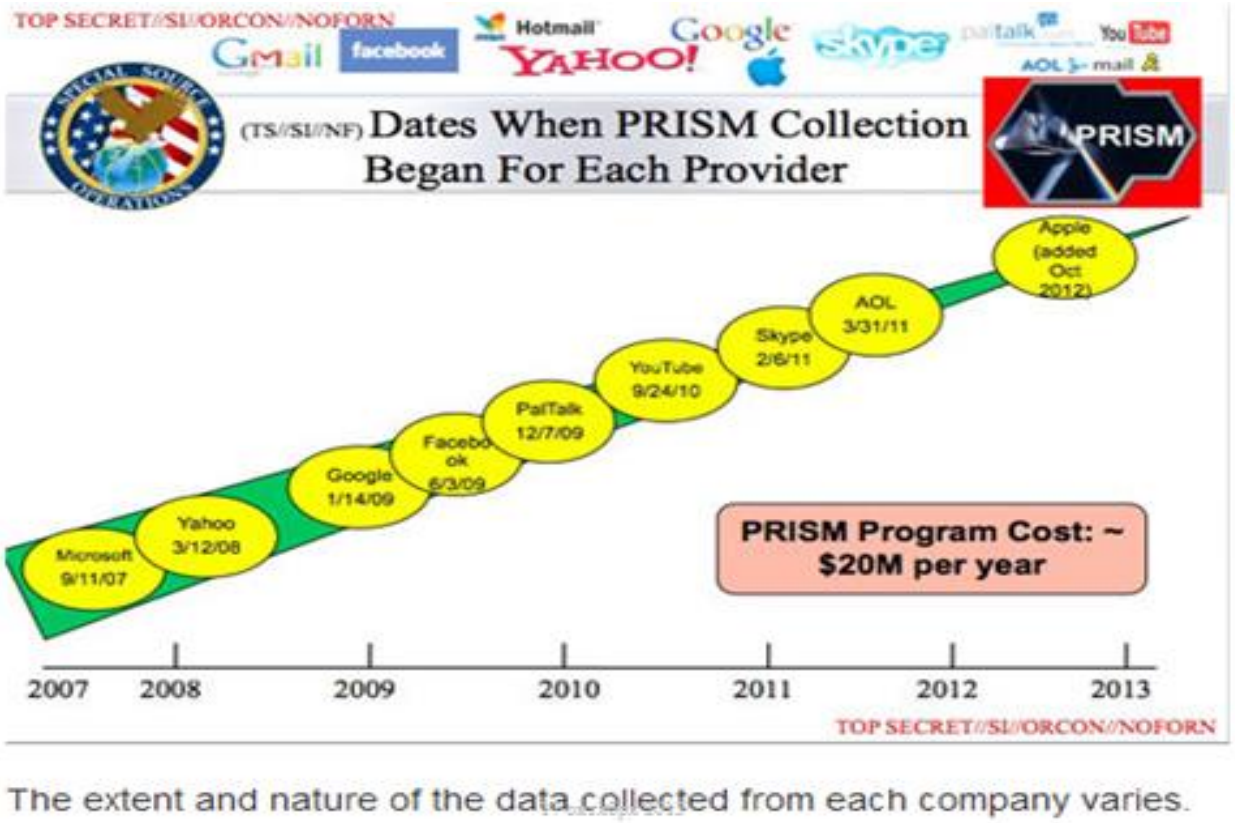
АНБ тесно взаимодействует с иностранными разведками. США, Великобритания, Канада, Австралия и Новая Зеландия входят в секретное союзное объединение по сбору данных в рамках глобальной системы радиоэлектронной разведки «Эшелон» (AUSCANNZUKUS или Five Eyes), основанной в формате США-Великобритания ещё в 1947 г. Спецслужбы этих стран обмениваются развединформацией, в том числе о гражданах своих государств. Позднее к альянсу присоединился ряд стран НАТО, в том числе Норвегия, Дания, ФРГ и Турция.[6]

---

[5] The Guardian от 11 июня 2013 г.

[6] http://ru.wikipedia.org/wiki/%D0%AD%D1%88%D0%B5%D0%BB%D0%BE%D0%BD_%28%D1%81%D0%B5%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D0%B0%D1%8F_%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D0%B0%29 17.12.2013

В рамках проекта «Prism» АНБ и британский Центр правительственной связи - ЦПС (Government Communications Headquarters, GCHQ)[7], начиная с 2007 г., наладили сотрудничество с мировыми ИКТ-компаниями: «Microsoft», «Yahoo», «Google», «Facebook», «PalTalk», «AOL», «Skype», «YouTube» и «Apple» для сбора и обмена разведданными (на слайде).[8]



The extent and nature of the data collected from each company varies.

Такое сотрудничество позволяет спецслужбам прочитывать интернет-историю, электронные письма пользователей и отслеживать передачу файлов в глобальном информационном пространстве.

«Под колпаком» лидеры государств и иностранные дипломаты

АНБ прослушивало телефонные разговоры 35 глав различных государств. Контактные данные агентство получало от сотрудников

[7] http://ru.wikipedia.org/wiki/%D6%E5%ED%F2%F0_%EF%F0%E0%E2%E8%F2%E5%EB%FC%F1%F2%E2%E5%ED%ED%EE%E9_%F1%E2%FF%E7%E8
[8] http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

различных ведомств, в том числе Белого дома, Госдепартамента и Пентагона[9].

Спецслужбы США отслеживали переговоры канцлера Германии А.Меркель с 2002 г, в том числе и до ее избрания на этот пост[10], разговоры членов правительства Испании[11] и перехватывало интернет-трафик и телефонные переговоры президента Бразилии Дилмы Роуссефф и мексиканского лидера Энрике Пенья Ньето. Электронную почту последнего спецслужбы США начали вскрывать еще за месяц до его избрания на пост президента[12]. В 2010 г. АНБ получило доступ к электронной почте президента Мексики Фелипе Кальдерона и письмам мексиканских министров, которые касались дипломатических, экономических и политических вопросов[13].

Британский ЦПС прослушивал телефонные разговоры и мониторил компьютеры министра финансов Турции и 15 членов турецкой делегации, а также других участников саммита «Группы двадцати» в Лондоне в 2009 г., в том числе Президента России Д.А.Медведева[14]. В 2005 г. британский ЦПС следил за деятельностью министра иностранных дел ЮАР и другими дипломатами[15].

Характерно, что спецслужбы США и Великобритания незаконно взламывали практически все используемые в сети Интернет стандарты криптографии. В силу этого они имели доступ к чувствительной информации, содержащей, в том числе, и коммерческую тайну компаний по всему миру, и иным зашифрованным данным.

---

[9] The Guardian от 24 октября 2013 г.
[10] Der Spiegel от 26 октября 2013 г.
[11] El Pais от 25 октября 2013 г.
[12] TV Globo от 2 сентября 2013 г.
[13] Der Spiegel от 20 октября 2013 г.
[14] The Guardian от 17 июня 2013 г.
[15] The Guardian от 17 июня 2013 г.

Для взлома шифров АНБ использует имеющиеся у него суперкомпьютеры, а также прибегает к услугам высокопрофессиональных хакеров. Ежегодно на эти цели США тратят более 250 млн.дол.[16].

При этом АНБ предпринимает попытки взлома так называемого «Лукового маршрутизатора»[17], разработанного в США и позволяющего пользователям сохранять анонимность в сети Интернет. С помощью специальной программы АНБ способно получать доступ к файлам, хранящимся на компьютерах пользователей, их паролям и сведениям об их интернет-деятельности (на слайде)[18].

Кибернаступление США

Анализ документов показывает, что в 2011 г. спецслужбы США совершили 231 наступательную кибероперацию. Три четверти из них

[16] The Guardian от 6 августа 2013 г.

[17] Луковая маршрутизация (Onion routing) - технология анонимного обмена информацией через компьютерную сеть. Сообщения неоднократно шифруются и потом отсылаются через несколько сетевых узлов, называемых луковыми маршрутизаторами. Каждый маршрутизатор удаляет слой шифрования, чтобы открыть трассировочные инструкции, и отослать сообщения на следующий маршрутизатор, где все повторится. Таким образом промежуточные узлы не знают источник, пункт назначения и содержание сообщения. На 2009 год, анонимная сеть Tor является доминирующей технологией, которая использует луковую маршрутизацию.

[18] The Guardian от 4 октября 2013 г.

были направлены против Ирана, России, Китая и Северной Кореи. К концу 2013 г. планировалось поставить под американский контроль 85 000 стратегически отобранных компьютеров по всему миру, для их последующего вывода из строя[19]. Всего же АНБ выделило 61 000 целей для проведения наступательных кибероперациий по всему миру[20].

В апреле 2013 г. АНБ создало тайный список своих основных «мишеней». Среди них Китай, Россия, Иран, Пакистан, Северная Корея, Афганистан, Германия и другие страны, а также Евросоюз. При этом все страны оцениваются по шкале от 1 до 5, где 1 – высший приоритет для АНБ. Из европейских государств наибольший интерес для США – Германия.[21]

Программа Quantum

АНБ располагает «тайными каналами связи» для того, чтобы получать доступ к компьютерам, которые не подключены к интернету, – программой Quantum[22].

В рамках этой программы американские спецслужбы успешно внедряли жучки в компьютеры и сети, используемые армиями России и Китая, компьютеры мексиканской полиции и мексиканских наркокартелей, а также в технику «партнеров США по борьбе с терроризмом», таких как Саудовская Аравия, Индия и Пакистан.

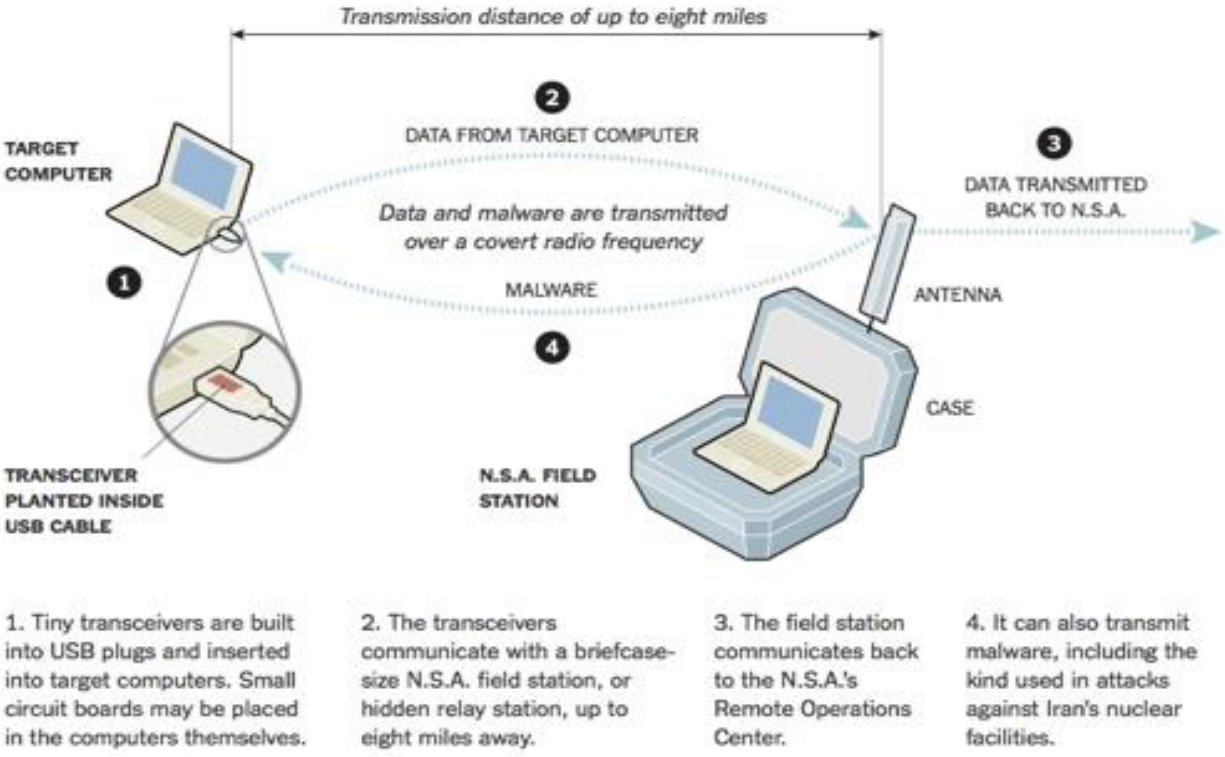
Чтобы осуществлять слежку, АНБ внедрило крошечные беспроводные модули и шпионское программное обеспечение примерно в 100 тыс. персональных компьютеров, распространенных по всему миру.

По команде АНБ эти компьютеры могут быть легко превращены в ботнет для кибератак. Технология также может быть использована для незаметного изменения хранящейся на компьютере информации.

---

[19] The Washington Post от 31 августа 2013 г.
[20] The South China Morning Post от 11 сентября 2013 г.
[21] Der Spiegel от 26 августа 2013 г.
[22] http://safe.cnews.ru/top/2014/01/15/new_york_times_anb_zarazhaet_rossiyskie_voennye_pk_ne_podklyuchennye_k_internetu_556423

Сотрудник АНБ может получить беспроводной доступ к компьютеру с интегрированным в него тайным модулем с расстояния в несколько километров, активировав специальное устройство слежения.



Поместить модуль в персональный компьютер можно несколькими способами: это может сделать агент, производитель компьютера или сам пользователь, сам того не осознавая (модуль, например, может быть помещен в USB-кабель).

Спецслужбы США называют такие действия «проактивной защитой» от киберугроз со стороны других стран. Однако сами США выступают резко против аналогичных закладок, которые, по их данным, устанавливают в свое телекоммуникационное оборудование китайские производители Huawei и ZTE.

В США указанные технические средства не применяются. Представитель АНБ в ответ на запрос NYT заявил, что они не занимаются хищением коммерческих тайн иностранных конкурентов компаний из США.

Хотя источники сообщают, что беспроводные жучки внедряются в том числе в ПК, которыми пользуются европейские торговые ассоциации.

Недавно германское издание Spiegel опубликовало 50-страничный каталог жучков, которые могут заказывать и внедрять сотрудники агентства. Жучки предназначены для внедрения в оборудование ведущих производителей, включая Cisco, Huawei, Juniper, Dell и др.

Анализ киберпрограмм США показывает, что американские военные все больше фокусируются на развитии ударных возможностей в информационном пространстве. Согласно опубликованному «секретному бюджету» американских спецслужб, в 2013 г. из федерального бюджета на нужды разведки было выделено 52,6 млрд.дол. Больше всего средств запросило ЦРУ – 14,7 млрд.дол. , АНБ - 10,8 млрд.дол. и Национальное управление военно-космической разведки США - 10,3 млрд.дол. Основные статьи расходов: предупреждение американских властей об угрозах, борьба с терроризмом, противодействие распространению оружия, проведение активных спецкибероперациий и контрразведка[23]. Приоритетом контрразведки определено противодействие разведдеятельности Китая, России, Кубы, Пакистана, Ирана и Израиля.[24]

В октябре 2012 г. была издана секретная директива президента США, согласно которой, наступательные операции в информационном пространстве предоставляют исключительные возможности для США продвигать свои национальные интересы в глобальных масштабах[25]. Американским военным и разведслужбам поручено подготовить план с указанием списка целей, против которых будет применяться кибероружие.

В рамках проекта «План икс» в США создается карта мирового информационного пространства в режиме реального времени. При этом операции будут осуществляться, естественно, без предупреждения объекта нападения.

---

[23] The Washington Post от 29 августа 2013 г.
[24] The Washington Post от 29 августа 2013 г.
[25] The Guardian от 7 июня 2013 г.

Планом предусматривается уничтожение информационной инфраструктуры противника, в частности вывод из строя компьютерных систем критически важных объектов.

В случае неотвратимости кибернаступления противника предусматривается нанесение превентивного удара.

В директиве заложена возможность проведения таких операций и в информационном пространстве США, но только после указания президента.

«Цифровой фашизм» США?

Опубликованные документы убедительно показывают, что спецслужбы США имели доступ практически к каждому пользователю Интернета (и не только!). Особое место отводилось государственным, дипломатическим, экономическим и иным чувствительным источникам информации. Так, АНБ следило за 38 посольствами и миссиями, в том числе представительствами ЕС в Нью-Йорке и Вашингтоне и штаб-квартирой МАГАТЭ в Вене. При этом наряду с идеологическими противниками США и странами Ближнего Востока в этот список попали посольства Франции, Италии, Греции, Японии, Мексики, Южной Кореи и Турции[26].

При этом АНБ осуществляет сбор персональных данных на территории США, что запрещено национальным законодательством. Действуя с разрешения американского суда по делам о надзоре за деятельностью иностранных разведслужб, АНБ, благодаря своим программам слежки, перехватывает до 75% всех интернет-коммуникаций в стране[27].

С 2001 по 2011 гг. в США по разрешению суда функционировала программа «Stellar Wind» по сбору так называемых «метаданных». Изначально «Stellar Wind» собирала данные о телефонных звонках, совершенных из США за границу или в пределах США абонентов, которые не являлись американскими гражданами. Однако позднее АНБ получило

[26] The Guardian от 30 июня 2013 г.
[27] The Wall Street Journal от 20 августа 2013 г.

полномочия собирать данные и о гражданах США[28]. В 2007 г. под контролем спецслужб оказалось около 34 тысячи человек, включая 3 тысячи граждан США.

Характерно, что с 2008 г. АНБ отслеживает всю интернет-деятельность граждан США, подозреваемых в связях с иностранцами. Официально программа была разрешена секретной директивой № 424 в ноябре 2010 г. При этом АНБ использует компьютерные алгоритмы для создания детальных схем контактов и поведения американцев. Информация берется как из открытых, так и конфиденциальных источников и сохраняется на специальных серверах до года[29]. Программа способна перехватывать 20 млрд. «событий» в день и обрабатывать их за 1 час.

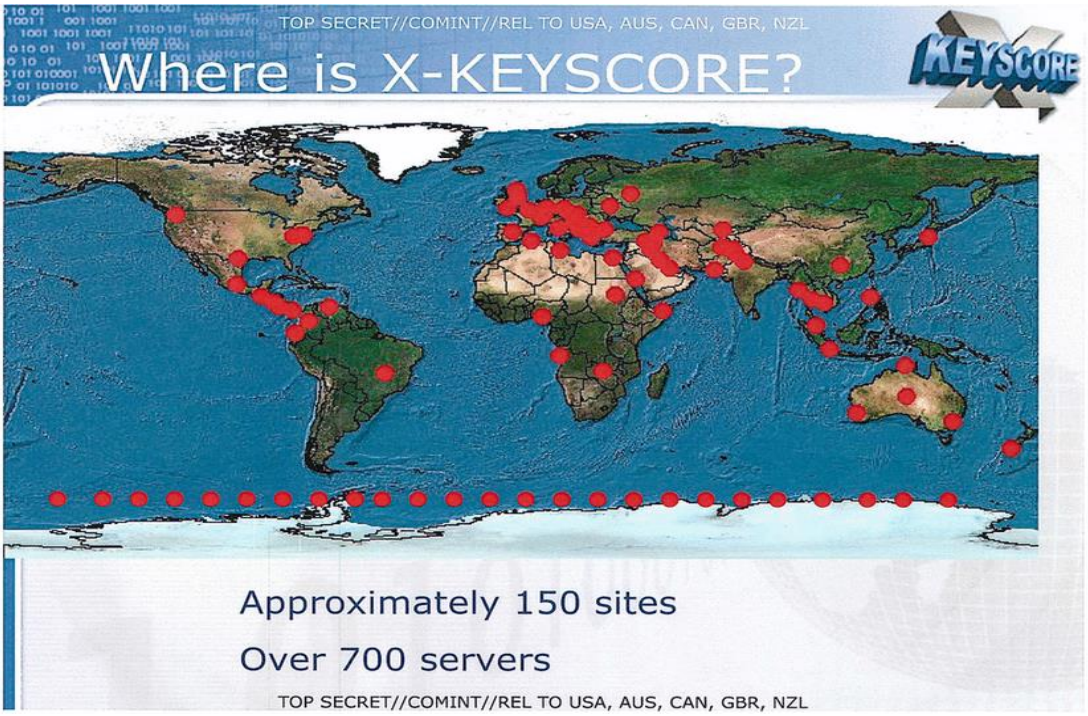
Важным инструментом геоинформационного господства США является программа «XKeyscore». Она способна мониторить практически все действия пользователей в сети Интернет, собирает о них все сведения, включая содержание электронных писем и переписку в социальных сетях. В докладе АНБ от 2007 г. говорится о том, что в рамках программы была собрана информация о 850 млрд. телефонных звонках и 150 млрд. электронных записях. Ежедневно в эту базу данных добавлялось 1-2 млрд. записей. В 2012 г. в течение месяца этой программой было собрано, по меньшей мере, 41 млрд. записей[30].

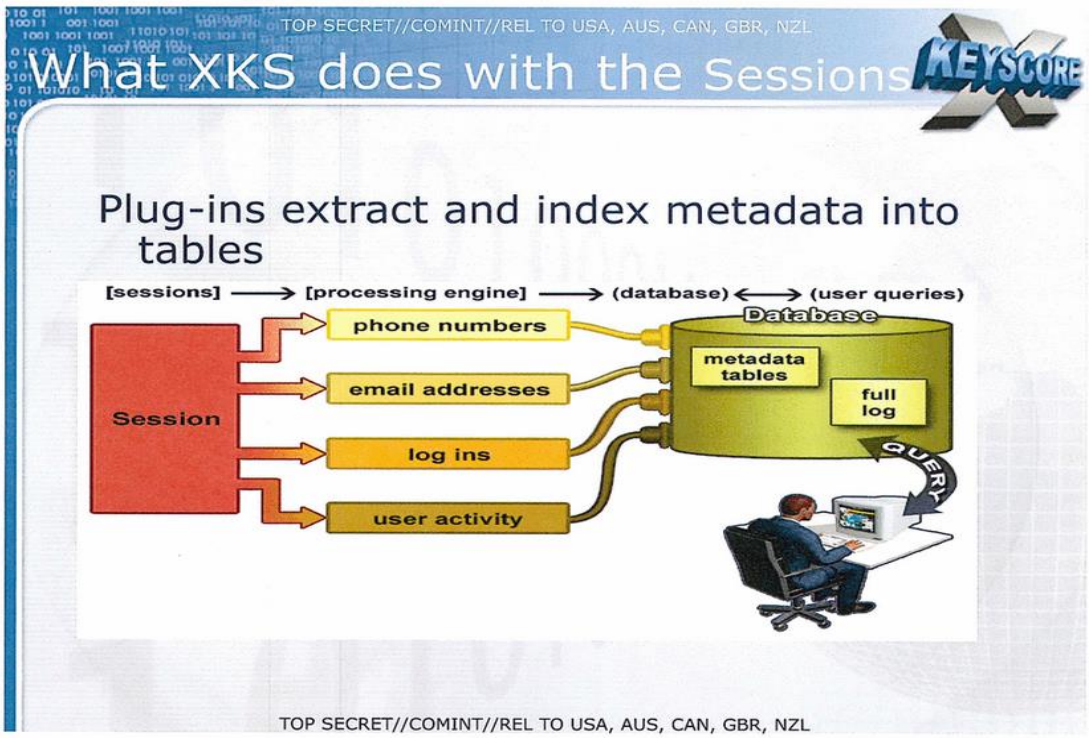
X-Keyscore - секретная программа компьютерного слежения, осуществляется совместно АНБ США, Управлением радиотехнической обороны Австралии и Службой безопасности правительственных коммуникаций Новой Зеландии. Предназначена для слежения за иностранными гражданами во всем мире, деятельность осуществляет с помощью более чем 700 серверов, расположенных в США и на территории

[28] The Guardian от 27 июня 2013 г.
[29] The Guardian от 30 сентября 2013 г.
[30] The Guardian от 31 июля 2013 г.

стран-союзников США, а также в посольствах и консульствах США в нескольких десятках стран, в том числе в Москве, в Киеве и Пекине. [31]

Ниже приводятся слайды из секретной презентации программы, о её глобальном размещении и функционале.[32]





[31] http://top.rbc.ru/politics/12/08/2013/869734.shtmlhttp://top.rbc.ru/politics/12/08/2013/869734.shtml Э.Сноуден: Сервер-шпион американских спецслужб находится в Москве

[32] http://www.slideshare.net/xkeyscore/xkeyscore-nsa-program-presentation 18.12.2013

При этом X-Keyscore способна выявлять также гражданство иностранцев, анализируя язык, используемый в сообщениях электронной почты, перехваченных в странах Латинской Америки, особенно в Колумбии, Эквадоре, Венесуэле и Мексике. По данным журнала Der Spiegel, программа X-Keyscore также имеет возможность сохранять на протяжении нескольких дней метаданные и содержание перехваченных сообщений.[33]

Следует подчеркнуть, что «XKeyscore» выявляет гражданство иностранцев, анализируя язык, используемый в сообщениях электронной почты, перехваченной в странах Латинской Америки, особенно в Колумбии, Эквадоре, Венесуэле и Мексике[34].

С 2010 г. АНБ отслеживало международные платежи частных лиц, в том числе по пластиковым картам «Visa», и составило собственную базу данных. В 2011 г. в ней содержалось 180 млн. записей, 84% из них – по транзакциям с помощью кредитных карт. АНБ мониторило данные по транзакциям через международную банковскую систему «Swift» и шпионило за держателями кредитных карт в Европе, на Ближнем Востоке и в Африке.

Кроме того, с 2006 г. АНБ получило доступ к внутренним коммуникациям трех крупнейших мировых авиакомпаний, в том числе и к системе бронирования российской компании «Аэрофлот». И, наконец, американские спецслужбы и ведомства осуществляли слежку за арабским телеканалом «Al Jazeera» и другими СМИ.

ИКТ – гиганты на «спецслужбе» США

Благодаря умышленно заложенным в поставляемое программное обеспечение «лазейкам» АНБ способно взломать любую систему его защиты, созданную американскими ИКТ-компаниями. Так, компания «Microsoft» в течение последних трех лет предоставляла доступ американским спецслужбам к сообщениям пользователей и возможность обходить

[33] German Intelligence Agencies Used NSA Spying Program — SPIEGEL ONLINE 18.12.2013
[34] O Globo от 6 июля 2013 г.

собственную криптографическую защиту для перехвата писем и чатов почтового клиента «Outlook».

С 2013 г. «Microsoft» сотрудничала с ФБР с тем, чтобы облегчить АНБ доступ через программу «Prism» к облачному хранилищу файлов «SkyDrive» (им пользуется более 300 млн. чел).

Данные, полученные программой «Prism», направлялись также в ФБР и ЦРУ. При этом число прослушиваний «Skype» возросло в три раза, начиная с июля 2012 г., то есть через 9 месяцев после того, как компания «Microsoft» купила «Skype»[35].

Компания «Verizon» по требованию американского суда предоставляла АНБ данные (местоположение звонившего, телефонные номера абонентов, длительность разговора) о телефонных переговорах американских граждан[36].

Характерно, что спецслужбы США используют сверхмощные компьютеры для взлома кодов и сотрудничают с некоторыми технологическими компаниями в США и за рубежом для создания своей «точки входа» в их продукты[37]. Так, проект «Bullrun» позволяет АНБ заниматься криптоанализом. При этом возможности США по декодированию известны лишь ограниченному кругу ведущих аналитиков из государств, объединения «Пять глаз» (на сами эти страны программа «Bullrun» не распространяется).

Великобритания - главный «спецпартнер» США

Британский Центр правительственной связи (ЦПС) – главный партнер спецслужб США. В рамках секретной программы «Tempora» ЦПС тесно сотрудничал с такими компаниями, как «British Telecom», «Vodafone Cable», «Global Crossing», «Verizon Business», «Level 3», «Viatel» и «Interut»[38].

[35] The Guardian от 12 июля 2013 г.
[36] The Guardian от 6 июня 2013 г.
[37] O Globo от 6 июля 2013 г.
[38] The Guardian от 21 июня 2013 г.

Компании предоставляли спецслужбам неограниченный доступ к оптоволоконным кабелям, по которым передаются данные о содержании телефонных переговоров, электронных писем и сообщений в социальной сети «Facebook» своих пользователей. В качестве компенсации им выплачивались денежные средства для поддержания своих сетей в исправном состоянии (394 млн.дол. - в 2011 г., 278 млн.дол. - в 2013 г.). Эти деньги выделялись на программы по сбору данных «Fairview» (94 млн.дол.), «Blarney» (65 млн.дол), «Stormbrew» (46 млн.дол.), «Oakstar» (9 млн.дол.).

Информация хранилась на серверах ЦПС в течение 30 дней, а длительность работы самой программы составила как минимум 20 месяцев. Спецслужбы ежедневно получали в свое распоряжение свыше 600 млн. телефонных переговоров, имели доступ к 200 оптоволоконным кабелям, соединяющим Европу и Америку, с пропускной способностью до 10 гигабайт в секунду (контролируя одновременно до 46 кабелей). За это время была собрана информация о 2 млрд. пользователях сети Интернет. ЦПС инвестировала программы, позволяющие получать личную информацию из мобильных телефонов и приложений. Анализ показывает, что ШКПС превосходит АНБ по количеству отслеживаемой информации.

Характерно, что за период с 2010 г. США выплатили ЦПС около 160 млн.дол. за возможность получать доступ к британским разведывательным программам и влиять на них[39]. При этом АНБ оплачивает половину стоимости одной из разведывательных систем Великобритании, расположенных на Кипре[40].

Резюмируя, следует отметить, что ЦПС тесно сотрудничает с АНБ для обеспечения британских и американских военных проведения спецкибероперациий. При этом ШКПС становится все более финансово зависимой от американских источников: с 2006 г. по 2012 г. внешние дотации выросли с 23 млн.дол. до 244 млн.дол.[41]

[39] The Guardian от 1 августа 2013 г.
[40] The Guardian от 2 августа 2013 г.
[41] The Guardian от 2 августа 2013 г.

Дилемма Германии – спецпартнер и спецобъект мониторинга США

Согласно документам Der Spiegel, немецкие спецслужбы BND (внешняя разведка) и BfV (контрразведка) получили возможность использовать X-Keyscore.[42] В этих документах BND была охарактеризована как один из самых успешных партнёров АНБ в сборе информации. Из примерно 500 млн файлов, ежемесячно получаемых АНБ от коллег из ФРГ, порядка 180 млн оказывались в доступе спецслужбы благодаря X-Keyscore[43].

Объем потока информационных данных, проходящих через один из крупнейших мировых узлов интернет-траффика во Франкфурте-на-Майне, достигал 2,5 терабайтов в секунду.

Офисы «Yahoo» в Германии, как и ирландские офисы «Apple», «Facebook», «Microsoft» и «Skype» в Люксембурге и позволяли спецслужбам США с помощью программы «Prism» беспрепятственный доступ к персональной информации граждан ЕС[44]. При этом США следили за немецкими компаниями в интересах американской промышленности. Ежегодный ущерб от американской прослушки оценивается от 30 до 60 млрд.евро.

В ответ на американскую «киберэкспансию» в июле 2013 г. канцлер ФРГ А.Меркель предложила выработать по линии ЕС стратегию развития информационных технологий. На саммите ЕС главы государств и правительств 28 европейских стран приняли специальное заявление, в котором выразили озабоченность действиями США[45].

Германия и Франция выступили с инициативой вступить в двусторонние переговоры с США с целью решения проблемы

[42] http://top.rbc.ru/society/21/07/2013/866925.shtml СМИ: Разведка ФРГ применяла шпионскую программу АНБ 18.12.2013
[43] Der Spiegel от 20 июля 2013 г.
[44] Der Spiegel от 10 июня 2013 г.
[45] Interfax от 25 октября 2013 г.

прослушивания телефонных переговоров путем заключения с Вашингтоном некого "пакта о недопустимости слежки" друг за другом.[46]

К 2018 г. ФРГ планирует увеличить число сотрудников в отделе технической разведки и технического переоснащения БНД, вложив в нее 100 млн.евро. При этом правительство ФРГ аннулировало 2 августа 2013 г. так называемые административные соглашения от 1968/1969 гг. с США и Великобританией.

В МИД ФРГ летом 2013 г. был введен пост уполномоченного по вопросам информационной безопасности. Его занял 57-летний дипломат Дирк Бренгельман, главной задачей которого определено обеспечение защиты информационных сетей и свободы в Интернете.

Характерно, что 28 августа 2013 г. по инициативе Федерального ведомства по охране конституции полиция ФРГ произвела в разведывательных целях воздушную съемку здания Генерального консульства США во Франкфурте-на-Майне, а также прилегающей к нему территории, так как именно через этот узел американские спецслужбы перехватывали наибольшее количество информации.

Латинская Америка – «кибервотчина» США

АНБ имело доступ к миллиардам электронных писем и телефонных звонков, проходивших через территорию стран Латинской Америки. Особое значение придавалось Бразилии. Под прикрытием сотрудничества американских и бразильских телекоммуникационных компаний (в т.ч. местное подразделение «Google», отделение бельгийской компании «Swift»)[47]АНБ следило за деятельностью крупных частных и государственных компаний, в том числе «Petrobraz», по таким стратегически важным вопросам, как организация тендеров, разработка нефтяных месторождений, проекты в оборонной сфере.

[46] BBC от 25 октября 2013 г.
[47] TV Globo от 9 сентября 2013 г.

Участник системы «Эшелон» Канадский Центр безопасности коммуникаций совместно со спецслужбами США участвовал в шпионаже против Министерства горнодобывающей промышленности и энергетики Бразилии. Шпионаж осуществлялся с помощью компьютерной программы «Олимпия» в интересах частных компаний[48]. Канадские спецслужбы интересовались схемами коммуникаций министерства, перехватывая телефонные разговоры, переговоры и электронную переписку чиновников, а также самого министра. Отчет о результатах проделанной работы был представлен Канадой в июне 2012 г. на закрытой конференции представителей государств – членов объединения спецслужб «Эшелон» («Пять глаз»).

Комиссия сената Бразилии по расследованию фактов шпионажа спецслужб США заслушала проживающего в Бразилии американского журналиста Г.Гринвальда. Именно ему в свое время Э.Сноуден передал разоблачительные документы. Публикации в СМИ на основе этих документов вскрыли факты слежки спецслужб за телефонными переговорами и электронной перепиской президента Бразилии Дилмы Роуссефф, бразильских дипломатов, сотрудников стратегически важных министерств и компаний южноамериканской страны.

Разоблачительные материалы о деятельности американских спецслужб против Бразилии стали причиной охлаждения в отношениях между двумя странами. Глава бразильского государства с трибуны Генассамблеи ООН выступила с резким осуждением подобной шпионской деятельности. Бразилия выдвинула инициативу создать механизмы гражданского контроля над интернетом с целью обеспечить безопасность его пользователей, не ограничивая их права на свободный доступ к ресурсам мировой сети.

В открытом письме Сноудена, адресованном народу и властям Бразилии, он отмечает, что был впечатлен резкой критикой деятельности американских спецслужб и шпионажа со стороны США, а также выразил

[48] Toronto Star от 7 октября 2013 г.

готовность помочь Бразилии расследовать слежку АНБ в обмен на политическое убежище.[49]

Бразилия предприняла шаги для снижения зависимости от американских интернет-компаний и сервисов, т.е. укреплению информационного суверенитета. Принято решение о развитии национальной системы электронной почты (с планами стать сервером автономной региональной сети), укреплении безопасности правительственной связи, реформе национального законодательства – введении обязательного правила хранения электронных баз данных на территории страны, отзыве лицензий у компаний, уличенных в пособничестве кибершпионажу.

Намечено ужесточить контроль над использованием зарубежного технического оборудования, исключить применение несертифицированных элементов, увеличить ответственность операторов и технического персонала, минимизировать закупки американских комплектующих и элементной базы для наиболее важных информационных систем.

В 2014 г. предусматривается создание Центра контроля трафика сети Интернет в г.Форталеза. В 2014-2015 гг. правительство намерено осуществить запуск национального спутника связи, и проложить две оптоволоконные линии коммуникаций (одна для связи со странами Карибского бассейна и некоторыми европейскими государствами, а вторая – со странами Африки).

Тема международной информационной безопасности (МИБ) стала приоритетной для Бразилии. Бразилия намерена углубить дебаты по вопросам управления сетью интернет и активизировать деятельность рабочей группы, созданной в соответствии с резолюцией 67/195 в рамках Комиссии по науке и технике в целях развития.

[49] http://ria.ru/world/20131217/984619539.html#ixzz2nnVXU6I8

13 сентября 2013 г. министры обороны Бразилии и Аргентины подписали соглашение о совместных шагах по противодействию кибершпионажу со стороны США.

Эквадор на полях текущей сессии Совета ООН по правам человека провел встречу, посвященную «разоблачителям» нарушений прав человека и связанным с этим правовым и нравственным проблемам, на которой виртуально присутствовал и основатель «Wikileaks» Дж.Ассанж.

Особая роль Франции

АНБ вело широкомасштабную слежку за Францией. Только за период с 10 декабря 2012 г. по 8 января 2013 г. АНБ перехватило 70,3 млн. телефонных разговоров французских граждан, представителей политической и деловой элиты страны, сотрудников министерств и ведомств. Также перехватывалась электронная переписка пользователей, которая обрабатывалась компаниями «Wanadoo» и «Alcatel-Lucent»[50].

Особая роль Франции заключается в том, что она создала и использует собственную систему Frenchelon - аналог PRISM. (на слайде).[51]

[50] Le Monde от 21 октября 2013 г.
[51] Le Monde от 4 июля 2013 г.

Другие «спецобъекты» США

Швеция является одним из секретных партнеров АНБ США и тесно сотрудничает с США и Великобританией в деле тотальной прослушки. Радиокоммуникационная служба шведской обороны (FRA) снимает информацию с подводных кабелей, осуществляя слежку за странами Балтии и за российскими фирмами и передавая информацию АНБ.

Зафиксировано 9 случаев несанкционированного или необоснованного сбора, хранения, обработки и воссоздания чувствительной или неоправданно подробной информации, в том числе о физических лицах, недопустимого использования поисковых понятий, недостаточной отчетности и ведения документации, затрудняющей контроль.

Индия. С помощью программ «Boundless Informant» и «Prism» американские спецслужбы осуществляли слежку за Индией, перехватывая информацию о внутренней политике, стратегических и коммерческих интересах страны, ее ядерной и космической программах и т.д. АНБ наблюдало за государственными учреждениями страны и чиновниками различного уровня, учеными и другими лицами, представляющими интерес для США. Слежка велась за индийской миссией ООН в Нью-Йорке и Посольством Индии в Вашингтоне.

Следует отметить, что у Индии имеется Национальная разведывательная сеть NATGRID (акроним англ. National Intelligence Grid), которая консолидирует базы данных нескольких министерств и ведомств, для облегчения спецслужбам Индии оперативного доступа к требуемой информации. Идея создания NATGRID возникла после терактов в Мумбаи в 2008 г.[52]

Италия. Британские и американские разведывательные службы в массовом порядке ведут мониторинг телефонных сообщений, в том числе военного и коммерческого характера, и интернет-трафика в Италии.[53]

---

[52] http://ru.wikipedia.org/wiki/NATGRID
[53] Espresso от 24 октября 2013 г.

Нидерланды. В декабре 2012 - январе 2013 гг. в рамках программы «Boundless Informant» АНБ прослушало телефоны около 2 млн. граждан.[54]

Бельгия. Американские спецслужбы с 2011 г. следили за клиентами крупнейшего оператора связи Бельгии «Belgacom», перехватывая международные телефонные разговоры. В этих целях британский ЦПС (GCHQ) через фальшивые аккаунты социальной сети LinkedIn внедрил шпионскую программу в сеть бельгийского оператора.[55]

Было «заражено» 25 тысяч компьютеров компании. Больше всего США интересовались подразделением «Belgacom» - «Bics», которое обеспечивало международную связь по всему миру, отслеживались контакты с Йеменом, Сирией, Афганистаном, Анголой, Демократической Республикой Конго и еще рядом стран, к которым разведка США проявляет особый интерес[56].

В силу этого Министр иностранных дел Бельгии Д.Рейндерс и внес предложение о приостановке процесса подписания документа о трансатлантическом сотрудничестве по вопросам торговли и инвестиций с США до выяснения всех обстоятельств дела.

Израиль. США делятся с израильскими разведывательными службами необработанными разведданными, которые могут включать в себя конфиденциальную информацию об американских гражданах. Об этом стало известно из «Меморандума о взаимопонимании», заключенного между АНБ и его израильским аналогом[57].

Следует подчеркнуть, что боевой кибервирус «Stuxnet», поразивший компьютеры на иранской АЭС в Бушере, был разработан США совместно с Израилем[58].

Китай. АНБ проникло на серверы китайских мобильных телефонных компаний и читало миллионы текстовых сообщений. АНБ взломало десятки компьютеров в престижном университете Циньхуа в

[54] Dutch news от 21 октября 2013 г.
[55] http://www.interfax.ru/world/txt/341907 18.12.2013
[56] De Standaard от 16 сентября 2013 г.
[57] Los Angeles Times от 11 сентября 2013 г.
[58] The Register от 8 июля 2013 г.

Пекине и компьютеры «Pacnet» – крупнейшей телекоммуникационной компании со штаб-квартирами в Гонконге и Сингапуре. Учитывая это обстоятельство, КНР создала систему защиты «Золотой щит».[59]

Пакистан. Спецслужбы США осуществляли компьютерную слежку за Пакистаном, в частности, за программой пакистанского ядерного оружия. [60]

Характерно, что американский спецназ, участвовавший в операции по ликвидации Усамы бен Ладена, получал команды со спутников, которые передавали сигнал через специальные приемники, находившиеся на территории Пакистана[61].

Австралия. АНБ сотрудничало с Управлением радиотехнической обороны Австралии и Службой безопасности правительственных коммуникаций Новой Зеландии для реализации программы «XKeyscore»[62].

Австралийская компания «Telstra» сотрудничала с правительством США, храня информацию о звонках, совершенных между США и другими странами. Соглашение было подписано в 2001 г. и, по сути, давало компании возможность отслеживать содержание разговоров абонентов[63].

Норвегия. По данным газеты Dagbladet со ссылкой на документы, обнародованные Э. Сноуденом,[64] за период с 10 декабря 2012 г. до 8 января 2013 г. АНБ перехватило на территории страны 33 млн звонков, что составляет 10% от всего трафика мобильной связи в Норвегии. Таким образом, Норвегия оказалась страной, в которой американцы отследили наибольшее количество данных в соотношении с количеством жителей.

Следует отметить, что все три спецслужбы Норвегии на следующий день после публикации отклонили утверждения газеты. [65]

---

[59] The South China Morning Post от 11 сентября 2013 г.
[60] The Washington Post от 2 сентября 2013 г.
[61] The Washington Post от 29 августа 2013 г.
[62] The Sydney Morning Herald от 8 июля 2013 г.
[63] The Guardian от 12 июля 2013 г.
[64] Dagbladet 19.11.2013
[65] http://www.interfax.ru/world/txt/341907

Международное сообщество за неприкосновенность личной жизни в цифровой век

С учетом волны возмущения противоправной деятельностью спецслужб США Германия и Бразилия в конце октября 2013 г. обратились в ООН с инициативой обсуждения проекта резолюции, которая на межгосударственном уровне распространила бы на Интернет право на невмешательство в частную жизнь, закрепленное в Международном пакте о политических и гражданских правах.

26 октября 2013 г. Третий комитет Генеральной ассамблеи ООН, рассматривающий права человека, единогласно принял резолюцию "Право на неприкосновенность личной жизни в цифровой век", направленную против незаконной слежки за электронными коммуникациями.

Генассамблея подтвердила, что **те же права, которые человек имеет в офлайновой среде, должны также защищаться и в онлайновой среде, особенно право на неприкосновенность личной жизни.**

Кроме того, в документе содержится призыв Генассамблеи к государствам "провести обзор процедур, практики и законодательства, касающихся слежки за сообщениями, их перехвата и сбора личных данных". Также в принятой резолюции есть призыв к Верховному комиссару ООН по правам человека подготовить доклад о защите права на неприкосновенность личной жизни. [66]

Продажа кибероружия будет сокращена

Правительства 41 страны, подписавшей Вассенарские соглашения (США, Великобритании, России и большинства стран ЕС), намерены ограничить продажи систем слежения за интернет-трафиком, а также средств программного вторжения, которые обычно используют спецслужбы. Под действие соглашения подпадает любое программное обеспечение для сбора

[66] https://www.un.org/russian/news/story.asp?NewsID=20669 18.12.2013

метаданных.[67] Ограничивается и продажа программ для отслеживания действий пользователей в Интернете. Участники соглашения признали, что необходимо усилить контроль над программами, позволяющими «определять схемы отношений отдельных людей и групп». Исключение делается для компаний, использующих эти технологии для маркетинга или изучения поведения потребителей.

Жесткие ограничения накладываются также на распространение определенных типов вредоносного софта, особенно способного причинить ущерб компьютерам, сетям или оборудованию, управляемому с компьютера.

Западные спецслужбы особенно озабочены возможностью попадания потенциально опасных технологий в руки террористов и боевиков. Великобритания с будущего года вводит правила, обязывающие все компании, ведущие бизнес с правительством, обеспечить соблюдение стандартов кибербезопасности во всех цепочках субподрядчиков. В декабре 2013 г. премьер-министр Великобритании Д. Кэмерон во время своего визита в Китай (не подписавший Вассенарские соглашения) сообщил о возможном начале переговоров между двумя странами по кибербезопасности.

Инструменты наблюдения, средства вторжения и технологии для защиты от них активно разрабатываются частными компаниями разных стран мира. По оценке британского Агентства по торговле и инвестициям (UKTI), оборот мирового рынка средств кибербезопасности составляет 123 млрд фунтов стерлингов ($201 млрд) и растет ежегодно на 10%.

Позиция России

Россия в течение последнего десятилетия последовательно и прагматично выстраивает отношения с мировым сообществом в области МИБ, направленные на консолидацию усилий в противодействии угрозам в информационной сфере.

---

[67] http://www.vedomosti.ru/tech/news/20286881/prism-priznali-kiberoruzhiem#ixzz2nl3npzQy 17.12.2013

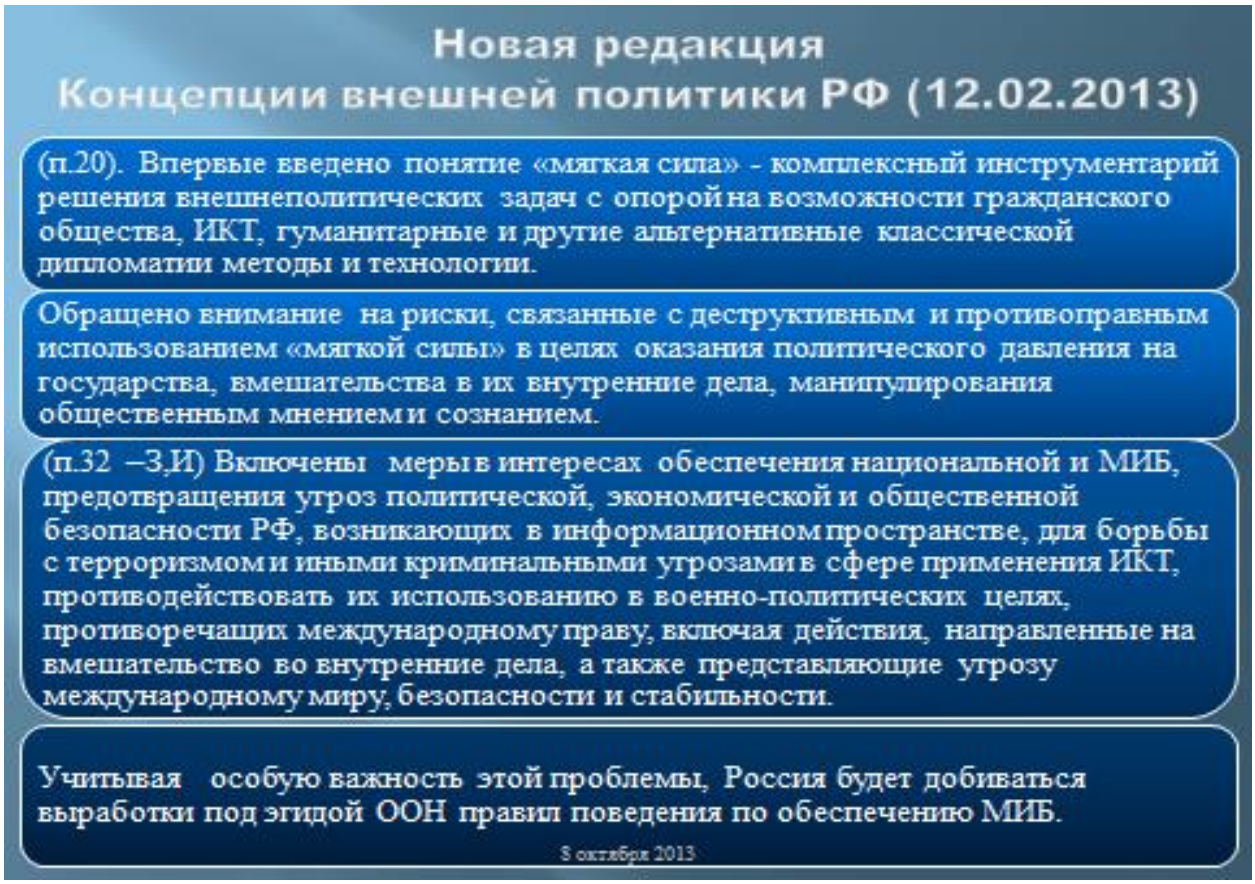
В октябре 2012 г., т.е. еще до разоблачений Э.Сноудена, исследователи из "Лаборатории Касперского" обнаружили кибервирус, нацеленный на компьютерные системы многих правительственных учреждений, включая посольства, ядерные исследовательские центры и предприятия нефтяной и газовой промышленности. Главной мишенью вируса были страны Восточной Европы, бывшие советские республики и страны Центральной Азии, хотя ее жертвы могли находиться и в любом другом месте, включая Западную Европу и Северную Америку.[68]

Программа могла похищать зашифрованные файлы и даже восстанавливать информацию, стертую с жесткого диска или флэшки.

В силу этого президентом России 15 января 2013 г. был издан соответствующий секретный указ Президента России (на слайде).

[68] http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide 18.12.2013

Позиция России по проблематике использования ИКТ и МИБ нашла отражение в новой редакции Концепции внешней политики России (на слайде).



В рамках саммита G8 в Сев. Ирландии (Лох-Эрн, 17.06. 2013 г.) президенты РФ и США приняли совместное заявление, в котором отметили понимание угроз в сфере использования ИКТ: военно-политического, криминального и террористического характера и объявили о заключении трех «прорывных» договоренностей по системе мер доверия между РФ и США. Однако, в связи с переносом визита Б.Абамы в Москву после саммита G20, были перенесены и ряд рабочих встреч по реализации договоренностей.

Тем не менее, Президентом Российской Федерации 24 июля 2013 г. Пр-1753 были утверждены «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года». К числу основных приоритетов отнесено участие России в формировании механизмов международного сотрудничества в

области противодействия угрозам использования ИКТ в террористических и экстремистских целях, в том числе для вмешательства во внутренние дела суверенных государств.

В целом Основы закрепляют стремление Российской Федерации к масштабному сотрудничеству в деле укрепления мер доверия в сфере применения ИКТ и повышения эффективности переговорного процесса в области формирования системы международной информационной безопасности.

Реализуя Основы, Россия внесла в повестку дня 68 сессии Генассамблеи ООН проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», который был консенсусом принят 6 ноября 2013 г.

В 2013 году достигнуто рекордное число соавторов российской резолюции - более 40 стран. Коспонсорство документа приобретает подлинно глобальный характер, охватывая все регионы мира, включая страны БРИКС, ШОС, СНГ, а также ключевые латиноамериканские и азиатские государства.[69]

Кроме того, Россия стала одним из инициаторов принятия Решения Постсоветом ОБСЕ от 3 декабря 2013 г. № 1106: «Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью снижения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий».

Косметические реформы разведсообщества США

20 января 2014 г. президент Барак Обама объявил о давно ожидавшихся реформах разведсообщества. Некоторые из мер предназначены к немедленной реализации, другие потребуют проработки и одобрения Конгресса. Основной смысл речи сводился к тому, что массовый сбор данных об американцах продолжится, однако доступ спецслужб к этой

[69] http://www.mid.ru/brp_4.nsf/newsline/9C738EC38849040244257C1D004302B7 18.12.2013

информации значительно ограничат. Обама пообещал не шпионить за главами дружественных государств и правительств. Перемены оказались косметическими. [70]

АНБ предписано обращаться за разрешением в Суд по вопросам надзора за иностранными разведками (СНИР), чтобы получить доступ к телефонным записям сотен миллионов американцев (за исключением экстренных случаев).

В перспективе Обама намерен передать функции сбора и хранения сведений от спецслужб некоему независимому, не подконтрольному властям консорциуму. План того, как это нужно сделать, представят генеральный прокурор и разведсообщество.

Ограничен круг американцев, к звонкам которых могут иметь доступ спецслужбы. Снимается и запрет на неразглашение банками и телефонными компаниями полученных от спецслужб писем с запросом информации. Одно из самых популистских изменений – создание группы адвокатов, которые смогут защищать частные и гражданские свободы в СНИР.

Тон выступления Обамы не оставил сомнений в том, что он пошел на уступки разведслужбам и попытался оправдать существующий порядок. Недаром ему аплодировали ярые защитники программ АНБ в Конгрессе.

Данным подходом недовольны правозащитники. По мнению создателя WikiLeaks Джулиана Ассанджа, речь Обамы была лишена конкретики и существенно положение дел не изменит. "Все, что мы видим, – это перебрасывание мяча на поле Конгресса и адвокатских групп", – сказал он. Ассандж не мог не вспомнить об Эдварде Сноудене, с подачи которого в США и созрел протест против массовой слежки.

Президент США обещал не шпионить за "близкими друзьями и союзниками", имея в виду глав дружественных государств и правительств. С другой стороны, список "друзей" не публикуется.

[70] http://www.centrasia.ru/newsA.php?st=1390191840 23.1.2014

Реакции официальных лиц в, т.ч. в Берлине, были сдержанными. Критичнее выступили журналисты. Бравший у Обамы интервью Клаус Клебер заявил: немцы отнеслись к речи Обамы скептически и осторожно, многие были разочарованы ею, даже те, кто считает себя настроенным проамерикански. Так, журнал Spiegel обвинил АНБ за превращение Интернета в систему вооружения.[71]

Между тем наделала шума статья, размещенная на американском сайте BuzzFeed. Она отражает **настроения в отношении Сноудена в военно-разведывательной среде, которые сводятся к доходящему до извращения желанию убить его.**

В этих условиях понятно редкое прямое интервью Э.Сноудена журналу The New Yorker,[72] в котором он выразил уверенность, что его действия за прошедшие девять месяцев не повлекли за собой каких-либо угроз национальной безопасности США. По его словам, сам президент Обама отмечал, что дискуссия, начатая раскрытием сведений об АНБ, укрепит Америку. По словам американского президента, все последствия слива информации будут очевидны еще лишь «годы спустя».

Однако ждать пришлось недолго. 22 января 2014 г. в обстановке строжайшей секретности Эдвард Сноуден дал в Москве телеинтервью немецкому телеканалу NDR.[73]

В своем интервью Сноуден подчеркнул, что передал журналистам всю информацию, и сам ею уже не владеет. Вместе с тем в ходе беседы экс-сотрудник ЦРУ раскрыл некоторые тонкости и нюансы уже известных фактов.

Так, по его мнению, нельзя исключать, что АНБ могло прослушивать не только мобильный телефон канцлера Ангелы Меркель, но и шпионить за другими членами правительства ФРГ. Так или иначе, подытожил Эдвард, миллионы данных граждан ФРГ оказываются в распоряжении АНБ.

---

[71] http://www.centrasia.ru/newsA.php?st=1390191840 23.1.2014
[72] http://inotv.rt.com/2014-01-22/Snouden-Ostavit-menya-v-Rossii 23.01.2014
[73] http://www.rg.ru/printable/2014/01/27/snouden-site.html 27.01.2014

Кроме того, **Сноуден обвинил АНБ и в экономическом шпионаже**. У него имеется достоверная информация, доказывающая, что если немецкий электротехнический концерн Siemens располагает информацией, которая важна для национальных интересов США, но не имеет ничего общего с вопросами национальной безопасности, то такая информация все равно используется американской стороной.

В своем интервью Сноуден особо подчеркнул, что всегда действовал в одиночку и не заключал сделок с другими государствами в обмен на политическое убежище…

Действительно, «Snowdengate» еще далеко не завершен… А пока будем предельно бдительны и внимательны при использовании ИКТ!