УДК 327.84

# «УОТЕРГЕЙТ 2.0»: РАЗОБЛАЧЕНИЯ ТЕХНОЛОГИЙ АНБ США

© 2014 г. **П.А. Шариков**[*]
*Институт США и Канады РАН, Москва*

*Летом 2013 г. весь мир был шокирован откровениями бывшего сотрудника американского Агентства национальной безопасности Эдварда Сноудена о технологиях, которые применяет АНБ для доступа к конфиденциальной информации клиентов ведущих мировых интернет-провайдеров. Разоблачения спровоцировали серьёзные международные последствия, а также внутриполитические волнения, прокатившиеся по Соединённым Штатам.*

**Ключевые слова**: *Информационная революция, нарушение конфиденциальности, Интернет, АНБ.*

Регулирование деятельности средств массовой информации стало одним из актуальных направлений деятельности американской государственной власти ещё в период после завершения Войны за независимость. Учитывая специфику американской истории конца XVIII – начала XIX веков, основным направлением в данной области было противодействие антиправительственной деятельности. В 1798 г., во многом из-за угрозы начала войны с Францией, в Соединённых Штатах был принят закон «О подстрекательстве к мятежу» [28], который устанавливал уголовное наказание за публичную критику федерального правительства. Практика преследования за подстрекающие к мятежу пасквили времён первых колонизаторов быстро укоренилась на американской почве. На протяжении XVII–XVIII веков критиков правительства наказывали либо по решениям судов, либо по принятым законодательным актам. Даже после окончания Войны за независимость суды отдельных штатов продолжали применять эти законы. Но пресса в большинстве случаев просто игнорировала их. Так продолжалось до тех пор, пока Конгресс не принял вышеупомянутый закон 1798 г., по которому критика федерального правительства стала приравниваться к попытке мятежа и считаться уголовным преступлением [1]. По другой версии причиной принятия данного закона явилась разворачивавшаяся в тот период борьба между республиканцами и федералистами. Закон был принят при втором президенте США, федералисте Дж. Адамсе, а спустя три года, когда к власти пришёл Т. Джефферсон, все осуждённые по этому

[*] **ШАРИКОВ Павел Александрович – кандидат политических наук, руководитель Центра прикладных исследований Института США и Канады РАН.** E-mail: pasha.sharikov@gmail.com

Работа выполнена при поддержке гранта Президента Российской Федерации для государственной поддержки молодых российских учёных – кандидатов наук № МК-189.2013.6

закону лица были помилованы. Президент Джефферсон считал, что данный закон противоречит первой поправке к американской конституции [4] (гарантирующей свободу слова и печати).

Верховный суд США признал неконституционным закон «О подстрекательстве к мятежу» лишь в 1964 г., в связи с делом «"Нью-Йорк таймс" против Салливана»*. Решение суда было вынесено в пользу «Нью-Йорк таймс», а это судебное разбирательство стало одним из основных прецедентов, относящихся к свободе прессы. Верховный суд назвал закон «О подстрекательстве к мятежу» (1798 г.) неконституционным. «По словам судьи Бреннана, это было историческое решение. Возвращение правительством сумм штрафов, уплаченных по этому закону обвиняемыми, помилование осуждённых по этому закону президентом Джефферсоном, суждения, высказанные судьями Верховного суда прошлых лет – всё это наглядно показывало, что понятие подстрекающего к мятежу пасквиля просто «несовместимо с Первой поправкой» Конституции США» [7].

Данное решение Верховного суда Соединённых Штатов действительно носило исторический характер. Благодаря ему американские СМИ получили возможность активно критиковать действия властей. Как представляется, уже принятие данной нормы послужило предпосылкой для двух крупнейших событий в истории развития журналистики и свободы слова в США (ими стали «Бумаги Пентагона» [25] и «Уотергейт»).

Современная ситуация, складывающаяся вокруг реакции на разоблачения бывшего сотрудника Агентства национальной безопасности США Эдварда Сноудена (*Edward Snowden*), напоминает Уотергейтский скандал, потрясший США 40 с лишним лет назад. В то время серьёзного внутриполитического кризиса президент Р. Никсон вёл предвыборную кампанию с целью своего переизбрания на второй президентский срок. Для получения информации о планах политических противников по личному указанию Никсона была проведена секретная операция по установке подслушивающей аппаратуры в штаб-квартире Демократической партии в столичном административно-гостиничном комплексе «Уотергейт». Последняя попытка установки «жучков» была по чистой случайности сорвана ночным сторожем комплекса, в результате чего участники операции были задержаны с поличным [4].

Американское общество было шокировано самим фактом подобной деятельности со стороны правительства.

Авторитетнейшая газета «Вашингтон пост», поручила Б. Вудварду и К. Бернштайну написать статью про взлом штаб-квартиры Демократической

* 29 марта 1960 г. одна из крупнейших американских ежедневных газет «Нью-Йорк таймс» опубликовала статью под названием *Heed their rising voices* («Прислушайтесь к их всё более громким голосам»), в которой говорилось, что полиция штата Алабама арестовывала М.Л. Кинга 7 раз. Несмотря на то, что представитель полиции Алабамы, одного из наиболее прореспубликански настроенных штатов Юга США, Л.Б. Салливан не упоминался в статье, неправомерные действия в отношении чернокожего борца за права человека вменялись именно ему. Согласно записям, М.Л. Кинг арестовывался 4 раза, что послужило причиной возбуждения уголовного дела Салливана против редакции газеты. «Нью-Йорк таймс» не стала публиковать опровержение, несмотря на письменное обращение Салливана.

партии. Серия их статей, последовавшая после инцидента 17 июня 1972 г., стала журналистским расследованием, за которым последовало судебное разбирательство.

Публикации «Вашингтон пост», ставшие возможными после окончательной отмены закона «О подстрекательстве к мятежу», спровоцировали не только мощнейший общественный резонанс, но и поставили вопрос об импичменте президенту Р. Никсону. Несколько высокопоставленных сотрудников Белого дома были обвинены в противозаконной деятельности, а сам президент был вынужден подать в отставку, создав, таким образом, первый и на сегодняшний день единственный прецедент в американской истории.

Заголовок газеты «Вашингтон пост» 9 августа 1974 г. гласил *Nixon resigns* («Никсон уходит в отставку»), а журналисты впоследствии опубликовали бестселлер «Вся президентская рать» [11]. Авторы политического детектива, получившего Пулитцеровскую премию, поведали о ходе своего расследования, сыгравшего решающую роль в исторической отставке президента Соединённых Штатов.

В середине 1970-х годов, после произошедших утечек, сенатор Фрэнк Чёрч выступил с инициативой создания в Сенате США специального комитета, работа которого была бы сосредоточена вокруг оценки деятельности специальных служб и разработки законодательного обоснования для деятельности. Результаты работы комитета Чёрча легли в основу разработки законодательства об иностранной разведке во второй половине 1970-х годов.

Стоит отметить, что в культуре Соединённых Штатов существует такое понятие, как «*whistleblower*» («правдолюбец» – свистящий в свисток)[*]. Безусловно, особое внимание «искателей правды» всегда привлекала деятельность американских специальных служб. В 1998 г. американский Конгресс принял закон о защите уислблоуеров, в котором говорилось, что сотрудники ЦРУ, желающие сделать достоянием общественности какие-либо нарушения разведывательного управления, обязаны действовать через Конгресс [15].

Все упомянутые события стали заметными вехами в истории американского политического развития. Как представляется, «Уотергейт», дело «Викиликс», «дело Эдварда Сноудена» и тому подобные инциденты обострили многие проблемы американского общества, остающиеся актуальными едва ли не с колониальных времён. К этим проблемам относятся полномочия разведывательных органов федерального правительства, государственная информационная политика, свобода прессы, ответственность исполнительной власти перед гражданским обществом.

В условиях информационной революции, распространения Интернета и новейших информационных технологий в американском обществе заметным изменениям были подвержены инструменты деятельности специальных служб относительно доступа к конфиденциальной информации граждан. В этой связи, особый интерес представляют так называемые «технологии 2.0», получив-

[*] Так называют людей, делающих общественным достоянием секретную информацию о противозаконной, аморальной или общественно вредной деятельности какой-либо организации. Перевести на русский язык это слово невозможно, в данной работе они будут называться уислблоуеры.

шие особенно активное развитие в настоящее время. Понятие *Web 2.0* появилось задолго до того, как было придумано конкретное определение. Один из идеологов «технологий 2.0» Тим О'Рейли в 2005 г. определил *Web 2.0* как «методику создания систем, которые с помощью учёта сетевых взаимодействий становятся тем лучше, чем больше людей ими пользуются. Особенностью *Web* 2.0 является принцип привлечения пользователей к наполнению и многократной выверке информационного материала» [6]. Бизнес-модель *Web 2.0* доказала свою эффективность. Именно благодаря использованию данной схемы привлечения новых пользователей в начале XX века в Соединённых Штатах сформировался рынок телекоммуникационных услуг. Для этого рынка характерно существование нескольких монополий, которые собирают в своих сетях до 100% всей информации, передаваемой американскими гражданами посредством Интернета.

Следующий крупный скандал, связанный с утечкой заметного объёма информации о деятельности правительства произошёл в 2010 г. Скандал, связанный с сайтом «Викиликс», как представляется, был вызван резким наращиванием разведывательного потенциала американских спецслужб, предпринятым после колоссального провала американской разведки с целью противодействия террористическим организациям после сентября 2001 г.

Развитие Интернета и всемирной информационной сети, активизация террористической деятельности, направленной против Соединённых Штатов, заставили администрацию Дж. Буша-мл. пересмотреть приоритеты в области обеспечения национальной безопасности США. После трагедии 11 сентября 2001 г., администрация Дж. Буша-младшего предприняла различные меры для того, чтобы подобные события не повторились.

Реформы президента Буша спровоцировали бурное обсуждение и серьёзную критику правительства по трём основным вопросам: «противоречие между обеспечением национальной безопасности и гражданскими свободами, в первую очередь связанное с вмешательством в частную жизнь, и свободой слова; необходимость собирать разведывательную информацию с помощью информационных коммуникационных технологий у лиц, находящихся за пределами Соединённых Штатов; взаимодействие с провайдерами информационных услуг для сбора подобной информации» [16].

Ряд крайне непопулярных мер предполагал сбор колоссального объёма информации. Согласно изменённым стандартам, к категории информации, относящейся к вопросам обеспечения национальной безопасности, стало относиться гораздо большее количество информации. Стандарты секретности также были изменены. Для работы с такими массивами информации требовались новые подходы. Ни разведка, ни Государственный департамент, ни военные не были в состоянии справиться (хранить, анализировать и работать) с такой задачей в одиночку.

Следующая беспрецедентная утечка информации о деятельности спецслужб США произошла в 2013 г. Бывший сотрудник технической службы АНБ Эдвард Сноуден раскрыл не столько факты, сколько саму технологию деятельности спецслужб. Оказалось, что в отличие от Уотергейтского скандала, государство следило не за политическими оппонентами, а фактически имело доступ к кон-

фиденциальной информации каждого пользователя Интернета, не только граждан США, но каждого клиента американских интернет-компаний.

Как представляется, масштабная деятельность американских спецслужб в области доступа к конфиденциальной информации граждан, имела ряд предпосылок, связанных, в первую очередь, с объявленной президентом Дж. Бушем-мл. в 2002 г. стратегией превентивных действий. Вместе с тем, критики реформы разведывательного сообщества выражали серьёзное беспокойство, что вменяемые специальным службам полномочия противоречат Конституции, в частности четвёртой поправке к ней.

Эта поправка гласит: «Право народа на охрану личности, жилища, бумаг и имущества от необоснованных обысков и арестов не должно нарушаться. Ни один ордер не должен выдаваться иначе, как при наличии достаточного основания, подтверждённого присягой или торжественным заявлением; при этом ордер должен содержать подробное описание места, подлежащего обыску, лиц или предметов, подлежащих аресту» [5].

Таким образом, отцы-основатели Соединённых Штатов заложили в основу конституционного строя положение о том, что в случае подозрения гражданина в противоправной деятельности, любые досудебные действия, связанные с доступом правоохранительных органов к конфиденциальной информации, возможны только при условии разрешения соответствующего органа, а именно судьи. Американским законодательством были предусмотрены и соответствующие процедуры. Спустя 200 лет после подписания Конституции, данная норма стала применяться и в отношении телефонных разговоров и электронных средств связи. Сбор конфиденциальных данных, таким образом, необходим для предоставления доказательств в суд.

Реформа разведывательного сообщества, проведённая администрацией президента Дж. Буша-мл. в рамках «Стратегии национальной безопасности 2002 г.» изменила задачи деятельности органов национальной безопасности.

Термин «превентивная оборона», придуманный министром обороны США У. Перри в середине 1990-х, подразумевал использование средств дипломатии, международно-политического воздействия на потенциальную угрозу, с тем чтобы она не превратилась в реальную. «Стратегия национальной безопасности» администрации Дж. Буша-мл. предоставляла Соединённым Штатам возможность вести военные действия против потенциальной угрозы.

Сбор конфиденциальной информации в таком случае осуществлялся не в целях предоставления доказательств в суд, а для проведения специальных, в том числе военных операций (например таких, как задержание С. Хуссейна или ликвидация У. бен Ладена). Деятельность спецслужб при этом распространялась не только на американских граждан, но на всех пользователей упомянутых Э. Сноуденом интернет-компаний.

Президент России В.В. Путин заявил, что доступ российских спецслужб к конфиденциальной информации граждан осуществляется исключительно с санкции суда и в рамках законодательства с целью дальнейшего предоставления доказательств для рассмотрения в суде. «В условиях борьбы с международным терроризмом это (то, что электронная разведка занимается контролем над гражданами. – *П.Ш.*) приобретает глобальный характер, и в целом такие

методы работы востребованы. Вопрос только в том, насколько они контролируются обществом. Ведь нельзя просто, допустим, прослушать телефонный разговор, допустим, в России – уж точно могу вам сказать – без соответствующих санкций суда» [2].

Очевидно, что при соблюдении «традиционной» юридической процедуры (разрешение судьи или прокурора), решить поставленные задачи, связанные с проведением превентивных действий в отношении подозреваемых, было бы невозможно. После принятия соответствующего законодательства «обновлённые» американские спецслужбы во главе с Агентством национальной безопасности заметно изменили характер своей деятельности и стали заниматься сбором информации, появляющейся в результате цифрового взаимодействия.

Согласно разоблачениям Эдварда Сноудена, ключевым элементом в системе сбора конфиденциальной информации об американских и иностранных гражданах является программа *PRISM*, в разработке которой, судя по всему, он принимал непосредственное участие.

В презентационных слайдах, которые были опубликованы американскими и британскими газетами, продемонстрированы масштабы и основные источники информации, которыми пользовались американские спецслужбы.

Используя программу *PRISM*, американские спецслужбы теоретически могли получать любую информацию, передаваемую клиентами таких телекоммуникационных гигантов, как «Майкрософт», «Гугл», «Фейсбук», «Эппл» (*Microsoft, Google, Facebook, Apple)* и др.

Даже не стоит упоминать, что практически каждый пользователь информационных технологий является клиентом хотя бы одной из упомянутых компаний. Все они хорошо знакомы и российским пользователям.

Безусловно, «Майкрософт» и другие вышеупомянутые компании являются американскими, однако их пользователи рассеяны по всему миру. Эти компании не имели бы такого влияния, если бы не развивались в Соединённых Штатах, где для этого государством созданы благоприятные условия. Но в настоящее время, спрос на продукцию этих компаний расширился до глобальных масштабов. Воспользоваться услугами любой американской корпорации – интернет-гиганта может любой пользователь интернета в любой точке планеты. Все компании имеют свои представительства во многих странах и городах. Пользователи «доверяют» работу с информацией этим компаниям, а в ряде случаев у них просто не остаётся иного выбора. Более того, пользователи этих сервисов получают возможность некоего их объединения, создания общих информационных ресурсов.

Существуют, разумеется, и другие сервисы, однако они менее популярны, и, как правило, несовместимы друг с другом. А из-за отсутствия «массовости» использования – информация, которая хранится и передаётся через сервера рядовых провайдеров, представляет меньший интерес для американских спецслужб. Нельзя, конечно, исключать, что АНБ имело доступ и к этим серверам, но однозначно можно утверждать, что данных, доступных с серверов упомянутых выше интернет-гигантов было более чем достаточно для «тотальной осведомлённости». Если допустить, что данные, представленные Сноуденом, достоверны, то можно утверждать, что получаемых спецслужбами данных было

достаточно для того, чтобы контролировать деятельность практически всех «продвинутых» пользователей Интернета.

Особый интерес представляет тот факт, что многие современные интернет-компании предоставляют своим клиентам услуги по так называемому «облачному» принципу организации данных. «Облачные» технологии позволяют хранить всю необходимую информацию на одном или нескольких серверах, обеспечивая доступ к ней с разных устройств. Использование подобной технологии, как представляется, в ещё большей степени облегчило работу американским спецслужбам.

Важно также отметить, что помимо собственно текстовых, звуковых, видео и графических сообщений, сервера хранили большое количество технической информации, такой, как местоположение пользователя, его перемещения, история просмотра интернет-страниц, информация о контактах и т.д. (так называемая «метаинформация»).

Такая информация также играет большую роль. К примеру, американская пресса сообщала, что иракские экстремисты смогли найти месторасположение американских войск по так называемому геотэгу [29]. Один из американских военнослужащих разместил в Интернете файл с фотографией, который содержал техническую информацию о точном месторасположении, где он был сделан. Благодаря этой метаинформации террористы узнали, куда необходимо нанести удар.

После скандальной публикации разоблачений Э. Сноудена в британской газете «Гардиан» (*The Guardian)* последовали многочисленные расследования и заявления представителей упомянутых Сноуденом организаций.

Так, АНБ США опубликовало справочную информацию, в которой раскрыло принципы соблюдения раздела 702 закона «Об иностранной разведке» и раздела 215 закона «Патриот», а также полномочия американских спецслужб по сбору конфиденциальной информации о гражданах США.

В справке, в частности, говорилось, что в соответствии с разделом 702 закона «Об иностранной разведке», «сбор конфиденциальной информации осуществлялся в отношении иностранных граждан. Американское правительство не имеет права осуществлять подобные действия в отношении американских граждан, независимо от того, на территории какого государства они находятся. Сбор информации может быть осуществлён с разрешения специального суда, в компетенцию которого входит решение вопросов, связанных со сбором разведданных (*Foreign Intelligence Surveillance Court*), а также генерального прокурора и директора национальной разведки. Разрешение выдаётся при условии весомых доказательств того, что человек занимается террористической или иной антиамериканской деятельностью. Доказательства тщательным образом документируются, а разрешение не нарушает четвёртую поправку к Американской Конституции. Если полученная информация не представляет ценности для американских спецслужб, она должна быть оперативно уничтожена» [8].

Согласно разделу 215 закона «Патриот», «американские спецслужбы имеют право собирать только телефонную «метаинформацию», т.е. с какого и на какой номер, откуда и когда осуществлялся звонок, но не содержание самого телефонного разговора. Эти данные хранятся в специально защищённом хра-

нилище, а доступ к ним есть лишь у некоторых сотрудников со специальным допуском, и осуществляется только при специальном запросе и с разрешения определённых сотрудников АНБ численностью меньше дюжины» [12].

Белый дом опубликовал доклад, обосновывающий полномочия специальных служб на основе принятого американского законодательства [23].

Директор АНБ генерал Кейт Александер сам был вынужден «оправдываться» перед законодательной властью. Так, 18 июля 2013 г. прошли открытые слушания в Комитете по разведке Палаты Представителей, на которых Александер заявил, что если бы такая программа как *PRISM* существовала ранее, террористические акты 11 сентября 2001 г. можно было бы предотвратить.

На слушаниях присутствовал заместитель генерального прокурора США Джим Коул, который разъяснил детали американского законодательства, разрешающие использование системы *PRISM*. Кроме того, Коул заявил, что информация о деятельности АНБ была доступна американским законодателям. Заместитель генерального прокурора США подробно рассказал, каким образом с какой периодичностью и перед кем Агентство национальной безопасности отчитывалось о своей деятельности [12].

Опровержения данных, представленных Сноуденом, не последовало, вместе с тем, Александер неоднократно повторял, что деятельность АНБ не нарушает четвёртую поправку к Конституции, и гарантирует сохранение конфиденциальности американских граждан.

Оправдания и опровержения последовали и от оказавшихся замешанными в скандале представителей интернет-компаний.

Компания «Майкрософт» опубликовала опровержение данных, предоставленных Э. Сноуденом в газете «Гардиан» – той же самой, к которой обратился сам Сноуден в самом начале скандала. В заявлении «Майкрософт» говорится, что компания «сотрудничала с американским правительством, как в целях правоохранительной деятельности, так и в интересах национальной безопасности. Передача данных о клиентах осуществлялась в соответствии с принятыми законодательными процедурами (*we provide customer data only in response to legal processes*). Более того, в заявлении компании говорилось, что в ряде случаев органам государственной безопасности было отказано в доступе к клиентской информации, если разглашение конфиденциальной информации подразумевало нарушение действующего законодательства [18].

Ларри Пейдж сказал, что его компания «никогда не предоставляла прямой доступ американскому или иному правительству к своим серверам и до вчерашнего дня не имела представления о программе *PRISM*. Юридическая служба «Гугл» внимательно изучает все запросы о разглашении конфиденциальных данных, поступающие от американских органов государственной безопасности, и предоставление доступа происходит исключительно в соответствии с действующим законодательством» [33]. В подтверждение своих слов, Пейдж заявил, что «Гугл» добивается изменения американского законодательства о транспарентности и прозрачности взаимодействия телекоммуникационного сектора экономики с правительством. В доказательство своих слов он представил ссылку на доклад, в котором содержится информация об удовлетворённых и неудовлетво-

рённых запросах американского правительства в «Гугл» относительно предоставления конфиденциальных сведений клиентов [17].

Компания «Эппл» также опубликовала похожее заявление, в котором заявила, что сотрудники компании ничего не слышали про программу *PRISM* и предоставляют доступ к конфиденциальной информации своих клиентов только при условии предъявления судебного ордера. И, последовав примеру своих коллег из компании «Гугл» «яблочники» раскрыли некоторые цифры, отражающие количество правительственных запросов на клиентскую информацию [9].

Практически такое же заявление сделал и глава «Фейсбук» Марк Цукерберг. О программе *PRISM* он не слышал, все запросы тщательно обрабатывались юридической службой и удовлетворялись в соответствии с законодательством [34]. «Фейсбук» также опубликовала данные о запросах американской разведки о доступе к конфиденциальной информации о гражданах [14].

Таким образом, все ключевые интернет-провайдеры – участники «Сноуденгейта» – подтвердили, что органы американской государственной безопасности обращаются к ним с просьбами о предоставлении конфиденциальной информации о клиентах. Более того, представители всех этих компаний заявили, что удовлетворяют подобные запросы в соответствии с принятым американским законодательством. Вместе с тем, ряд экспертов утверждает [10], что прямой доступ к серверам компаний мог быть обеспечен незаметно, т.е. компании могли даже не знать о том, что такая деятельность ведётся.

Важно отметить, что судебный ордер требуется только для того, чтобы получить информацию о гражданине США, получение информации об иностранных гражданах происходит без какой-либо юридической санкции.

Вместе с тем, активизировались американские правозащитники. Более 60 правозащитных американских организаций обратились в Комитет по юстиции Сената США с письмом, в котором приветствовали действия, направленные на оценку деятельности спецслужб, и выдвинули ряд требований, которые должны быть учтены в ходе наметившейся очередной реформы разведывательного сообщества [19].

Управление национальной разведки опубликовало короткое заявление, в котором говорилось, что деятельность американских спецслужб не использовалась в отношении американских граждан, а велась против иностранцев за рубежом [24]. В ходе реформы разведывательного сообщества, проведённой администрацией Дж. Буша-мл., в целях повышения эффективности противодействия террористическим сетям, изменились задачи специальных служб в области получения доступа к конфиденциальным данным. Раньше конфиденциальность граждан могла быть нарушена спецслужбами, чтобы предоставить доказательства в суд, и для этого требовался ордер (разрешение) судьи или прокурора. Стратегия национальной безопасности президента Дж. Буша-мл. провозгласила политику нанесения превентивного удара по террористам. Сбор конфиденциальной информации в таком случае осуществлялся не в целях предоставления доказательств в суд, а для проведения специальных операций (например, таких как задержание С. Хуссейна или ликвидация У. бен Ладена). Деятельность спецслужб при этом распространилась не только на американских граждан, но на всех пользователей упомянутых Э. Сноуденом интернет-компаний.

Несмотря на мощнейшую волну критики, генерал К. Александер заявил, что несколько террористических актов были предотвращены именно благодаря системе *PRISM*. Не было сделано ни одного заявления о сворачивании программ, и, судя по всему, государственные расходы на эти цели не сократятся.

Следует отметить, что реакцией АНБ на «Сноуденгейт» стало не повышение ответственности и транспарентности деятельности организации, а повышение требований к обеспечению информационной безопасности с целью предотвращения дальнейших утечек информации.

Генерал Александер на конференции по безопасности в Аспене заявил, что АНБ в настоящее время тестирует новые правила, согласно которым, если сотруднику необходимо скопировать секретные данные на переносной носитель, необходимо присутствие и разрешение другого сотрудника, имеющего допуск к секретной информации [22]. При этом Александер признал, что это заметно усложнит работу организации, но это вынужденная мера. Данное положение напоминает правило «двойного ключа» – необходимого условия для запуска ядерных ракет, исключающего возможность единоличного принятия такого решения.

В ходе некоторых слушаний в американском Конгрессе вокруг программы *PRISM* и заявлений Э. Сноудена для объяснения были вызваны руководители всех американских спецслужб, имевших возможность получать доступ к конфиденциальным данным [33]. Глава киберкомандования США и по совместительству директор Агентства национальной безопасности Кейт Александер не отрицал фактов, разглашённых Э. Сноуденом. Он заявил, что если бы террористы знали, каким образом американские спецслужбы получают информацию, они бы использовали другие методы связи, в результате чего могли погибнуть американские граждане.

На слушаниях в комитете Палаты представителей по ассигнованиям, Александер также отметил, что гарантия конфиденциальности и неприкосновенности частной информации американских граждан – основной приоритет деятельности Агентства национальной безопасности и киберкомандования. Вместе с тем, генерал особо подчеркнул, что стремится «нормализовать» кибероперации и сделать их полноценным элементом американского политического и военного потенциала [29].

Вместе с тем, «дело Сноудена» омрачило успех, достигнутый между Россией и Соединёнными Штатами по вопросам кибербезопасности. В течение двух лет проходили двусторонние встречи между российским Советом безопасности и помощниками американского президента по кибербезопасности – Майклом Шмидтом и Майклом Дэниелом. Результатом работы стало Соглашения о новой области сотрудничества.

Эдвард Сноуден заметно осложнил российско-американские отношения, фактически нивелировав объявленную в 2009 г. «перезагрузку». Президент Обама объявил, что отменяет запланированную встречу с президентом В.В. Путиным в Москве в ходе саммита Большой двадцатки. Под угрозой оказались все успехи, достигнутые сторонами, причём не только по вопросам кибербезопасности, но и в других важнейших областям сотрудничества.

Эдвард Сноуден принял решение остаться в Москве, и, проведя почти месяц в международной зоне московского аэропорта, получил официальное временное разрешение на нахождение на территории России в течение года. Президент РФ Путин поставил условие, при котором Сноудену будет позволено остаться: последний должен прекратить любую деятельность, наносящую вред Соединённым Штатам.

Оставшись в России, уже после получения с официального разрешения, Эдвард Сноуден продолжает «подливать масла в огонь», заявив, в частности, что на территории Москвы находится главный шпионский сервер американских спецслужб, через который они получают информацию о россиянах [7].

Последующие разоблачения Сноудена о том, что помимо конфиденциальной информации «обычных» пользователей АНБ имело доступ к информации мировых политических лидеров, окончательно превратили проблему секретных операций американских спецслужб в один из сложнейших вопросов международных отношений.

В октябре 2013 г. генерал Александер объявил о том, что уходит в отставку вместе со своим заместителем. Сменяется поколение «отцов-основателей» кибербразведки. Возможно, это повлечёт за собой изменение американской стратегии в отношении киберпространства. Как отмечено выше, Кейт Александер совмещал две должности – командующего стратегическим киберкомандованием и директора АНБ. Подобная ситуация подчинялась определённой логике. Вместе с тем, в экспертном сообществе Соединённых Штатов в настоящее время ведутся дискуссии относительно возможности назначения двух разных людей на эти должности.

Ожидать быстрого изменения стратегии не приходится, так как для этого потребуется политическая воля президента Соединённых Штатов, который сейчас находится в тяжёлой ситуации в связи с обсуждением вопросов федерального бюджета. Кроме того, уже не за горами очередная избирательная кампания, в которой примут участие новые кандидаты. Принятие какого-либо серьёзного решения, связанного с военной стратегией, может спровоцировать очередные баталии в Конгрессе, а в итоге может оказаться непопулярным и негативно отразится на результатах голосования.

Нельзя исключать и того, что электронная разведка станет более секретной. В ходе «разбора полётов» после откровений Эдварда Сноудена, Кейт Александер заявлял о том, что необходимо изменить принцип работы сотрудников АНБ с секретными данными. Все объявленные меры в отношении секретной информации, озвученные руководством Агентства национальной безопасности заключались в том, чтобы впредь исключить возможность утечек информации.

Возвращаясь к интернет-провайдерам, отметим, что невозможно представить себе, каким количеством конфиденциальной информации обладают эти компании, или оценить масштабы переданных данных в спецслужбы США. Согласно утверждениям Сноудена, программа *PRISM* получала информацию с серверов этих компаний напрямую [14]. Система *PRISM* ориентирована на доступ к информации крупнейших мировых телекоммуникационных компаний,

контролирующих в совокупности все 100% мирового рынка. Крайне сомнительно, что АНБ откажется от взаимодействия с этими компаниями.

Военный аспект информационного противоборства не являлся предметом российско-американских отношений. Несмотря на подписанное в июне 2013 г. Соглашения о новой области сотрудничества, достигнутые договорённости носят во многом политический характер. Изменение руководства даёт шанс включить различные аспекты военного использования информационного пространства в российско-американский диалог по проблемам кибербезопасности.

Сбор информации становится едва ли не важнейшим фактором национальной безопасности и экономической конкурентоспособности. Вряд ли можно оспорить утверждение представителей американских спецслужб, что благодаря системе *PRISM* было предотвращено несколько террористических актов. Вместе с тем, нельзя исключать и того, что сбор данных в интернет-пространстве позволял решать не только проблемы национальной безопасности. Нельзя исключать, что система *PRISM* обеспечивала получение информации экономического характера, которая позволила американским компаниям добиться заметного информационного преимущества, гарантировав экономическую конкурентоспособность. И всё это при ничтожных финансовых издержках (в 20 млн. долл. в год).

Нельзя также исключать и того, что система *PRISM* не единственная, позволяющая получать конфиденциальные данные. Вместе с тем, есть все основания полагать, что сбор информации американскими спецслужбами продолжится, пример программы *PRISM* демонстрирует, что подобные системы легко утаить, а новая система, скорее всего, будет ещё более секретной.

В своё оправдание представители интернет-компаний, оказавшихся участниками «Сноуденгейта» заявили, что передавали информацию только при соответствующих запросах и с соблюдением всех необходимых юридических процедур. Э. Сноуден, однако, не утверждал, что передача информации осуществлялась сознательно – нельзя исключать, что АНБ получало информацию без уведомления соответствующих сторон.

В марте 2014 г. администрация президента Б. Обамы заявила о желании реформировать электронную разведку, и с этой целью готовится новый законопроект [27]. Скорее всего в этом законе будут учтены выводы комиссии, сформированной ранее президентом для расследования соответствующей деятельности АНБ. Возглавил комиссию Ричард Кларк, ставший первым в истории помощником президента США по кибербезопасности. В опубликованном по результатам работы комиссии докладе «Свобода и безопасность в меняющемся мире» [21] содержится 46 рекомендаций по реформе спецслужбы.

Указанное заявление администрации президента Обамы имеет не только внутриполитическое, но и международное значение. Из-за разоблачений Эдварда Сноудена перед американским политическим руководством встало множество вопросов. Самой скандальной, пожалуй, явилась информация о том, что АНБ собирало конфиденциальные данные про канцлера Германии Ангелу Меркель.

Обсуждение вопросов международной деятельности АНБ США было запланировано на мартовский 2014 г. саммит США – ЕС. Но события на Украине потребовали изменения повестки дня саммита, и данный пункт был вычерк-

нут. Вместо этого, на саммите было объявлено о начале «диалога по вопросам кибербезопасности между США и ЕС» [31], который должен укрепить и расширить их взаимодействие и сотрудничество по следующим направлениям:

- международное развитие кибербезопасности;
- продвижение и защита прав человека в сети;
- международные вопросы безопасности, такие, как нормы поведения в киберпространстве, меры по укреплению доверия в киберпространстве, применение действующих норм международного права;
- укрепление потенциала кибербезопасности третьих стран.

Необходимо отметить, что многие из этих пунктов совпадают с предложениями Российской Федерации, внесёнными ею на многочисленных международных дипломатических площадках (некоторые формулировки даже остались неизменными!). Но данный шаг, всё-таки, направлен против России и нацелен на усиление международной коалиции по вопросам кибербезопасности и ослабление дипломатической позиции России по этому вопросу.

Администрация Барака Обамы также выступила с предложением сложить с США полномочия по глобальному управлению Интернетом и передать эти функции международному сообществу [30]. Данное заявление удивительно тем, что в течение предыдущих 15 лет все попытки передать функции управления корпорацией ИКАНН (интернет-корпорации по распределению доменных имён и номеров, учреждённая Министерством торговли США) Организации Объединённых Наций наталкивались на непреодолимое сопротивление со стороны Соединённых Штатов. Нынешний неожиданный ход США, как представляется, обусловлен критикой разведдеятельности АНБ со стороны международного сообщества.

«Сноуденгейт» также продемонстрировал пробелы в международном праве, решение которых станет более сложной задачей.

Администрация Обамы оказалась в крайне сложной ситуации, ведь ей важно демонстрировать политическую волю как перед иностранными коллегами, так и перед американскими гражданами. В не менее сложной ситуации оказалась и Россия. Предоставив убежище Эдварду Сноудену, Москва оказалась втянута в конфликт с Вашингтоном, результатом которого уже стали срыв запланированной на сентябрь 2013 г. двусторонней встречи президентов В.В. Путина и Б. Обамы и ухудшение двусторонних отношений, в том числе в области кибербезопасности.

Как представляется, инциденты, подобные «Викиликс» и «Сноуденгейту» являются обратной стороной формирующегося информационного общества, наряду с колоссальными достижениями и безусловными преимуществами, открывающимися в результате информационной революции. Современные уислблоуеры – такие как Б. Мэннинг и Э. Сноуден действовали не через Конгресс. Судя по тому, как отреагировали американские конгрессмены, данная информация не стала бы достоянием общественности, если бы Мэннинг и Сноуден соблюдали законодательство о уислблоуерах, принятое в 1998 году.

С сожалением приходится признать тот факт, что, поскольку с развитием информационных технологий, с учётом того, что хранить секреты становится всё сложнее, а получить различного рода информацию становится всё проще,

доверия между государствами, нациями и другими субъектами международных отношений становится всё меньше.

Нельзя исключать и того, что международный скандал, вызванный разоблачениями Эдварда Сноудена спровоцирует дальнейшее наращивание военного информационно-технологического оборонительного потенциала.

Очевидно, что в сфере получения информации о политических конкурентах, как это было в случае с Р. Никсоном, или о военных противниках, контртеррористическая направленность системы *PRISM* предоставляет заметное преимущество. Вместе с тем, неизбежно возникает противоречие между гражданскими правами (в первую очередь правом на сохранение конфиденциальности информации) и интересами национальной безопасности. Раскрытие программы *PRISM* продемонстрировало, что в поиске «золотой середины» между гарантией свободы и обеспечением безопасности американское правительство вновь потерпело неудачу. Попытки легализовать подобные программы неизбежно наталкиваются на мощную волну сопротивления, в основном, со стороны правозащитников. Попытка осуществлять подобные программы секретно в очередной раз обернулась скандалом из-за внутренней утечки информации. Отказываться от подобной деятельности американское правительство, разумеется, не собирается.

## Список литературы


1. Американская ассоциация юристов. Правовая инициатива в Центральной и Восточной Европе. Центр права и средств массовой информации. Серия «Журналистика и право». Выпуск 8. С. 21.

2. Встреча В.В. Путина с руководством и корреспондентами телеканала *Russia Today*. 11 июня 2013 г. (http://president.kremlin.ru/news/18319).

3. *Дорохов Р.*, *Никольский А.* Шпион в центре Москвы // Ведомости. 12.08.2013. 144 (3406).

4. *Иванян Э.А.* История США. М.: Дрофа, 2004. С. 503–505.

5. Конституция США. Поправка IV.

6. *О'Рейли Тим*. Что такое Веб 2.0. // Компьютерра. 18.10.2005 (http://computerra.ru/think/234100/).

7. Правовые вопросы журналистики и телекоммуникаций в США. М.: Институт проблем информационного права. 2005. Серия «Журналистика и право». Выпуск 53. С. 21 (например, знаменитая *Wikipedia* или сервис «Яндекс пробки», автоматически собирающий и предоставляющий информацию от самих пользователей о ситуации на дорогах крупных городов России).

8. 149791922-National-Security-Agency-Section-702-of-FISA-and-Section-215-of-PATRIOT-Act-Fact-Sheets.pdf.

9. Apple's Commitment to Customer Privacy. June 16, 2013 (http://www.apple.com/apples-commitment-to-customer-privacy/).

10. *Barton G.* and *Poitras L.* U.S. Mining Data from 9 Leading Internet Firms; Companies Deny Knowledge // The Washington Post. June 7, 2013.

11. *Bernstein C.*, *Woodward B.* All the Presidents Men. Simon & Schuster, 1972.

12. Congressional Hearings. House Select Intelligence Committee Holds Hearing on Disclosure of National Security Agency Surveillance Programs. June 18, 2013 (http://west moreland.house.gov/images/6-19-13%20Intel%20Hearing%20Transcript%20NSA%20Leaks.pdf).

13. Edward Snowden Identifies Himself as Source of NSA Leaks – As It Happened // The Guardian. 9.06.2013 (http://www.guardian.co.uk/world/2013/jun/09/nsa-secret-surveillance-lawmakers-live?INTCMP=SRCH).

14. Facebook Global Government Requests Report (https://www.facebook.com/about/government_requests).

15. *Fisher Louis*. National Security Whistleblowers. 30.12.2005. P. 1.

16. The Foreign Intelligence Surveillance Act: An Overview of Selected Issues Updated. CRS Report to Congress RL34279. 7.07.2008.

17. Google Transparency Report (http://www.google.com/transparencyreport/userdatarequests/US/).

18. How Microsoft Handed the NSA Access to Encrypted Messages // The Guardian Friday. 12.07.2013.

19. https://www.cdt.org/files/pdfs/Letter-Judicary-Committee-NSA.pdf

20. *Lewis Anthony*. Make No Law. Vintage Books, 1992. P. 65.

21. Liberty and Security in a Changing World. Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies. December 12, 2012 (http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf).

22. NSA Pilots 2-person Rule to Thwart Leaks. By Eric Cabrow. July 22, 2013. Govinfosecurity

23. Obama Administration White Paper on NSA Surveillance Oversight // (http://apps.washingtonpost.com/g/page/politics/white-house-surveillance-reform-plan/388/).

24. ODNI Statement on the Limits of Surveillance Activities. June 16, 2013 (http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/880-odni-statement-on-the-limits-of-surveillance-activities).

25. The Pentagon Papers.

26. *Reed John*. Insurgents Used Cell Phone Geotags to Destroy AH-64s in Iraq, 15.03.2012 (http://defensetech.org/2012/03/15/insurgents-used-cell-phone-geotags-to-destroy-ah-64s-in-iraq/).

27. *Savage Ch.* Obama to Call for End to N.S.A.'s Bulk Data Collection // The New York Times. March 24, 2014 (http://www.nytimes.com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html?emc=edit_na_20140324&nlid=61925389&_r=1).

28. The Sedition Act of 1798 (закон был принят вместе с тремя другими законами, необходимыми для противодействия антиправительственной деятельности).

29. Statement of General Keith B. Alexander, USA Commander, United States Cyber Command Director, National Security Agency Chief, Central Security Service before the Senate Committee on Appropriations "Cybersecurity: Preparing for and Responding to the Enduring Threat", 12.07.2013 (http://www.appropriations.senate.gov/ht-full.cfm?method=hearings.view&id=33dda6f9-5d83-409d-a8c5-7ada84b0c598).

30. *Timberg C.* U.S. to Relinquish Remaining Control Over the Internet // The Washington Post. March 15, 2014 (http://www.washingtonpost.com/business/technology/us-to-relinquish-remaining-control-over-the-internet/2014/03/14/0c7472d0-abb5-11e3-adbc-888c8010c799_story.html).

31. U.S.-EU Cyber Cooperation. March 26, 2014 (http://www.whitehouse.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation).

32. US House of Representatives Permanent Select Committee on Intelligence. Hearings on "How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries", 18.06.2013 (http://intelligence.house.gov/hearing/how-disclosed-nsa-programs-protect-americans-and-why-disclosure-aids-our-adversaries).

33. What the ...? Posted: Friday, June 07, 2013. Posted by Larry Page, CEO and David Drummond, Chief Legal Officer (http://googleblog.blogspot.ru/2013/06/what.html).

34. *Zuckerberg Mark*. 7 июня в 14:45 возле Менло-Парк. I want to respond personally to the outrageous press reports about PRISM: (https://www.facebook.com/zuck/posts/10100828955847631).