МОСКОВСКИЙ ЦЕНТР
КАРНЕГИ

РОССИЙСКО-АМЕРИКАНСКИЕ ОТНОШЕНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПАВЕЛ ШАРИКОВ | НОЯБРЬ 2013

В современном мире вопросы информационной безопасности становятся приоритетом не только на внутригосударственном уровне — они приобретают стратегически важный характер для всей системы международных отношений в целом. Кроме того, взаимодействие и сотрудничество в этой сфере становится перспективным направлением российско-американских отношений. В этой сфере между Россией и США намечаются противоречия, но вместе с тем в сфере информационной безопасности достигнуты и заметные успехи.

ВВЕДЕНИЕ

Под влиянием процессов информационной революции при формировании внешнеполитического курса развитых государств научно-технический фактор приобрел особое значение. Во второй половине XX в. одним из ключевых направлений научно-технического прогресса стало развитие технологий работы с информацией. Стремительное развитие и распространение информационных технологий, а также их влияние на социально-экономические и военно-политические аспекты деятельности человека не позволяли игнорировать эти процессы.

Результатом продолжающейся по сей день информационной революции стало усиление процессов глобализации. При всем многообразии различных подходов к этой проблеме большинство мировых экспертов сходятся во мнении, что информационная революция, стремительное развитие и распространение информационных технологий и Интернета во второй половине XX и в начале XXI в. имеют определяющее значение для развития современного общества.

Распространение и проникновение информационных технологий в экономику неизбежно приводит к усилению зависимости от информационной инфраструктуры. Нарушение ее функционирования является серьезным вызовом экономической безопасности, а также может стать угрозой национальной безопасности государства в целом.

ОБ АВТОРЕ

Павел Шариков — *руководитель Центра прикладных исследований Института США и Канады РАН, кандидат политических наук. Сфера научных интересов — информационные угрозы национальной и международной безопасности, формирование информационного общества, влияние информационной революции на международные отношения.*

Таким образом, наряду с очевидными благами, которые несут глобализация и информационная революция, имеется и ряд негативных последствий, связанных во многом с проблемами информационной безопасности, которые обращают на себя внимание политических лидеров, а также международного сообщества.

С момента создания и распространения Интернета прошло немногим больше двадцати лет. За это время угрозы информационной безопасности заметно эволюционировали от проблем мошенничества и краж (хакеров, маргиналов и тому подобных криминальных элементов) до стратегических угроз безопасности, исходящих от вооруженных сил противника.

Если учесть специфику развития и применения информационных ресурсов, становится очевидно, что ни в одной стране государственная власть не в состоянии обеспечить необходимый уровень информационной безопасности. Мировой опыт показывает, что создание информационных технологий происходит наиболее эффективно в частном секторе. А коммерческий успех предприятия, предоставляющего товары и услуги в сфере информационных технологий, возможен при наличии широкого спроса среди потребителей в глобальном масштабе. Практически любая мера, предпринятая государством в целях обеспечения информационной безопасности, так или иначе затронет интересы общества или бизнеса и станет препятствием для свободного развития информационных технологий.

Вместе с тем под влиянием угроз информационной безопасности в настоящее время формируется новая архитектура международной безопасности. Как представляется, данный процесс накладывается на проблемы становления полицентричной системы международных отношений. Учитывая, что информационные технологии могут быть использованы в целях поражения инфраструктуры противника, особую угрозу представляют военные разработки информационного оружия.

Технология Интернета была разработана американскими учеными, а источником распространения информационного пространства в глобальном масштабе стали именно Соединенные Штаты. В этой связи США первыми столкнулись с многочисленными последствиями информационной революции, а американское государство раньше остальных было вынуждено принять меры по противодействию информационным угрозам. Опыт американской политики в области информационных технологий уникален, однако сегодня с уверенностью можно говорить о том, что проблема противодействия информационным угрозам стала приоритетом национальной безопасности и внешней политики каждого развитого государства современного мира. Вместе с тем последние события свидетельствуют, что вопросы информационной безопасности делаются новым приоритетом на повестке дня двусторонних российско-американских отношений.

Информационная политика стала основным направлением внутренней политики Соединенных Штатов еще при администрации президента Билла Клинтона. По мнению Белого дома, доминирование в сфере информации достигалось через развитие и распространение информационных технологий, ускорение социально-экономического развития Соединенных Штатов. В период правления администрации Билла Клинтона действия государства были направлены на то, чтобы создать максимально благоприятные условия для развития коммерческих информационных технологий с целью развития экономики. В результате активного развития информационных технологий в США общество, бизнес и граждане получили беспрецедентный доступ к значительным информационным ресурсам.

Установленный государством благоприятный налоговый режим привел к массовому внедрению компьютеров, а затем и Интернета в социально-экономическую жизнь США. Информационные технологии превратились в локомотив развития американской экономики в 1990-е годы. С целью получения большей прибыли

от производства и торговли информационными технологиями американское государство провело реформу системы экспортного контроля высоких технологий. Американские компьютеры и программное обеспечение, а также модель управления Интернетом были навязаны в качестве стандарта пользователям мирового информационного пространства.

Политика США при президенте Джордже Буше была обусловлена обострившимися угрозами национальной безопасности после террористических актов 11 сентября 2001 г. В информационной сфере действия администрации Дж. Буша были направлены на установление глобального информационного контроля — не только на уровне государства, но и в глобальном масштабе. Этим были обусловлены внешнеполитические действия американской дипломатии в области международного сотрудничества в сфере развития информационных технологий и обеспечения информационной безопасности.

Как представляется, американская политика в этой сфере формировалась в поиске золотой середины между гарантиями свободного предпринимательства и принятием соответствующими органами необходимых мер для обеспечения информационной безопасности. Методом проб и ошибок американские политики пришли к выводу, что процесс обеспечения кибербезопасности должен основываться на тесном и взаимовыгодном сотрудничестве органов власти, бизнеса, гражданского общества и международного сообщества.

АМЕРИКАНСКИЕ ИНИЦИАТИВЫ

Администрация президента Барака Обамы сформулировала приоритетные задачи в сфере информационной безопасности в двух доктринальных документах: «Международной стратегии развития киберпространства»[1] и «Стратегии военной кибербезопасности»[2]. В них раскрывается позиция Белого дома в отношении информационной безопасности, стратегического развития глобального информационного пространства и роли вооруженных сил в обеспечении кибербезопасности.

Особый интерес представляет положение о том, что в ответ на кибератаки США готовы использовать любые средства — дипломатические, экономические и военные[3]. Авторы стратегии утверждают, что планируют применять политику сдерживания в отношении киберугроз. Однако это возможно исключительно при условии наличия у Соединенных Штатов наступательных кибервооружений. Согласно многочисленным источникам, подобные разработки ведутся, вместе с тем, разумеется, данная информация является государственной тайной. Важно отметить, что положения об американском наступательном информационном потенциале, судя по всему, содержатся в засекреченной части военной киберстратегии.

Вместе с тем, согласно открытым источникам, американские спецслужбы воспринимают киберугрозы более чем серьезно. Так, в 2009 г. директор национальной разведки США Деннис Блэр особенно отметил угрозу финансовому сектору американской экономики, исходящую от террористов. Причем на слушаниях в 2009 г. впервые прозвучала оценка разведывательного сообщества, в которой говорилось, что Россия и Китай обладают технической возможностью нанесения критического ущерба американской информационной инфраструктуре и сбору разведданных. Позднее Д. Блэр отметил, что для противодействия угрозам необходимо международное сотрудничество. В 2012 г. директор национальной разведки Джеймс Клэппер впервые заявил[4], что противодействие угрозам кибербезопасности является «растущим стратегическим интересом» (evolving strategic concern) американского политического руководства. Российские и китайские акторы упоминались как ключевые источники компьютерных атак на американские компьютерные сети и кражи объектов американской интеллектуальной собственности.

На слушаниях в текущем году вопросы кибербезопасности были поставлены на первое место. Дж. Клэппер утверждал [5], что государства и негосударственные акторы используют различные инструменты кибератак для достижения стратегических целей. Впервые в контексте обсуждения угроз кибербезопасности поднимался вопрос управления Интернетом и глобального регулирования информационного пространства.

Под влиянием необходимости обеспечить безопасность гражданских инфраструктур изменяются и внешнеполитические приоритеты Соединенных Штатов. Они ведут достаточно активную внешнеполитическую деятельность, направленную на укрепление сотрудничества по вопросам кибербезопасности с ключевыми военно-политическими союзниками. К сожалению, несмотря на многочисленные декларации, Соединенные Штаты не воспринимают Россию как полноценного стратегического союзника.

Вопросы кибербезопасности были включены в ряд международно-правовых договоров, посвященных коллективной безопасности, в частности в Тихоокеанский пакт безопасности (АНЗЮС). В официальном совместном заявлении, подписанном 15 сентября 2011 г. министрами обороны и иностранных дел США и Австралии, говорится, что «в случае кибератак, угрожающих территориальной целостности, политической независимости или безопасности любого из государств, Австралия и Соединенные Штаты проведут совместные консультации и выработают адекватные меры по противодействию угрозе» [6].

Особый интерес в данном контексте вызывает активизация усилий в области кибербезопасности в рамках Организации Североатлантического договора. Доктринально стратегия НАТО в области кибербезопасности была закреплена в «Стратегической концепции обороны и безопасности членов Североатлантического договора» [7], а также в декларации, подписанной по итогам лиссабонского саммита в ноябре 2010 г. [8] В июне 2011 г. была принята доктрина кибербезопасности, которая в данный момент недоступна широкой публике. Кроме того, в рамках НАТО создаются административные и организационные структуры, в функции которых входит обеспечение коллективной кибербезопасности.

Серьезного внимания заслуживает появившееся в марте 2013 г. «Пособие по международно-правовому регулированию кибервойны» [9]. Этот документ затрагивает самые сложные вопросы использования киберинструментов в вооруженных действиях. Авторы пособия проделали колоссальную работу по изучению норм международного права, регламентирующих использование информационных технологий вооруженными силами. Особый интерес представляет попытка интерпретировать транснациональные информационные атаки как нарушение государственного суверенитета, т. е. фактически как условие для применения ст. 5 Североатлантического договора.

В формирующемся полицентричном мире в условиях появления и развития различных акторов в системе международных отношений намечается противостояние США и Китая, в том числе в такой новой области, как киберпространство. В этом контексте большой интерес вызывает американо-китайское сотрудничество в сфере кибербезопасности.

И США, и Китай имеют немало союзников в киберпространстве. В этой связи особое место занимает Россия, учитывая многочисленные инициативы российских дипломатов. В частности, Россия и Китай являются участниками предложенной Российской Федерацией конвенции по международной информационной безопасности.

Проблема китайских киберугроз национальной безопасности Соединенных Штатов также осложняется и тем, что у США и Китая практически нет общих дипломатических площадок для обсуждения этих вопросов.

Фактически первая американо-китайская встреча на высшем уровне, на которой поднимались вопросы кибербезопасности, состоялась в начале июня этого года в США. Президент Б. Обама начал встречу с председателем КНР Си Цзиньпином с обсуждения вопросов кибербезопасности в рамках американо-китайского «Стратегического диалога по экономике и безопасности». На пресс-конференции Б. Обамы, состоявшейся после встречи с китайским руководством, американский президент заявил, что была достигнута договоренность о необходимости выработки общих подходов по вопросам кибербезопасности [10]. Си Цзиньпин между тем также заявил, что китайские власти обеспокоены проблемами кибербезопасности.

ПОЗИЦИЯ РОССИИ ПО ПРОБЛЕМАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вопросы кибербезопасности, безусловно, являются одним из важнейших приоритетов российской внешней политики. В «Стратегии национальной безопасности Российской Федерации до 2020 года» отмечается, что «угрозами военной безопасности являются: политика ряда ведущих зарубежных стран, направленная на достижение преобладающего превосходства в военной сфере, прежде всего в стратегических ядерных силах, путем развития высокоточных, информационных и других высокотехнологичных средств ведения вооруженной борьбы, стратегических вооружений в неядерном оснащении» [11]. В «Концепции внешней политики Российской Федерации» говорится, что в целях укрепления международной безопасности Россия «будет принимать необходимые меры в интересах обеспечения национальной и международной информационной безопасности, предотвращения угроз политической, экономической и общественной безопасности государства, возникающих в информационном пространстве, для борьбы с терроризмом и иными криминальными угрозами в сфере применения информационно-коммуникационных технологий, противодействовать их использованию в военно-политических целях, противоречащих международному праву, включая действия, направленные на вмешательство во внутренние дела, а также представляющие угрозу международному миру, безопасности и стабильности» [12].

Еще в 1998 г. российскими дипломатами был предложен термин «международная информационная безопасность» (МИБ), а основной площадкой для продвижения этой темы стала Организация Объединенных Наций. 23 сентября 1998 г. генеральному секретарю ООН Кофи Аннану было направлено специальное послание министра иностранных дел России. «Особый акцент в послании был сделан на необходимости предотвращения появления принципиально новой — информационной области конфронтации, способной спровоцировать новый виток гонки вооружений. В этой связи подчеркивалось, что речь идет о создании информационного оружия (ИО) и опасности возникновения информационных войн (ИВ). Принимая при этом во внимание уровень информатизации общества и одновременно уязвимость информационных структур, нельзя исключить возможности появления такого ИО, разрушительные свойства которого могут оказаться сравнимы с оружием массового поражения» [13].

По инициативе России в рамках ООН была создана Группа правительственных экспертов, главой которой стал российский дипломат Андрей Крутских. Идеи международной информационной безопасности были поддержаны международным сообществом, но вместе с тем встретили серьезную оппозицию со стороны американских экспертов. «В США ИКТ (информационно-коммуникационные технологии. — *П. Ш.*) являются мощным средством наращивания военного потенциала. Информационное оружие активно применялось американцами в ходе всех последних вооруженных конфликтов. США заинтересованы в том, чтобы сохранить свободу рук для военно-политического применения ИКТ, оставаясь, по сути дела, вне сферы регулирования международного права» [14].

Несомненно, успехом российской дипломатии следует считать тот факт, что резолюция Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», в которой были выражены российские идеи о МИБ, на протяжении многих лет принималась консенсусом в Генеральной Ассамблее ООН, несмотря на американскую оппозицию.

Российская позиция по вопросу международно-правового регулирования Интернета была неоднократно сформулирована в международно-правовых документах. Принципиальной особенностью российского подхода является стремление не допустить милитаризации глобального киберпространства. Как представляется, это основное необходимое условие для обеспечения «международной информационной безопасности».

Российскую позицию разделяет ряд других государств. В частности, особый интерес представляет подписание договора в рамках Шанхайской организации сотрудничества (ШОС). «25—27 октября 2006 г. во исполнение решения, содержащегося в Заявлении глав государств — членов Шанхайской организации сотрудничества по международной информационной безопасности от 15 июня 2006 г., состоялось учредительное заседание Группы экспертов государств — членов ШОС по МИБ. В ходе заседания была официально образована Группа и согласованы институциональные основы ее работы, а председателем консенсусом был избран эксперт Российской Федерации как государства, инициировавшего рассмотрение в ШОС проблематики МИБ. Выработанный Группой план действий по обеспечению международной информационной безопасности был одобрен Решением Совета министров иностранных дел государств — членов ШОС 9 июля 2007 г. и утвержден Решением Совета глав государств — членов ШОС, который состоялся 16 августа 2007 г.»[15]. Кроме того, успехом российской дипломатии можно считать регулярное обсуждение вопросов информационной безопасности на саммитах Организации Договора о коллективной безопасности[16].

Вместе с тем российская позиция наталкивается на противоречия в рамках Организации по безопасности и сотрудничеству в Европе. Как представляется, именно по причине обозначенных выше противоречий в конце прошлого года там не удалось достигнуть консенсуса, и международный документ о кибербезопасности не был принят[17].

В настоящее время позиция России отражена в концепции Конвенции об обеспечении международной информационной безопасности, представленной в рамках Второй международной встречи высоких представителей, курирующих вопросы безопасности, в Екатеринбурге (21—22 сентября 2011 г.). В ней, в частности, отмечается, что «...каждое государство-участник будет определять свой военный потенциал в информационном пространстве на основе национальных процедур с учетом законных интересов безопасности других государств, а также необходимости содействовать укреплению международного мира и безопасности. Ни одно из государств-участников не будет предпринимать попыток добиться господства в информационном пространстве над другими государствами»[18].

ПРОТИВОРЕЧИЯ ПО ВОПРОСАМ КИБЕРБЕЗОПАСНОСТИ В РОССИЙСКО-АМЕРИКАНСКИХ ОТНОШЕНИЯХ

Более двадцати лет потребовалось международному сообществу, чтобы прийти к пониманию острой необходимости создания универсальной международно-правовой базы, регулирующей вопросы информационной безопасности. Однако в подходах различных стран к этой проблеме намечается серьезное противоречие. С одной стороны, существует мнение, что глобальная информационная сеть представляет собой некое общее благо планетарного масштаба. В таком

случае подход к обеспечению информационной безопасности похож на решение, например, экологических проблем. Международные лидеры, которые придерживаются такой точки зрения, стремятся разработать единые нормы международного права, обязывающие национальные правительства внедрить их на внутриполитическом уровне. Как представляется, именно в этом и заключается подход Российской Федерации, выраженный в идее МИБ.

Всемирная сеть Интернет вряд ли тождественна понятию «информационное пространство», однако, учитывая разнообразие современных информационных технологий и протоколов связи, это его наиболее заметное выражение. В рамках данного подхода механизмы противодействия угрозам в информационном пространстве схожи с решением вопросов защиты окружающей среды, контроля над использованием космического пространства, возможно, общего использования арктических территорий.

Иными словами, во-первых, появление и реализация угрозы теоретически исключаются обязательствами, которые взяли на себя национальные правительства. При этом подразумевается, что правительства обладают действенными механизмами регулирования и контроля над «своим участком» на внутриполитическом уровне. Во-вторых, данный подход исключает возможность «присвоения» или единоличного использования некоего общего ресурса, но предполагает принятие государствами взаимных обязательств.

Другой подход заключается в том, что информационные ресурсы каждого государства относятся к его национальному суверенитету. Причем каждое государство оставляет за собой право реагировать на угрозы национальной (информационной) безопасности так, как посчитает нужным. Не отрицая необходимости разработки международно-правовой базы в области глобального регулирования информационного пространства, данный подход исключает внедрение внутригосударственного регулирования, ограничивающего свободное развитие информационных ресурсов.

Позиция Соединенных Штатов является вполне логичной. Как представляется, США придерживаются другого подхода к проблемам глобального управления Интернетом и регулирования информационного пространства. В значительной степени этот подход формируется под влиянием лобби американского бизнеса в области информационных технологий. Об этом, в частности, свидетельствует письмо, направленное представителями американского бизнес-истеблишмента в адрес спикера Палаты представителей Джона Боннера и лидера партии меньшинства Нэнси Пелоси в апреле 2012 г. в поддержку проекта Закона о разведке и обмене информации в киберпространстве (Cyber Intelligence Sharing and Protection Act). Авторы письма подтверждают, что усиление роли государства в развитии информационного пространства создаст препятствия развитию информационного сектора экономики. Вместе с тем они выражают озабоченность проблемами информационной безопасности, но тем не менее утверждают, что «информационная инфраструктура является частной собственностью, поэтому единственно верное направление противодействия угрозам кибербезопасности — государственно-частное партнерство»[19].

Поскольку информационные ресурсы в значительной степени создаются американскими информационно-телекоммуникационными гигантами, правительство США воспринимает любое препятствие их развитию, возникающее в других странах, как угрозу национальной экономической безопасности. Принятие международно-правовых норм, которые предлагаются международным сообществом, повлечет за собой введение различных мер на внутригосударственном уровне, что может препятствовать принципам свободной конкуренции на внутренних рынках. Американские телекоммуникационные компании, таким образом, могут потерять заметную

часть спроса, что, безусловно, негативно отразится на экономике Соединенных Штатов.

Вместе с тем международные противоречия, связанные с различными подходами к проблеме глобального управления информационным пространством, обострились в ходе попыток международного сообщества реформировать существующую систему управления Интернетом. В реальности информационное пространство и Интернет представляют собой сложнейшую систему, включающую как государственные, так и коммерческие элементы, существование и развитие которой зависит в меньшей степени от национальных правительств, но скорее от спроса со стороны населения и предложения, которое может быть реализовано в основном за счет частного сектора.

Реализация подобного подхода также осложняется рядом исторических особенностей развития Интернета. С момента создания и по сегодняшний день Соединенные Штаты обладают достаточно действенным механизмом управления Интернетом — Internet Corporation for Assigned Names and Numbers (ICANN). В 2009 г., с приходом президента Б. Обамы к власти, в ICANN прошли заметные реформы. Согласно новому доктринальному документу «Подтверждение обязательств» (Affirmation of Commitments), заключенному между министерством торговли США и ICANN, последняя получила бóльшую независимость. Кроме того, значительные полномочия в области управления Интернетом получил Правительственный консультативный комитет при ICANN (Government Advisory Committee).

В декабре 2012 г. в ходе Всемирной конференции по международной электросвязи произошла очередная попытка реформирования глобальной системы управления Интернетом на саммите Международного союза электросвязи (МСЭ) в Дубае. Принятый в ходе конференции международный документ [20] значительно расширяет полномочия органов государственного управления в сфере регулирования Интернета, а соответственно — и глобального управления информационным пространством. Принятие этого документа вызвало серьезное недовольство американских законодателей. Накануне конференции Конгресс единогласно принял резолюцию, осуждающую увеличение государственных полномочий в сфере информации [21]. А глава американской делегации на конференции МСЭ Терри Крамер заявил, что «будет активно противодействовать российским предложениям по реформе МСЭ», назвав российские предложения «самым большим разочарованием по сравнению с предложениями других стран» [22].

Обмен мнениями, происходивший в ходе конференции МСЭ между политическим руководством стран-участниц, подлил масла в огонь в сфере американо-китайских отношений. Китай принял сторону России и подписал новый регламент по управлению Интернетом. Это вызвало серьезную озабоченность американских властей.

Учитывая обострившиеся противоречия, перспективы сотрудничества России и США по вопросам информационной безопасности представлялись крайне сомнительными.

После ряда официальных визитов в июне 2011 г. было подготовлено совместное российско-американское заявление, посвященное вопросам кибербезопасности [23]. Обращает на себя внимание тот факт, что с американской стороны заявление подписано помощником президента США по кибербезопасности Говардом Шмидтом, с российской — заместителем секретаря Совета безопасности Николаем Климашиным. В заявлении говорится, что «взаимное понимание информационных угроз национальной безопасности способствует более эффективному взаимодействию между Россией и США в противодействии киберугрозам» [24].

В апреле 2013 г. состоялся визит в Москву сменившего Г. Шмидта на его посту Майкла Дэниела в составе

делегации Государственного департамента [25]. Судя по составу делегации, в ходе переговоров Соединенные Штаты не предполагали обсуждать военные вопросы международной информационной безопасности.

Спустя два месяца в ходе саммита «большой восьмерки» в Северной Ирландии Владимир Путин и Б. Обама подписали ряд документов, среди которых было заявление, посвященное проблемам кибербезопасности. В заявлении «О новой области сотрудничества в укреплении доверия» [26], в частности, декларировалось, что угроза национальному информационно-телекоммуникационному сектору является одной из самых серьезных угроз в XXI в. Эта угроза включает военно-политические и криминальные аспекты, особенно в данном контексте была выделена угроза терроризма. Сотрудничество России и Соединенных Штатов в этой сфере чрезвычайно актуально прежде всего для укрепления двустороннего понимания угроз информационной безопасности.

Президенты договорились создать механизм обмена информацией об угрозах кибербезопасности для защиты критически важных национальных информационных систем. В заявлении говорится о создании прямого канала связи между высокими должностными лицами в России и Соединенных Штатах для обмена такой информацией. Кроме того, было объявлено о создании двусторонней рабочей группы в рамках института президентских комиссий, которая должна быть создана в течение месяца и немедленно приступить к работе.

Очевидно, что проблема кибербезопасности становится новым приоритетом в повестке дня российско-американских отношений. Важно приложить усилия для того, чтобы глобальное информационное пространство стало сферой сотрудничества двух стран, но не конфронтации. Достигнутые в Северной Ирландии договоренности можно считать большим успехом в этой области, к тому же совместное заявление было подписано на фоне серьезных противоречий.

Косвенным образом разворачивающийся в настоящее время скандал вокруг бывшего сотрудника американских спецслужб Эдварда Сноудена может оказать негативное влияние на российско-американские отношения в сфере информационной безопасности.

Согласно информации, раскрытой Э. Сноуденом, американские спецслужбы получали различные данные от крупнейших американских телекоммуникационных гигантов. Отвечая на вопросы читателей The Guardian, Э. Сноуден упомянул Apple, Microsoft, Google, Skype, Facebook и пр. Общеизвестно, что практически каждый современный пользователь информационных технологий является клиентом хотя бы одной из упомянутых компаний. Каждая из них знакома и российскому пользователю.

Представить себе, каким количеством конфиденциальной информации обладали эти компании, не представляется возможным, так же как и оценить масштабы переданных в американские спецслужбы данных. Очевидно, что пользователями технологий и услуг упомянутых компаний являются далеко не только граждане США. Согласно утверждениям Э. Сноудена, программа PRISM получала информацию с серверов этих компаний напрямую [27].

В ходе расследований Конгресса ситуации вокруг программы PRISM и заявлений Э. Сноудена для объяснения были вызваны руководители всех американских спецслужб, имевших возможность получать доступ к конфиденциальным данным [28]. Командующий американским киберкомандованием и по совместительству директор Агентства национальной безопасности (АНБ) не отрицал фактов, разглашенных 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.

Управление национальной разведки опубликовало короткое заявление, в котором говорится, что деятельность американских спецслужб не использовалась в отношении американских граждан, но была предназначена для слежения за иностранцами за рубежом [29]. Таким образом, можно предположить, что действия американских спецслужб касались иностранных пользователей телекоммуникационных гигантов, среди которых немало граждан России. Подозрительным в данном контексте представляется, например, заявление Apple о том, что в список поисковых сервисов новой операционной системы iOS 7 включена российская компания «Яндекс».

Э. Сноуден принял решение остаться в Москве и, проведя почти месяц в международной зоне московского аэропорта, получил официальное временное разрешение на год находиться на территории России. Под угрозой оказался весь успех, достигнутый сторонами, причем не только по вопросам кибербезопасности, но и в других важнейших областях сотрудничества. Э. Сноуден стал поводом, который заметно осложнил российско-американские отношения, фактически нивелировав объявленную в 2009 г. «перезагрузку». Под угрозой срыва оказался российско-американский саммит, запланированный в ходе очередной встречи лидеров стран «большой двадцатки».

Оставаясь в России уже с официальным разрешением, Э. Сноуден продолжает подливать масла в огонь, в частности, заявив, что на территории Москвы находится главный шпионский сервер американских спецслужб, через который они получали информацию о россиянах [30]. Последующие его разоблачения о том, что помимо конфиденциальной информации «обычных» пользователей Агентство национальной безопасности (АНБ) имело доступ к информации мировых политических лидеров, окончательно сделали проблему секретных операций американских спецслужб одним из сложнейших вопросов международных отношений.

В свое оправдание представители телекоммуникационных компаний, оказавшихся участниками «сноуденгейта», заявили, что передавали информацию только при соответствующих запросах и с соблюдением всех необходимых юридических процедур, однако Э. Сноуден не утверждал, что передача сведений осуществлялась сознательно, — согласно его утверждениям, программа PRISM получала информацию с серверов этих компаний напрямую [31].

Нельзя исключать, что последующие разоблачения стали причиной объявления об отставке Кита Александера, главы АНБ и руководителя американского киберкомандования. Уже после объявления об отставке глава АНБ заявил, что «скорее согласится выслушивать критику, чем отменять программы, которые позволяют эффективно противодействовать угрозам национальной безопасности США» [32].

«Сноуденгейт» также продемонстрировал пробелы в международном праве, решение которых станет более сложной задачей. С сожалением придется признать и тот факт, что с развитием информационных технологий, с учетом того, что хранить секреты становится все сложнее, а получить различного рода информацию — все проще, доверия между государствами, нациями и другими субъектами международных отношений становится все меньше.

Нельзя исключать того, что международный скандал, вызванный разоблачениями Э. Сноудена, спровоцирует дальнейшее наращивание военного информационно-технологического оборонительного потенциала. Как представляется, необходимо усилить действия дипломатов, направленные на установление международного диалога по таким чувствительным вопросам.

ЗАКЛЮЧЕНИЕ

Основным приоритетом российско-американских отношений в сфере информационной безопасности является согласование позиций, поиск взаимовыгод-

ных путей сотрудничества в информационном пространстве.

Необходимо преодолеть наметившиеся противоречия, особенно обострившиеся в ходе саммита Международного союза электросвязи по управлению Интернетом.

Несмотря на инцидент с Э. Сноуденом, важно избежать эскалации конфликта в отношениях между Россией и Соединенными Штатами. Есть возможность использовать данный случай в качестве повода к развитию дальнейшего диалога по вопросам информационной безопасности.

Особое внимание стоит уделить военным вопросам кибербезопасности в двусторонних отношениях. Развитие кибервооружений может привести к новому витку гонки вооружений, изменению основ стратегической стабильности. Гонка кибервооружений будет непредсказуема в отличие от времен холодной войны и наращивания ядерного оружия.

России и Соединенным Штатам нельзя останавливаться на достигнутых в Северной Ирландии договоренностях. В условиях трансформации системы международных отношений и формирования полицентричного мира проблемы кибербезопасности приобретают иное значение.

В ближайшей перспективе необходимо прежде всего начать деятельность рабочих групп, создание которых предусмотрено российско-американским заявлением, подписанным в Северной Ирландии. Важно начать процесс обмена информацией о киберугрозах, а также принимать дальнейшие меры по укреплению доверия между двумя странами.

Примечания

[1] International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. — Washington D.C., May 2011.

[2] Department of Defense Strategy for Operating in Cyberspace. — Washington D.C., July 2011. — P. 10.

[3] International Strategy... — P. 14.

[4] Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee in Intelligence / J. R. Clapper, Director of National Intelligence // http://www.intelligence.senate.gov/120131/clapper.pdf. — Jan. 31, 2012.

[5] Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence / J. R. Clapper, Director of National Intelligence // http://www.intelligence.senate.gov/130312/clapper.pdf. — Mar. 12, 2013.

[6] *Pellerin Ch.* Panetta: Regional Defense, Cyber Highlight AUSMIN Talks American Forces Press Service // http://www.defense.gov/news/newsarticle.aspx?id=65337.

[7] Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government. — Lisbon, 19 Nov., 2010.

[8] Lisbon Summit Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council. — Lisbon, 20 Nov., 2010.

[9] Tallinn Manual on the International law applicable to cyber warfare / Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence; General Editor Michael N. Schmitt. — New York: Cambridge Univ. Press, 2013. — P. 25.

[10] Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting // http://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china-. — June 8, 2013.

[11] Стратегия национальной безопасности Российской Федерации до 2020 года. Утверждена указом президента Российской Федерации от 12 мая 2009 г. № 537 (http://www.scrf.gov.ru/documents/1/99.html).

[12] Концепция внешней политики Российской Федерации. Утверждена президентом Российской Федерации В. В. Путиным 12 февраля 2013 г. (http://mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/c32577ca0017434944257b160051bf7f!OpenDocument).

[13] НТР и мировая политика / Под ред. А. В. Бирюкова, А. В. Крутских. — М.: МГИМО-Университет, 2010. — С. 122.

[14] Там же. — С. 129.

[15] Инновационные направления современных международных отношений / Под общ. ред. д-ра ист. наук проф. А. В. Крутских. — М.: Аспект Пресс, 2010. — С. 144.

[16] См., например: http://www.dkb.gov.ru/session_fortnight/a.htm.

[17] См. подробнее: *Sternstein A.* Cyber early warning deal collapses after Russia balks // NextGov. — 2012. — Dec. 7 (http://cdn.nextgov.com/nextgov/interstitial.html?rf=http%3A%2F%2Fwww.nextgov.com%2Fcybersecurity%2F2012%2F12%2Fcyber-early-warning-deal-collapses-after-russia-balks%2F60035%2F).

[18] Конвенция об обеспечении международной информационной безопасности (концепция) // http://mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument.

[19] Multi-industry Letter to Speaker Boehner & Minority Leader Pelosi on CISPA // http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/MultiIndustryHouseCybersecurityBoehnerPelosi.pdf. — Apr. 17, 2012.

[20] Final Acts of the World Conference on International Telecommunications (Dubai, 2012) // http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf.

[21] S. CON. RES. 50: Expressing the sense of Congress regarding actions to preserve and advance the multistakeholder governance model under which the Internet has thrived // http://www.foreign.senate.gov/imo/media/doc/S%20Con%20Res%2050.pdf.

[22] Amb. Kramer on International Telecommunications Conference // http://translations.state.gov/st/english/texttrans/2012/11/20121129139303.html#ixzz2UZwOi5wW 29. — Nov. 2012.

[23] Joint Statement by Cybersecurity Coordinator Schmidt and Deputy Secretary Klimashin. — Washington D.C., 23 June 2011.

[24] Ibid.

[25] http://www.kommersant.ru/pda/kommersant.html?id=2181665.

[26] Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия // http://news.kremlin.ru/ref_notes/1479. — 17 июня 2013 г.

[27] Edward Snowden identifies himself as source of NSA leaks — as it happened // The Guardian. — 2013. — 9 June (http://www.guardian.co.uk/world/2013/jun/09/nsa-secret-surveillance-lawmakers-live?INTCMP=SRCH).

[28] How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries // http://intelligence.house.gov/hearing/how-disclosed-nsa-programs-protect-americans-and-why-disclosure-aids-our-adversaries. — June 18, 2013.

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

[30] *Дорохов Р., Никольский А.* Шпион в центре Москвы // Ведомости. — 2013. — 12 авг. (http://www.vedomosti.ru/newspaper/article/507181/shpion-v-centre-moskvy).

[31] Edward Snowden identifies himself as source of NSA leaks — as it happened // The Guardian. — 2013. — June 9 (http://www.guardian.co.uk/world/2013/jun/09/nsa-secret-surveillance-lawmakers-live?INTCMP=SRCH).

[32] *Ackerman S.* Embattled NSA chief Keith Alexander rejects calls to limit agency's power Alexander goes before House committee and claims reports of NSA collecting millions of phone calls were 'absolutely false' // The Guardian. — 2013. — Oct. 29 (http://www.theguardian.com/world/2013/oct/29/nsa-chief-keith-alexander-house-hearing).
