Олег Демидов

СОЦИАЛЬНЫЕ СЕТЕВЫЕ СЕРВИСЫ В КОНТЕКСТЕ МЕЖДУНАРОДНОЙ И НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ[1]

Весной 2011 г. страны Магриба и Ближнего Востока захлестнула небывалая волна социальных протестов, повлекшая за собой отставку режимов в одних странах, репрессии вперемежку с лихорадочными реформами в других, а кое-где — гражданскую войну и фактический крах государственности. Эти события, отозвавшиеся эхом на огромном пространстве от Судана до Белоруссии, стали известны как *Арабская весна* и *твиттер/фейсбук-революции*. Второе из упомянутых названий отражает черту, характерную для большинства эпизодов ближневосточных протестов, — беспрецедентно активное использование участниками протестов информационно-коммуникационных технологий (ИКТ), и в первую очередь социальных сетевых сервисов. После волнений 2009 г. в Иране и Молдавии в рядах политиков, экспертов и СМИ прочно закрепился дискурс «ИКТ (и прежде всего соцсети) как главный двигатель волнений и революций *Арабской весны*».

Безобидная технология, призванная упростить досужее общение, приобрела черты оружия массового уничтожения (ОМУ), угрожающего стабильности и безопасности отдельных стран и международного сообщества в целом. Споры о роли социальных сетей в *Арабской весне* сегодня определяют основную суть дискуссии вокруг них, однако круг связанных с ними вопросов в рамках проблематики безопасности, конечно, гораздо шире.

Задача этой статьи состоит в том, чтобы проанализировать социальные сетевые сервисы и их влияние на развитие современного мира с позиций безопасности. Ключевой вопрос состоит в том, каким образом следует, с учетом тенденций последних лет, а также недавних и продолжающихся *революций онлайн* на Ближнем Востоке и в других регионах, рассматривать влияние социальных сетевых сервисов на международную безопасность, а также на национальную безопасность РФ. Этот вопрос влечет за собой еще два вопроса, первый из них — стоит ли рассматривать социальные сетевые сервисы как вызов, угрозу, либо, напротив, потенциальный фактор укрепления безопасности и технологию, способствующую ее обеспечению? Второй вопрос, рассматриваемый прежде всего на примере России, касается того, каков должен быть государственный политический курс, призванный учитывать развитие сетевых интернет-технологий и использовать его для укрепления безопасности.

Наконец, отдельным вопросам в рамках анализа является рассмотрение курса США в области использования ИКТ, и в том числе социальных сетевых сервисов для решения задач внешней политики. В частности, предпринимается попытка определить, несет ли подход Соединенных Штатов вызовы для международной безопасности, и если да, то в какой мере они обусловлены акцентом на использование социальных сетей и подобных им технологий.

Анализ упомянутой проблематики ведется с политологической точки зрения, не претендуя на правовую и техническую экспертизу. Рассмотрение социальных сетей в контексте безопасности, вынесенное в заголовок статьи, предполагает уход от правовых акцентов, рассмотрение и употребление таких понятий, как «национальная безопасность», «международная безопасность», вне специфического правового контекста. Технические аспекты проблематики смещены на задний план либо опущены в силу того, что не являются основным объектом анализа и требуют отдельных исследований. Они рассматриваются лишь в той мере, в которой необходимы для понимания изучаемой проблематики.

СОЦИАЛЬНЫЕ СЕТЕВЫЕ СЕРВИСЫ — ГРАНИЦЫ ПОНЯТИЯ

Объектом анализа в статье выступают социальные сетевые сервисы, хотя такая формулировка не является единственно приемлемой для рассматриваемого явления. Употребляются и такие термины, как «социальные сети», «социальные сетевые сообщества» и «социальные медиа». Во всех случаях речь идет о совокупности виртуальных сервисов и платформ, функцией которых является создание горизонтальных (т.е. сетевых) социальных связей между их пользователями. Русскоязычные обозначения являются кальками англоязычных терминов (social networking services, social network sites), более точно отражающих суть данного явления. В техническом смысле социальные сетевые сервисы являют собой классический пример Web 2.0. Так зачастую называют принцип проектирования систем, которые улучшаются и совершенствуются за счет возможностей сетевого взаимодействия и участия в нем широкого, не ограниченного изначально круга пользователей.

Единственное необходимое уточнение касается внутренней классификации социальных сервисов и ее оснований. В рамках статьи выделяются две категории таких сервисов:

а) собственно социальные сети — как универсальные, так и специализированные, профессиональные (*Facebook*, *Одноклассники*, *ВКонтакте*, *LinkedIn*, *MySpace*, *Friendster*, *Google+* и пр.);

б) квазисоциальные сообщества (блоговые сообщества, микроблоговые сервисы (*Twitter*), сообщества на интерактивных платформах типа *Ushahidi* и т. д. — данный перечень является открытым).

Провести четкое разграничение между обозначенными категориями достаточно сложно. Те же блоги могут быть лишь отдельным сервисом в рамках социальных комьюнити, обычные сайты могут иметь развитые социальные закладки, геосоциальные сети могут работать просто как сервис определения местонахождения, а могут приобретать полноценные социальные функции.

Можно лишь выделить тот перечень характеристик, которые в совокупности позволяют назвать тот или иной сервис социальной сетью. Подобный перечень был сформирован в еще в 2008 г. в примечательном исследовании *Social Network Sites: Definition, History, and Scholarship*. Его авторы выделили три ключевые характеристики *сайта социальной сети* (social network site)[2]. Речь идет о возможности создания личного профиля пользователя, хотя бы частично открытого для других людей, управлении списком пользователей, с которыми поддерживается связь, и возможности просмотра и отслеживания связей других пользователей.

Приведенный перечень, вероятно, нуждается в единственном уточнении: характеристики профиля пользователя должны иметь значение для социальной коммуникации. Геолокационный сервис не будет геосоциальной сетью, если к возможности определения координат пользователей не добавить их социально значимые характеристики — пол, возраст, хобби, цель посещения тех или иных локаций и т. д. Соответственно, все те сетевые сервисы, в которых отсутствуют какие-либо из перечисленных возможностей, относятся к *квазисоциальным сетям*.

Подобная классификация носит общий характер и не отражает многочисленных технологических нюансов, однако она допустима для целей этого исследования. Более подробная классификация социальных сетевых сервисов представлена в исследовании IEEE Computer Society за 2008 г.[3].

РЕВОЛЮЦИИ *ОНЛАЙН*, КОТОРЫЕ ТАК И НЕ ПРОИЗОШЛИ

На сегодняшний день, по прошествии полутора лет с начала событий *Арабской весны*, первоначальный энтузиазм и ажиотаж вокруг социальных сетевых сервисов как основной движущей силы революций на Ближнем Востоке и в Северной Африке поутихли как в глобальных СМИ, так и среди экспертов. В числе последних — исследователи Центра Беркмана по изучению интернета и общества при Гарвардском университете — одного из ведущих центров по изучению социальных сетей и новых интернет-сервисов: Этан Цукерман, Дана Бойд, Джиллиан Йорк, Майк Ананни и Бет Колеман. На скептических позициях также стоят отечественные исследователи, в числе которых нужно отдельно упомянуть эксперта ИМЭМО РАН Е. А. Степанову, посвятившую отдельное исследование роли ИКТ в *Арабской весне*[4].

Обобщенная позиция экспертных кругов РФ и Запада сводится к тому, что социальные сети не сыграли ведущей роли в событиях *Арабской весны*, они не были доминирующим каналом коммуникации оппозиционных сил и участников протестов. Вместе с тем они частично придали событиям в арабских странах ту скорость и динамику, которая застала врасплох их оппонентов — правительства и поддерживающие их силы. Как справедливо отметил на страницах газеты *Коммерсантъ* автор термина *твиттер-революция*, сотрудник Стэнфордского университета Евгений Морозов (Evgeny Morozov), без социальных сетей революции в арабских странах «однозначно произошли бы по-иному»[5].

Но можно ли утверждать, что социальные сети сыграли принципиальную и, главное, самостоятельную роль в развитии событий *Арабской весны*? На мой взгляд, такое утверждение неверно как минимум по следующим причинам:

1. Протестная деятельность по отношению к социальным сетевым сервисам носила преимущественно самодостаточный и независимый характер, а вот обратное утверждение неверно. События *Арабской весны* и, в меньшей степени, неудавшаяся попытка *революции онлайн* в Белоруссии в 2011 г. дают несколько оснований для такого вывода. Во-первых, протестная активность онлайн и реальные, уличные действия, сформировавшие революцию, разнятся по пику своей активности и не полностью совпадают во времени. Как отмечал бывший председатель правления Союза директоров ИТ России А. В. Коротков, «уличные акции в Египте продолжались и в отсутствие сколь бы то ни было значимого влияния интернет-коммуникаций». Зеркальный пример: в Сирии объявленные в *Facebook* дни гнева в 2011 г. не переходили в масштабные уличные акции, все изменилось лишь после произведенных властями арестов подростков, спровоцировавших массовые столкновения.

2. Протесты были и там, где активность в социальных сетях была близка к нулевой. Однако при этом протесты в тех государствах, где использование ИКТ было максимально активным, проходили по более мягкому сценарию. Некоторые эксперты считают такую корреляцию следствием *гуманизирующей* роли интернета. Однако в действительности причинно-следственная связь скорее носила обратный характер. Чем более развито государство в социально-экономическом отношении и чем либеральнее относится режим к свободе коммуникации, тем выше уровень проникновения ИКТ, включая социальные сети. Примеры Ливии и Йемена как государств, которые обладают весьма низкими показателями проникновения интернета даже по региональным меркам (менее 20%) и при

этом стали ареной весьма ожесточенных и массовых акций протеста, а потом и вооруженной борьбы, говорят сами за себя.

3. Социальные сети не были ни единственным, ни даже ключевым средством коммуникации и координации действий повстанцев. При этом, однако, они были основным средством популяризации их движений и публичного контакта с внешним миром — в отличие от спутникового телевидения, мобильной связи, СМС, мечетей и всех остальных площадок коммуникации. В египетских провинциях, равно как и в Каире, главной площадкой для координации действий протестующих и распространения их настроений были мечети, сразу по окончании пятничных намазов превращавшиеся в своеобразные командные пункты участников протестных движений. Точно так же ситуация обстояла и во всех странах региона с малозначительными нюансами.

4. Та же *рецептура* протестной онлайн-активности с акцентом на социальные сети, которая сопровождала и подкрепляла развитие событий в арабских странах, не привела к запуску аналогичного сценария в Беларуси. Хотя лидер оппозиционного «Движения будущего» Вячеслав Дианов уповает на технологии социальных сетей и микроблогов, акции его активистов за 2011 г. так и не вышли за рамки локальных. Это еще раз подтверждает тезис о том, что все решают не коммуникации сами по себе, а социально-политический фон и содержание процессов, развивающихся в той или иной стране. Оказавшись вне специфической среды Ближнего Востока и Магриба, где революции были подготовлены социально-политическими процессами, вызревавшими в течение десятилетий, отточенная технология координируемого через сети протеста дала сбой и утратила эффективность.

Кроме того, сами социальные сети в *Арабской весне* не проявили себя в качестве субъектов корпоративных интересов, подобных крупным транснациональным корпорациям (ТНК). Их руководство и менеджмент не пытались управлять протестной активностью или хотя бы направлять ее. Менеджер *Google* Ваиль Гоним [Wael Ghonim], названный СМИ «международным лицом египетской революции»[6], действовал сугубо как частное лицо, с 2010 г. развивая деятельность протестного сообщества (страница *We are all Khaled Said*) на платформе главного конкурента своего работодателя — *Facebook*. При этом г-н Гоним не координировал свою деятельность с представителями *Facebook*, хотя и выражал надежду встретиться с Марком Цукербергом, чтобы поблагодарить его за возможности, которые *Facebook* предоставила египтянам. Более того, свою деятельность в качестве интернет-активиста топ-менеджер *Google* на Ближнем Востоке поначалу осуществлял параллельно с исполнением своих обычных рабочих обязанностей в *Google*, ведя, по его собственному признанию, двойную жизнь. Эти факты зачастую упускаются из виду теми комментаторами, которые пытаются изображать *Арабскую весну* 2011–2012 гг. как искусственный и управляемый процесс, в той или иной мере спровоцированный гигантами ИТ-индустрии.

При этом любопытно, что подобные точки зрения озвучивали представители самых высших эшелонов российской власти. Так, 22 февраля 2011 г. президент России Д. А. Медведев в разгар протестов в Египте назвал происходящее сценарием, который «они раньше для нас готовили»[7]. Еще дальше пошел И. И. Сечин, на тот момент занимавший пост вице-премьера РФ, заявив в интервью *The Wall Street Journal*: «Надо пристальнее изучить происшедшее в Египте. Посмотреть, что делали в Египте, скажем, высокопоставленные руководители *Google*, какие там были манипуляции с энергией народа»[8]. Такая интерпретация событий *Арабской весны* может служить тревожным признаком, сигнализирующим о непонимании либо игнорировании реальных роли и места социальных сетевых сервисов в общественно-политических процессах.

Рассмотренные выше ситуации и примеры позволяют утверждать, что на сегодня социальные сетевые сервисы как разновидность сетевых технологий, а также их аудитория как специфическая самоорганизующаяся общность едва ли представляют угрозу безопасности как на уровне отдельных государств, так и на международном уровне. Соответственно, дискуссия относительно того, как следует реагировать на вызовы безопасности, исходящие от социальных сетей, представляет собой не совсем корректную постановку вопроса. Этот посыл может быть актуален для политического руководства РФ при рассмотрении ими проблематики социальных сетей. Искать возможные вызовы безопасности в связи с развитием социальных сетевых сервисов стоит не в их технологии, замыслах их руководства и уж точно не в действиях их пользователей.

СТРАТЕГИЯ США В КИБЕРПРОСТРАНСТВЕ И СОЦИАЛЬНЫХ СЕТЯХ: ВЫЗОВЫ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

При анализе *Арабской весны*, как и ее своеобразных *афтершоков* за пределами Ближнего Востока, национальные государства и их правительства обычно изображаются пассивными *жертвами* технологий сетевых сервисов, активно используемых участниками протестов. Действия госструктур рассматриваются лишь в плоскости реакции на угрозы, якобы исходившие из интернета. Исключением являются США, которым часто приписывается роль тайного организатора и режиссера *Арабской весны*.

В России версия о причастности США к революциям на Ближнем Востоке через тайные каналы влияния, такие как социальные сети, находит благодатную почву по ряду причин. Играет роль недоверие к Вашингтону и традиционно сильные антиамериканские настроения среди представителей российской элиты. Кроме того, комбинация антиамериканизма и очередной вариации теории заговора дает определенные политические очки политическим движениям левого толка, позиции которых в России лишь усиливаются. Наконец, склонность видеть в глобальных процессах, подобных *Арабской весне*, срежиссированные кем-то геополитические сценарии во многом исходит от непонимания подлинных причин таких процессов и некорректной оценки их потенциального влияния на Россию и ее союзников. Пытаясь определить возможное направление угрозы, политический истеблишмент в первую очередь смотрит туда, куда более всего привык смотреть со времен СССР — по другую сторону Атлантики.

Однако серьезной критики версия о наличии в *Арабской весне* элемента управляемости и координации ее событий из Вашингтона не выдерживает. Первая официальная реакция руководства США на события в Тунисе и Египте весной 2011 г. продемонстрировала растерянность Белого Дома и склонность к осторожной, выжидательной тактике. Поначалу президент США Барак Обама высказывался в поддержку режима Хосни Мубарака как оплота стабильности на Ближнем Востоке и ключевого партнера Вашингтона в регионе. Этот пример весьма показателен на фоне того, что революции *Арабской весны* не состоялись или не достигли цели там, где свержение режимов в наибольшей степени отвечает интересам США — а именно в Иране, — однако поставило под удар многие стратегические интересы США на Ближнем Востоке.

Так, свержение Мубарака лишило Вашингтон давнего союзника, занимавшего благоприятные для Белого дома позиции по вопросам борьбы с исламским фундаментализмом, палестино-израильского урегулирования, противодействия международному терроризму. События в Ливии втянули Вашингтон в военную кампанию, совершенно не нужную президенту Обаме на фоне войны в Афганистане и приближения выборов. Волнения на Аравийском полуострове затронули *жизненно важные* для США вопросы: стабильность поставок нефти из Саудовской Аравии, лояльность режима саудитов, выступающего главным противовесом Ирану, а также беспрепятственное размещение американских военных баз на Аравийском полуострове. Чтобы отразить масштаб интересов США в отношениях с саудитами,

достаточно сказать, что в 2010 г. Эр-Рияд объявил о долгосрочном плане закупок вооружений у Вашингтона на общую сумму в 60 млрд долл.

Наконец, общим для арабского мира итогом революций стал прорыв наружу аккумулированного за предыдущее десятилетие антиамериканизма и антивестернизма. В 2012 г. Белый дом попал в незавидной ситуации, на словах приветствуя «торжество свободы» в Египте и Тунисе и с тревогой ожидая дальнейшего усиления исламистов, после того, как прошедшие парламентские выборы в основном подтвердили рост их влияния в этих странах.

В общем и целом тезис о причастности США к *Арабской весне* лишен серьезных оснований. В то же время его сторонники вполне справедливо фиксируют острый интерес Вашингтона к *возможности* осуществления подобных трансформаций в управляемом режиме. Однако не стоит забывать, что, поневоле играя роль *объекта*, ощущающего на себе последствия развития ИКТ, государства в то же время являются и *субъектом*, который пытается освоить эти возможности и технологии (включая технологии сетевых сервисов) и превратить их в инструмент реализации своего политического курса.

Возможности социальных сетевых сервисов в социально-политическом, военном и иных аспектах не могут не привлекать Соединенные Штаты, которые всегда играли особую роль в развитии интернета. Являясь создателями Сети и сохраняя частичный контроль над корневыми DNS-серверами через ICANN[9], США сохраняют определенную преемственность своей политики. Вашингтон демонстрирует элементы *миссионерского* подхода к вопросам, связанным с интернетом, в частности продвижению свободы слова в Сети и обеспечению беспрепятственного доступа к ней населения каждой из стран. Даже тот факт, что технологии социальных сетей вдруг преподнесли своей родине неприятный сюрприз, поставив под удар ее интересы на Ближнем Востоке, не влияет на фундаментальные подходы Белого дома к данным вопросам. Хотя политика Вашингтона в области киберпространства выходит далеко за рамки тематики социальных сетевых сервисов, ее анализ все же необходим, так как отдельные грани проблемы (подобные социальным сетям в контексте безопасности) нельзя рассматривать, не видя общей картины.

Своеобразной *презентацией* американского курса в отношении интернета на высоком уровне можно считать выступления Госсекретаря США Хиллари Клинтон по проблематике интернет-пространства, которые состоялись дважды, с интервалом чуть больше года — 21 января 2010 г. и 15 февраля 2011 г., всегда порождая немалый резонанс в СМИ и экспертном сообществе. Наибольший интерес представляет вторая речь «Интернет, за и против: выбор и вызовы в мире, связанном глобальной сетью». Во-первых, в ней нашли комплексное отражение события *Арабской весны*, по ключевым аспектам которой, включая роль ИКТ, администрация Обамы до этого давала лишь разрозненные и хаотичные комментарии, за которыми не было видно целостной позиции. Во-вторых, озвученные в выступлении г-жи Клинтон инициативы простираются далеко за рамки президентского срока Барака Обамы, что свидетельствует о серьезности курса Белого дома. В-третьих, в отличие от 2010 г. февральская речь оказалась весьма насыщена анонсами конкретных программ и проектов, в значительной степени завязанных на социальные сервисы и родственные им технологии.

Кроме того, взгляды Белого дома на развитие киберпространства уже в полной мере находят отражение в доктринальных документах американских ведомств. В числе последних следует упомянуть прежде всего Международную стратегию по действиям в киберпространстве [International Strategy for Cyberspace], опубликованную Белым домом 16 мая 2011 г. Ее своеобразным логическим развитием в военной плоскости стала Стратегия Министерства обороны по действиям в киберпространстве [Department of Defense Strategy for Operating in Cyberspace], частично рассекреченная в июне 2011 г. В совокупности с рядом крупных проектов в области киберпространства, о которых прессе стало известно в мае-июле

2011 г., принятие киберстратегий позволяет говорить о том, что проблематика интернета выходит на принципиально новый уровень в повестке Белого дома — и в первую очередь в плоскости безопасности. Можно выделить несколько принципов, на которых опирается нынешнее «признание киберпространства»[10] на высшем уровне и которые напрямую затрагивают социальные сетевые сервисы, хотя и не ограничиваются ими.

В первую очередь речь идет о закреплении и индоктринации курса Вашингтона на «глобальную войну с цензурой в интернете»[11]. Свобода в интернете стала идеологическим стержнем речи Госсекретаря и доминирующей идеологемой Вашингтона в отношении киберпространства в целом[12]. В плане предлагаемых лозунгов и ценностей Соединенные Штаты не слишком выделяются из ряда других государств, преимущественно членов ЕС, обладающих развитым ИКТ-сектором. В частности, такие страны, как Эстония, Греция, Финляндия, уже в течение нескольких лет признают доступ в интернет неотъемлемым правом человека, выступая против каких-либо его ограничений, включая цензуру, а не так давно этот тезис получил внушительную поддержку и на международном уровне. 7 июня 2011 г. был опубликован доклад ООН, в котором признается в качестве одного из неотъемлемых право на доступ в интернет[13]. От положений международной киберстратегии Вашингтона данный перечень отличает лишь отсутствие в нем прямой увязки права на доступ в интернет с демократическими ценностями.

Подход Вашингтона можно было бы рассматривать в сугубо положительном ключе, несмотря даже на характерное для США стремление увязывать развитие ИКТ со становлением демократических институтов. Но, как известно, дьявол кроется в деталях. Разделяя общепринятые ценности и преследуя близкие многим государствам цели политики в отношении интернета, США берут на себя чрезмерно амбициозную роль и опасно раздвигают рамки допустимых мер по реализации этой политики. Так, потенциальные риски для международной безопасности представляет принцип экстерриториальности борьбы США за свободу и безопасность в киберпространстве. Его чеканная формулировка прозвучала в февральской речи Хиллари Клинтон: «США защищают свободу [общения в интернете] повсюду и призывают все остальные страны к тому же»[14]. Более того, Госсекретарь не преминула привести список государств — «врагов свободного интернета», на которые будут в первую очередь направлены инициативы ее ведомства. Любопытно, что в список, включающий Сирию, Иран, Китай, Кубу и Вьетнам, попали две страны из бывшего перечня государств-изгоев [rogue states], актуального при администрации Джорджа Буша-младшего. Эта деталь высвечивает определенную параллель между риторикой г-жи Клинтон и догмой Буша-младшего о «демократии на марше». В обоих случаях в основе лежит видение США как проводника тех или иных универсальных ценностей, имеющего право на односторонние превентивные действия в отношении государств, их не разделяющих.

Однако доктринальные документы могут оказывать реальное влияние на ситуацию в области безопасности лишь в том случае, когда их положения и принципы получают практическое наполнение и отражаются в конкретных проектах и инициативах. Реализация курса, заложенного в американских программных стратегиях и выступлениях, является *лакмусовой бумажкой*, определяющей, будет ли реализован тот потенциал влияния на международную безопасность, который в них заложен.

На сегодняшний день можно выделить две группы проектов, которые позволяют утвердительно ответить на этот вопрос. В центре этих проектов оказываются технологии мобильной связи, а также инструменты Web 2.0, прежде всего социальные сетевые сервисы. К сожалению, в обоих случаях уместно говорить о том, что инициативы Вашингтона несут в себе значительный негативный потенциал для международной безопасности.

Во-первых, речь идет о проектах Госдепартамента по созданию так называемых *теневых* систем мобильной и интернет-связи для поддержки оппозиции в авторитарных государствах. Информация о них появилась в июне 2011 г., опять же

в контексте *Арабской весны,* однако соответствующие планы ведомства были четко обозначены еще в выступлении Госсекретаря Хиллари Клинтон в феврале 2011 г. Одна из разработок связана с усовершенствованием технологии Bluetooth, которое позволит создать систему автоматизированного распространения текста и мультимедийного контента по скрытой сети из «доверенных пользователей»[15]. Еще один проект, также находящийся в стадии реализации, предполагает строительство автономных сетей мобильной связи, способных обеспечивать покрытие на территории, не подконтрольной США и их союзникам. Отрабатывая подобную технологию на своих военных базах в Афганистане, США заимствуют опыт жителей КНДР, использующих китайские приграничные сотовые вышки для передачи сообщений через мобильные телефоны[16].

Не менее активно развиваются проекты, призванные обеспечить оппозиции возможность доступа в интернет в обход контролируемых государством сетей. Наиболее примечательным из них является так называемый *интернет в чемоданчике*, предполагающий создание компактного устройства, которое можно незаметно ввезти в страну и развернуть с помощью него сеть с выходом в интернет и довольно обширным покрытием. По словам представителей интернациональной команды разработчиков проекта из 12 стран, речь идет об «изолированной сетевой инфраструктуре, которую невозможно контролировать, нельзя отследить и очень трудно уничтожить»[17]. Систему также предполагается снабдить технологией, мешающей идентификации пользователя. *Чемоданчик* должен позволить оппозиции в авторитарных государствах координировать свои действия онлайн и поддерживать связь с миром даже в условиях полной блокировки интернета государством. Госдепартамент не скрывает, что основной задачей тех групп и движений, которым планируется предоставлять доступ к данной технологии, является «подрыв репрессивных режимов»[18].

Такая риторика указывает на то, что в Белом доме ищут возможность повторить *Арабскую весну* в управляемом варианте — в нужной стране и в нужное время, причем в основном с помощью интернета и мобильной связи. Прежде всего такая тактика способствует дестабилизации обстановки в тех странах, где она применяется. Например, в Иране, который является первоочередной мишенью Госдепартамента в связи с эскалацией кризиса вокруг ядерной программы Тегерана, каждый всплеск протестов приводил к новому витку репрессий и кровопролитию, приближая ситуацию к опасному тупику и социальному взрыву. Режимы, которые Белый дом хочет *подорвать* в первую очередь, не похожи на режимы Бен Али в Тунисе и даже Хосни Мубарака в Египте — по уровню авторитаризма и готовности применять силовой ресурс в целях самосохранения они стоят куда ближе к свергнутому режиму Муаммара Каддафи в Ливии. Все, чего можно достичь с помощью *чемоданчика* в Иране, Китае, Туркмении и прочих нелюбимых Вашингтоном *автократиях*, это спровоцировать новую волну насилия с неясным исходом, но никак не добиться торжества свобод, о которых говорит г-жа Клинтон.

Ярким примером служит развитие событий в Сирии, где противостояние повстанцев и режима Башара Асада, начавшееся с мирных акций протеста, к середине 2012 г. вылилось в полномасштабную гражданскую войну. Хотя США не использовали против режима Асада секретные ИКТ-разработки, предпочитая традиционные методы влияния на ход внутреннего конфликта (в том числе инструктаж повстанцев и массированную информационную поддержку по всему спектру от официальной дипломатической риторики до тех же социальных сетей), важен сам итог такого подхода. Ситуация в Сирии в целом не лежит на совести Белого дома, но вклад в эскалацию насилия и расширение его масштабов, по-видимому, все же был сделан. Применение более изощренных инструментов, подобных описанным проектам в области интернет-технологий, ничем не изменило бы ситуацию. То же будет верно, если говорить о гипотетических вариантах применения *интернет-чемоданчика* для подогрева протестных настроений в Иране и любой другой стране.

Еще больше вопросов вызывают инициативы Пентагона, получившие название *SMISC* (Социальные медиа в стратегической коммуникации). В рамках проекта делается фокус исключительно на сетевые социальные сервисы; целью его является использование социальных сетей, видеохостингов и микроблогов в целях разведки, контрразведки и ведения информационно-пропагандистской борьбы. Проект предполагает использование социальных сетей напрямую в военных целях, информация о нем появилась в открытых источниках в июле 2011 г., вскоре после частичного обнародования военной киберстратегии Пентагона. Достаточно изощренная с технологической точки зрения концепция предполагает разработку специальной программы, которая, будучи неким образом развернута в крупнейших сетевых сервисах (*Facebook, Twitter, YouTube*), позволит осуществлять широкий спектр задач, де-факто лежащих в плоскости военной разведки. В числе прочего программа должна позволять военным и спецслужбам «противодействовать враждебным кампаниям влияния с помощью контрсообщений, отслеживать враждебную по отношению к США пропаганду и помогать вести контрпропаганду»[19].

Система, разработка которой является целью гранта Управления перспективных научно-исследовательских разработок Минобороны США (более известна как DARPA), ориентирована на чрезвычайно широкий круг задач. В частности, в ее функции входят обнаружение, классификация и анализ появляющихся в социальных сетях сообщений на предмет наличия в них информации, имеющей ценность для военной разведки или представляющей опасность для США. К такой информации относятся сведения о морально-психологическом состоянии военнослужащих и различных групп населения отдельных стран и регионов, общественные тенденции, новые идеи или планирующиеся события, а также факты распространения недружественной пропаганды и дезинформации[20]. Несмотря на то что проект можно назвать технологически прогрессивным и даже задающим новые стандарты обработки информации в сетевых сервисах, его влияние на международную безопасность и развитие интернета следует признать деструктивным по целому ряду соображений.

Прежде всего вызывают серьезные сомнения надежность и достоверность информации, получаемой в результате подобного проекта. Ставящиеся задачи исключительно сложны даже при использовании традиционных методов разведывательной и контрпропагандистской деятельности. При осуществлении же таких задач в киберпространстве на порядок вырастает риск дезинформации, информационных помех и неверной интерпретации полученных данных. Разведывательная деятельность Пентагона через социальные сети может быть достаточно легко *обессмыслена* путем массового создания в социальных сетях бот-акканутов военнослужащих, и это лишь одно из возможных решений.

Подобное препятствие останется проблемой самих Соединенных Штатов, но лишь до тех пор, пока на основе этих данных не будут приниматься военно-стратегические решения. Недостаточно тщательный анализ данных из соцсетей в этом случае может стать причиной искаженных, неверных оценок военными и спецслужбами США ситуации в других странах, протекающих в их обществах процессов, отношения их социальных групп к Соединенным Штатам. В случае дипломатических кризисов и конфликтных ситуаций подобная информация может стать одним из факторов, толкающих руководство США к жесткой реакции, эскалации кризиса — словом, привести к ошибке в стратегических решениях, что несомненно отразится на международной безопасности.

Второй негативной стороной *SMISC* является то, что инициативы Пентагона не могут не беспокоить другие государства и не провоцировать их ответную реакцию. Есть все основания полагать, что эта реакция будет носить весьма негативный характер как в смысле международной безопасности, так и в плане продвижения свободы в интернете, за которое столь активно выступает Белый дом. Своей политикой США в лице Пентагона дают крупный козырь в руки изоляционистским режимам и вообще сторонникам управляемого и жестко регулируемого

интернета. В этом смысле стоит согласиться с экспертом российского интернет-сообщества А. Сидоренко, по словам которого «резкая политизация интернета играет на руку как раз авторитарным режимам, которые стремятся интернет плотно контролировать»[21].

Наконец, инициатива Пентагона, получив широкую огласку, бьет по самим социальным сетям, представляя их как потенциальные инструменты тайных военных программ. Это может стать дополнительным фактором, под действием которого авторитарные режимы вновь усилят давление на компании, обеспечивающие деятельность социальных сетевых сервисов на их территории. В частности, такие тенденции можно прогнозировать в Китае, Иране и даже в России, где существуют мощные лоббистские группы, выступающие за более плотный контроль над интернет-коммуникациями и, одновременно, видящие в США едва ли не ключевой источник угроз национальной безопасности РФ. Хотя логика этих групп, преимущественно состоящих из высокопоставленных представителей силовых структур, страдает изъянами, их влияние бесспорно — его иллюстрацией может служить инициатива ФСБ о запрете сервисов *Skype, Hotmail* и *Gmail*, от которой так и не отказались с тех пор, как в 2010 г. она впервые была озвучена.

Таким образом, Россия также может пострадать от программ Пентагона, заплатив за вынужденные меры по обеспечению безопасности национального сегмента сети торможением его развития. По мнению экспертов, *SMISC* способны представлять реальные риски для национальной безопасности России. Как отметил главный редактор журнала *Национальная оборона* И.Ю. Коротченко, данные, публикуемые в российских сетях (например, в ныне уже неактивном сервисе «место службы» на *Одноклассниках* и многих других подобных ресурсах) представляют богатый источник развединформации[22].

Инициативы Госдепартамента и Пентагона делают курс США в отношении киберпространства в значительной степени антиконструктивным. При этом под удар попадают те самые ценности, которые США стремятся продвигать и поддерживать — свобода в интернете (включая свободу доступа), отсутствие цензуры и жесткого контроля со стороны государства, единство и гармоничное развитие киберпространства, беспрепятственное развитие интернет-компаний и технологий.

Американская доктрина в отношении интернета стоит на прогрессивном фундаменте, однако воплощается при помощи не совсем адекватного инструментария и с идеологическими перекосами. Пытаясь реагировать на угрозы, исходящие из киберпространства, Белый дом придает функцию военных и политических инструментов технологиям, которым она изначально не присуща. Социальные сервисы, в отличие от ARPANET и многих других достижений ИКТ, изначально развивались как общедоступное трансграничное средство общения. Использование их в тайных разведывательных и тем более военных целях во многом противоречит тем качествам, которые выдвинули их на авансцену развития сегодняшнего глобального интернет-сообщества.

Неосмотрительные инициативы Вашингтона, таким образом, подстегивают процесс, который в случае своего дальнейшего развития может вылиться в полномасштабную *милитаризацию киберпространства*, способную стать одной из серьезных международных проблем наряду с милитаризацией космоса. Текущие тенденции свидетельствуют о том, что США стремятся не столько к тому, чтобы остановить этот процесс, сколько к тому, чтобы обеспечить себе позицию лидера в данном направлении. Притом что социальные сетевые сервисы оказываются на острие стратегий Белого дома, их применение в описанных выше целях действительно претендует на статус нового серьезного вызова международной безопасности, хотя вне контекста государственной политики социальные сервисы, повторимся, такого вызовы не несут.

СОЦИАЛЬНЫЕ СЕТИ И НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ: ЗА РАМКАМИ *ТВИТТЕР-РЕВОЛЮЦИЙ* И МЕЖДУНАРОДНОЙ ПОВЕСТКИ ДНЯ

Разумеется, значение соцсетей в современном обществе не исчерпывается ретрансляцией и поддержанием социальных волнений и протестной активности, даже если рассматривать их сугубо применительно к сфере международной и национальной безопасности. Использование социальных сетевых сервисов в интересах национальной и международной безопасности возможно, и оно уже развивается сразу по многим направлениям.

1. Первым из них являются различные разновидности *краудсорсинга* (от англ. crowdsourcing) — явления, получившего свое наименование в 2006 г. в статье Джэка Хауи (Jeff Howe) в журнале *Wired*[23]. Краудсорсинг означает передачу каких-либо действий, работ и функций вообще неопределенному внешнему кругу лиц на неоплачиваемой основе. За прошедшие несколько лет с момента своего создания краудсорсинг онлайн получил широкое распространение не только на Западе, но и во многих других регионах и странах, включая Россию.

За последнее время одним из наиболее ярких и успешных проектов подобного рода в России стала «Карта помощи пострадавшим от пожаров», созданная в 2010 г. известным интернет-активистом и теоретиком Григорием Асмоловым (Gregory Asmolov). Это онлайн-сообщество функционирует на базе специальной платформы *Ushahidi*, позволяющей в рамках единого сервиса агрегировать и ретранслировать информацию с мобильных телефонов (через СМС-сообщения), электронной почты, а также обычных веб-сайтов. «Карта» показала себя как весьма эффективная информационная сеть, своеобразный узел, на который оперативно поступала информация о текущих событиях по различным каналам. Сама платформа была создана в 2008 г. с целью сбора и обмена информацией о случаях насилия после президентских выборов в Кении. Проекты на платформе *Ushahidi* помогали специальным службам спасать людей после землетрясений в Чили и на Гаити в 2010 г. Схожей технологией интерактивных карт *OpenStreetMaps* также успешно пользовались на Гаити американские спасатели, о чем упоминала Госсекретарь США Хиллари Клинтон в своей речи о свободе в интернете 21 января 2010 г.[24].

Словом, целесообразность сотрудничества государства с такими сообществами достаточно очевидна, однако в России такое взаимодействие сегодня практически отсутствует. Как отмечал г-н Асмолов на встрече Президента РФ с представителями интернет-сообщества, «мы видим все больше и больше примеров, когда сетевое общество может быть равноценным партнером государства в решении тех или иных социальных проблем»[25]. Но одновременно создатель «Карты помощи» признал, что контакты с Министерством чрезвычайных ситуаций (МЧС) РФ были установлены лишь по инициативе самих представителей комьюнити, а помощи от Министерства на тот момент фактически так и не последовало. Как отмечает соавтор проектов г-на Асмолова А. Сидоренко, МЧС демонстрирует собой образец «полного провала во взаимодействии с сетевыми технологиями».

Несмотря на радикальность такой оценки, наличие проблем взаимодействия нельзя не признать. В частности, власти достаточно неохотно идут на контакт с сообществами, деятельность которых направлена на защиту общественной безопасности в частности на борьбу с преступностью и пресечение незаконной деятельности. Таким краудсорсинг-проектом в РФ является сайт *Гдеказино.ру*, где также используется технология интерактивных карт для обмена данными об объектах азартного бизнеса. Проект оказался востребован правоохранительными органами, лишь когда президент РФ Д. А. Медведев лично отдал распоряжение российскому генпрокурору Юрию Чайке провести проверки по адресам казино, указанных на сайте[26].

По ряду перечисленных направлений государство не только не выступает с уже назревшими инициативами, но и игнорирует те предложения и идеи, которые поступают из общественной и экспертной среды. На встрече Президента России

Д. А. Медведева с представителями российского интернет-сообщества 19 апреля 2011 г. предложения о налаживании взаимодействия властных структур с сетевыми *краудсорс-комьюнити* встретили положительный отзыв президента, однако не получили реального развития[27].

Как следует из слов самого Д. А. Медведева на упомянутой встрече, на сегодня внимание к сетевым сообществам у государственных структур возникает в отдельных случаях, не на системном уровне, не в отлаженном рабочем режиме.

По отдельным направлениям взаимодействие госструктур с проектами формата краудсорсинга уже зарождается на уровне региональных органов власти. Так, по словам А. Сидоренко, правительство Пермского края использует данные краудсорсинга, например, таких ресурсов, как *Streetjournal.ru* и *Roards.teron.ru*. Определенный обратный отклик со стороны государственных органов вызывают проекты блогера А. А. Навального *Rospil.info* и *Rosyama.ru*, которые по некоторым параметрам можно причислить к краудсорсингу. Кроме того, в последнее время определенный интерес к краудсорсингу отмечается со сторону научно-аналитических институтов, близких к правительству. Как отметил Григорий Асмолов, автор ряда краудсорсинг-проектов, «позитивным примером является то, что при поддержке ИНСОР[28] разрабатывается платформа для взаимопомощи в кризисных ситуациях *Виртуальная рында — атлас помощи*».

Однако эти тенденции пока не распространяются на вопросы обеспечения безопасности в силу ряда причин. Во-первых, играют роль объективные ограничения, такие как секретный характер деятельности многих госструктур в сфере безопасности, а также централизованный характер обработки информации и принятия решений в них, весьма далекий от *grass-roots* уровня краудсорсинга. Однако не менее важны изъяны в работе российских госорганов, ответственных за обеспечение безопасности, и в первую очередь силовых структур. Речь в том числе идет об их традиционной закрытости, определенном консерватизме и запаздывающем освоении новых форматов взаимодействия с общественными структурами, а также вытекающем отсюда недоверии к этим структурам и используемым ими технологиям.

Между тем необходимость укрепления связей и наращивания сотрудничества госструктур с интернет-сообществом из числа опрошенных мной экспертов отметили представители ряда российских федеральных ведомств и самого интернет-сообщества. Таким образом, основная рекомендация для органов государственной власти РФ должна сводиться к необходимости преодоления:

а) инертности и пассивности органов, отвечающих за безопасность, в отношении социальных сервисов и наполняющих их сообществ пользователей как потенциальных партнеров в исполнении своих функций;

б) *ручного управления* взаимодействием госструктур с интернет-сообществом, препятствующего налаживанию устойчивого двустороннего сотрудничества и укоренению его системного характера.

2. Другая сфера применения социальных онлайн-сервисов не столь однозначна и даже противоречива в плане влияния на безопасность. Речь идет о социальных сервисах как инструменте формирования информационной картины событий и общественного мнения. Обычно принято говорить как о традиционных СМИ, так и об интернет-медиа (к числу которых принадлежат и соцсети), используя негативный контекст *информационного оружия*. Однако опыт РФ и других стран показывает, что эта медаль также имеет свою вторую сторону, и социальные сетевые сервисы могут быть как *мечом*, так и *щитом* в информационном противоборстве.

Первым классическим примером применения социальных медиа в качестве *оборонительного средства* принято считать действия израильских блогеров во время Второй Ливанской войны. В 2006 г. небольшая, но чрезвычайно активная израильская блогосфера в основном отражала шквал международной критики, который

обрушился на руководство страны не только из арабского мира, но и из многих западных стран и ООН, особенно после печально известного эпизода бомбардировки г. Каны израильскими ВВС в ночь на 30 июля 2006 г., унесшего жизни 28 мирных жителей. Усилиями блогеров удалось опровергнуть намеренно завышенное Хезболлой в 2 раза число жертв бомбардировки; также во многом благодаря израильской блогосфере был установлен постановочный характер фотографий с места бомбардировки, которые ранее были растиражированы такими ведущими СМИ, как *Reuters.* Наконец, израильские блогеры активно защищали свою страну и в других национальных сегментах блогосферы, включая российский, что в определенной степени повлияло на отношение общественности в России к действиям израильской стороны в конфликте.

Для России не менее ярким примером активности онлайн-сообществ в условиях агрессивной информационной кампании стала *Пятидневная война* 2008 г. Во время повального осуждения действий РФ на международном уровне блогосфера стала одной из немногих площадок, на которых активно отстаивалась альтернативная версия событий, не столь негативная для имиджа РФ. По сути, именно блогосфера не позволила российской стороне *всухую* проиграть информационную битву в августе 2008 г. Российским блогерам и сочувствующим активистам из-за рубежа удалось предпринять ряд действий, которые хотя и не переломили общую картину конфликта в Сети и глобальных СМИ, однако внесли в нее ряд корректив.

Так, коллективный флэшмоб российских блогеров привел к убедительной победе пророссийской позиции в голосовании на сайте CNN — на вопрос «Оправданы ли действия России в Грузии?» утвердительно ответили 92%, или 273,9 тыс. человек[29]. Благодаря блогерам скандальную известность получил новостной выпуск *Fox News*, в котором ведущий не дал беженкам из Южной Осетии (Аманде Кокоевой и Лоре Тедеевой-Коревиски) высказать в эфире обективную точку зрения. Наконец, определенный вклад в укрепление доверия к российской точке зрения внесли блоги очевидцев с места событий, включая военных специалистов, журналистов и просто жителей Южной Осетии.

На фоне активности рядовых граждан в блоговых, микроблоговых сервисах и социальных сетях (*Facebook, ВКонтакте*) реакция официального Кремля и российских СМИ выглядела удручающе запоздалой и неубедительной, о чем неоднократно говорилось впоследствии. Единственным мероприятием в сфере информационной борьбы стал пресс-тур для зарубежных журналистов по Цхинвали, состоявшийся 12 августа 2008 г., после окончания боевых действий, когда *мейнстримная* антироссийская точка зрения на конфликт уже закрепилась в массовом сознании жителей зарубежных государств.

Однако Минобороны РФ вынесло из этих событий определенные уроки. В январе 2012 г. в открытом доступе появился документ ведомства под названием «Концептуальные взгляды на деятельность Вооруженных сил Российской Федерации в информационном пространстве»[30]. Представляя собой, по сути, новый доктринальный продукт Минобороны в области информационного противоборства, «Концептуальные взгляды…» уделяют большое внимание вопросам информационного освещения конфликтов и влияния на формирование общественного мнения. Так, в рамках задач по сдерживанию и предотвращению конфликтов предполагается «публично, объективно и своевременно разъяснять мировой общественности причины и истоки конфликта». Отмечается, что такие меры позволяют создать в «глобальном информационном пространстве» климат, удерживающий организаторов конфликта от его дальнейшей эскалации.

Не ограничиваясь этим пунктом, авторы документа также отмечают роль информационной работы непосредственно *в ходе* конфликта. В частности, постоянное информирование СМИ и работа с общественным мнением в ходе конфликтной ситуации призваны «эффективнее влиять на ее деэскалационное развитие». В целом, несмотря на громоздкость формулировок, в документе вполне четко и здраво отмечаются задачи информационного обеспечения деятельности воору-

женных сил. Появление подобных наработок говорит о том, что российские силовые структуры начали активно восполнять тот пробел, который существовал ранее в теоретическом осмыслении ИКТ и глобальных СМИ применительно к спектру их прямых ведомственных задач.

3. Еще одна сфера применения соцсетей, довольно близкая к краудсорсингу, — использование подобных сервисов в качестве систем экстренного оповещения о чрезвычайных ситуациях, катастрофах и различных угрозах. Пионерами в данном направлении являются США: в апреле 2011 г. стало известно о том, что Министерство национальной безопасности планирует использовать популярные социальные сети, в том числе *Twitter* и *Facebook,* для оповещения граждан страны о террористических угрозах. Более того, по данным СМИ, в будущем система может вовсе заменить традиционную для страны цветовую шкалу террористической угрозы.

Другой пример дала полиция австралийского штата Квинсленд в декабре 2010 г. — январе 2011 г. Во время мощнейшего наводнения и вызванной им массовой эвакуации жителей стандартная система оповещения стала давать сбои из-за возросшего потока запросов на сайты госучреждений и частичного отключения мобильной связи. В этой ситуации было принято решение о дублирующем оповещении населения через страницы на *Facebook* и *Twitter* полицией Квинсленда, а также службой информации аэропорта столицы штата г. Брисбена. Идея дала результат — активность пользователей не повлияла на работу серверов социальных сетей и позволила частично разгрузить сайты упомянутых госучреждений. Наконец, получать информацию из социальных сетей в кризисных ситуациях стремятся сами пользователи — в Японии сразу после цунами 11 марта 2011 г. поток *твитов* из Токио возрос многократно, превысив 1200 сообщений в час[31].

Нандан ***Унникришнан****, директор по евразийским исследованиям, старший научный сотрудник Исследовательского фонда Observer, Рахул Пракаш, младший научный сотрудник, Институт исследований безопасности Исследовательского фонда Observer — по электронной почте из Дели:* В августе 2012 г. мы в очередной раз стали свидетелями того, как интернет и социальные сети могут быть использованы для создания паники и дезорганизации повседневной жизни в отдельно взятой стране. Распространение *фейковых* фото- и видеоматериалов и искаженных слухов об антимусульманских погромах в Ассаме и Мьянме и реакции на них спровоцировало массовое бегство представителей определенных этноконфессиональных групп из ряда индийских городов. Учитывая культурное, этническое и конфессиональное многообразие Индии, использование естественного потенциала для социальных волнений представляет серьезный предмет озабоченности для властей. Наиболее яркий эпизод недавних событий, когда до 300 тыс. человек бежали из Бангалора после распространения в социальных сетях сообщений о скором начале погромов, служит примером того, как интернет может использоваться для подрыва социальной гармонии. Правительству необходимо выработать политику и стратегии предотвращения подобных ситуаций. Как бы то ни было, делать это следует, не выходя за рамки ключевых положений индийской конституции — включая нормы о свободе слова и самовыражения. Соответственно, полная блокировка сайтов по образцу китайской модели для Индии неприемлема.

Таким образом, в информационно развитых странах и органы власти, и само общество начинают уделять внимание социальным сетям как источнику и ретранслятору информации в тех ситуациях и направлениях деятельности, которые напрямую связаны с обеспечением безопасности. В будущем эта тенденция, без сомнения, будет набирать силу по мере адаптации госструктур к прогрессу ИКТ.

Что касается России, то на этом поле какой-либо целенаправленной активности российских госструктур пока не наблюдается. Так, принятые Госдумой РФ 22 апреля 2011 г. поправки в закон «О противодействии терроризму» вводят цветовую шкалу террористической угрозы, но не предполагают использования соцсетей для информирования населения, в отличие от американского законопроекта. Возможно, причина лежит в более низкой по сравнению с США степенью проникновения данных сервисов в РФ — около 20% населения по сравнению с 45% в Штатах[32]. Но и теракты в России происходят не в пример чаще, даже если не брать в расчет Северо-Кавказский федеральный округ с крайне низким уровнем проникновения интернета.

Другим свидетельством слабого прогресса российских госорганов в освоении ИКТ для задач экстренного оповещения стали катастрофические наводнения на Кубани в июле 2012 г., когда оповещения не было вовсе. Представляется, что деятельность госорганов в этой области должна получить импульс критики со стороны гражданского общества, а также импульс идей и предложений от частного сектора, чтобы ситуация начала выправляться. Для этого, однако, необходима хотя бы минимальная терпимость властей к критике и готовность к восприятию частных инициатив, о чем затруднительно говорить в случае с Крымском.

РАЗВИТИЕ СОЦИАЛЬНЫХ СЕТЕЙ В РФ — ПРОБЛЕМЫ И ЗАДАЧИ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ С ТОЧКИ ЗРЕНИЯ БЕЗОПАСНОСТИ

В дискуссии о роли соцсетей в контексте безопасности принципиально важен вопрос идентификаций их пользователей. По словам одного из ведущих российских экспертов в области информационного права, решение этой проблемы является «основной на сегодня задачей, стоящей перед Россией и другими странами в сфере управления интернетом». При этом идентификация в соцсетях неразрывно связана с общей проблемой идентификации пользователей в интернете. Ее актуальность частично вытекает из уже упомянутых выше примеров, таких как случай *сирийской блогерши*, хотя он и не описывает все потенциальные риски, связанные с так называемой активной анонимностью в Сети. Ситуация, когда пользователь может с легкостью обойти существующие средства идентификации, открывает возможности для кибермошенничества, размещения общественно опасного и неприемлемого контента, проявлений экстремизма и социальной агрессии онлайн.

Уже сейчас эта тема включается в рабочую повестку российских структур, в ведении которых находятся вопросы национальной безопасности. Согласно нашему источнику в СБ РФ, «в последнее время в повестке Совета стало уделяться внимание проблеме терроризма в социальных сетях». Корни проблемы во многом уходят в максимально свободный (до июня 2011 г.) режим регистрации пользователей *ВКонтакте*. До сих пор эта социальная сеть выдает сотни и тысячи результатов в поиске страниц, групп, заметок и видео с призывами к «джихаду против неверных», построению «имарата кавказ», бунту мусульманского населения РФ против федералов и т.д.

В свою очередь, такое обилие неприемлемого контента объясняется тем, установить личность пользователя, выложившего его в сеть, практически невозможно. Отсюда и следует огромное количество профилей «муджахидов», «воинов ислама», немыслимых для *Facebook*, *LinkedIn, Google+*. Даже наполняя подобный профиль определенной личной информацией, пользователи знают, что останутся безнаказанными, если только лично ими не заинтересуется ФСБ (что крайне

маловероятно по понятной причине — за всеми не уследишь). Кроме того, 15 марта 2011 г. *ВКонтакте* удалось выиграть в суде во многом прецедентное дело, связанное с размещением в сети контента, нарушающего права правообладателя[33]. Однако согласие суда с доводами представителей социальной сети, что ответственность за размещаемые материалы лежит на пользователях, лишь дает зеленый свет дальнейшим нарушениям подобного рода со стороны *де-факто анонимных* пользователей.

Решения проблемы варьируются в зависимости от различных технологических путей их реализации. Наивысшая надежность идентификации в теории может быть достигнута при использовании программ и технологий, которые предполагают шифрование (кодирование) и снабжение цифровой подписью той информации, которой обмениваются пользователи. Классическим примером таких программ служит система PGP (*англ.* Pretty Good Privacy), разработку которой начал в 1991 г. небезызвестный американский программист Филипп Циммерман (Philip Zimmermann). Уже в первой версии программы, основанной на принципе *Сети доверия* [Network of Trust], предполагался механизм открытых и закрытых ключей, а также цифровых сертификатов, взаимное подтверждение которых и обмен ключами формировали *Сеть доверия* между пользователями, куда не мог вклиниться посторонний или злоумышленник.

Однако сегодня такие программы заведомо неприемлемы для коммерчески ориентированных крупных сетевых сервисов, соревнующихся друг с другом в простоте и дружественности пользовательского интерфейса, а также в легкости расширения круга контактов каждого из пользователей. Более того, по мнению эксперта МГИМО (У) МИД РФ В. В. Каберника, проблематичными для социальных сетей могут стать и менее радикальные варианты, такие как перевод работы с данными сервисами в HTTPS, защищенное расширение протокола HTTP, поддерживающее шифрование вводимых данных. Так как ключевое значение в современных социальных сетях, как упоминалось выше, имеют ссылки на посторонний аудио- и видеоконтент, размещаемый в незащищенном HTTP, работа пользователей с ними будет существенно затруднена. Компромиссным вариантом, с точки зрения эксперта, мог бы стать перенос в HTTPS процедуры регистрации и авторизации пользователя в социальных сетях.

Сами социальные сети, по крайней мере в РФ, пытаются решать проблему идентификации пользователей исходя из собственной логики, далеко не всегда успешной. С 11 июля 2011 г. *ВКонтакте* ввела регистрацию пользователей по номерам мобильных телефонов, избрав компромиссный вариант между закрытой системой регистрации и открытой, имевшей место ранее. Привязка аккаунта к номеру сотового является вариантом идентификации, который довольно эффективен в том случае, когда все пользователи являются гражданами РФ, где мобильный номер (промежуточная ступень идентичности в данном случае) приобретается по паспорту. Но считать этот путь полностью успешным мешает трансграничность *ВКонтакте*, присущая любой крупной социальной сети. Как уже упоминалось, около 40 млн аккаунтов в сети Павла Дурова зарегистрированы за пределами РФ, а значит, их хозяева приобретают мобильные номера в соответствии с зарубежным законодательством. По данным на начало апреля 2011 г., *ВКонтакте* насчитывалось 16,5 млн аккаунтов пользователей из Украины[34], где мобильные номера не привязаны к документам, удостоверяющим личность владельца. В странах Европы, таких как Испания, мобильные номера вообще не закреплены за каким-либо конкретным провайдером сотовой связи. В результате, идентификация 30% пользователей соцсети оказывается фиктивной. Таким образом, подход, избранный *ВКонтакте*, должен дополняться решениями, которые покрывали бы упомянутые *серые зоны*.

В их числе можно упомянуть привязку аккаунта в соцсети к банковскому счету пользователя, вариантом которой можно считать распространение на социальные сети правил электронных платежных систем, таких как *PayPal, Webmoney, Яндекс.Деньги* и другие. Преимуществом такого решения стала бы высокая

надежность идентификации и ценность аккаунта в глазах пользователя (особенно если в Пользовательское соглашение с соцсетью будет включен пункт о заморозке определенной суммы на счете в случае нарушения его положений). В настоящее время можно выделить две уязвимых места в данной идее:

а) охват пользовательской аудитории в данном случае опять же будет неполным. По информации на март 2011 г., банковские счета имели лишь 47% россиян[35], хотя среди молодежи, которая составляет костяк аудитории социальных сетей, этот процент существенно выше. Кроме того, неясно, каким образом удастся выстроить сотрудничество социальных сетей с зарубежными банками, не ведущими деятельность в РФ;

б) увязка аккаунта с банковским счетом может встретить сопротивление как самих социальных сетей и всех стейкхолдеров данной отрасли, так и банков, которые попросту столкнутся с необходимостью обработки потока не нужной им информации.

Ожидать подвижек по второму пункту можно лишь при условии успешной и массовой коммерциализации услуг социальных сетей, ориентированной именно на их оплату с банковских счетов. Первые шаги в этом направлении в начале июля 2011 г. сделали две крупнейшие социальные сети РФ (*ВКонтакте* и *Одноклассники*), которые ввели возможность привязки оплаты платных услуг с карт банков-партнеров (вместо платных СМС)[36]. Ключевых вопроса здесь два: можно ли превратить такую *опцию* в *обязательство* и достаточны ли меры безопасности, применяемые для защиты вводимых пользователем банковских реквизитов. В плане безопасности предпочтителен путь *Одноклассников*, когда при регистрации пользователь работает в защищенной базе самого банка, уже после этого переходя в обычный интерфейс социальной сети. По сути, такая схема почти полностью укладывается в логику приводимых выше рекомендаций В. В. Каберника.

Но так или иначе перечисленные меры не решают проблемы идентификации пользователей полностью — для этого необходим комплексный подход, распространяющийся на все интернет-пространство. В РФ он пока отсутствует, так как не существует, во-первых, консенсуса относительно должной степени вмешательства государства в данную область; во-вторых, отсутствует единое видение этого подхода на техническом и юридическом уровнях. В данных условиях целесообразно тщательное и многоуровневое изучение зарубежного опыта, как положительного, так и негативного. Как отмечает известный российский эксперт в области информационного права, «сегодня отечественным органам власти необходим мониторинг наработок и решений других стран и международных организаций в данной области».

Между тем за рубежом наиболее интересные решения предлагают США, где в последние годы обсуждается идея введения *интернет-паспортов*, действие которых охватит не только социальные сервисы, но и всех пользователей Всемирной сети. В конце 2010 г. была впервые опубликована черновая версия Национальной стратегии достоверной идентификации в киберпространстве, [National Strategy for Trusted Identities in Cyberspace][37].

В основе документа лежит идея единой комплексной многоуровневой безопасной интернет-среды, действующей в условиях достоверной идентификации пользователей, а также надежной защиты их персональных данных. Стратегия ориентирована на физических лиц, а также прочих субъектов (нефизических лиц) — организации, услуги, продукцию программного обеспечения (ПО). Кроме того, стратегия учитывает глобальный характер Сети, подразумевая необходимость действия предлагаемых средств идентификации на трансграничном уровне. Ключевой принцип обеспечения безопасности интернет-среды — позволить всем субъектам коммуникации сообщать свои данные лишь в минимально необходимом объеме в каждом необходимом случае, при многоуровневом и предельно гибком ран-

Евгений ***Сатановский (Россия)****, президент Института Ближнего Востока — по электронной почте из Москвы:* Информационные технологии и кибертехнологии — это всего лишь инструмент революции, равно как и контрреволюции. Электронные СМИ и средства коммуникации позволяют куда эффективнее коллективно организовывать массы, чем газета или кинематограф во времена Ленина. Но и автомат Калашникова лучшее оружие, чем берданка или маузер. Актуальность информационной безопасности и кибербезопасности для традиционного и патриархального в своей основе региона Ближнего Востока — это проблема местных властей, руководства оккупационных сил или лидеров террористических группировок. Все они занимаются этим: одни, чтобы сохранить власть, другие, чтобы ее захватить, третьи, чтобы помешать вторым и поддержать первых. Техническое обеспечение любой войны и революции в ту или иную конкретную эпоху есть прежде всего вопрос о власти. И вопрос архиважный, как говаривал тот же В. И. Ленин с присущим ему грассированием.

жировании требований по тем ли иным транзакциям и разным типам субъектов, в остальных случаях сохраняя анонимность, не сообщая лишнюю информацию.

Для РФ подобные наработки могут представлять весьма большой интерес по следующим причинам:

а) технические средства идентификации в рамках *Экосистемы идентичности* [Identity Ecosystem] максимально диверсифицированы. Это устройства USB, специальное ПО, электронные смарт-карты, компьютерные чипы безопасности, программные сертификаты и даже средства мобильной связи. Весь арсенал технических средств объединяется едиными решениями, а соответствующие программные модули и сертификаты интегрируются едва ли не в любое устройство, позволяющее подключаться к интернету. В этом смысле *Экосистема* следует нынешнему тренду на максимальную диверсификацию средств доступа в интернет и расширение диапазона соответствующих устройств, включая мобильные телефоны;

б) в документе, вопреки опасениям алармистов, четко говорится об отсутствии монопольного контроля над системой со стороны государства и прямо прописан принцип мультистейкхолдеризма. Правительство США планирует строить *Экосистему* на равных началах с бизнесом, НПО и другими субъектами. При этом госорганы должны «показывать пример и быть лидерами в области идентификационных решений»[38]. Такой баланс весьма важен и для России, где традиционное доминирование государства в подобного рода проектах должно находить разумный противовес в лице частного сектора и за счет рассредоточения контроля над системой по мере ее развития;

в) работа в *Экосистеме идентичности* является добровольной для пользователей, которым предоставляется выбор между провайдерами идентификации, способами проведениями транзакций и услугами *Экосистемы*. В данном случае опять же важна диверсификация предлагаемых услуг и решений, которая позволит привлечь пользователей в качестве добровольных клиентов, а не навязывать систему идентификации административными и законодательными методами.

Таким образом, задачей российских органов власти должно стать тщательное изучение данной инициативы, применение ее удачных решений и принципов для разработки аналогичной отечественной концепции целостной системы идентификации пользователей. При этом органичной составляющей подобной системы по умолчанию могла бы стать идентификация пользователей в социальных сетях.

ЗАКЛЮЧЕНИЕ

Суммируя проделанный анализ, целесообразно будет привести ряд выводов и практических рекомендаций.

1. Социальные сетевые сервисы, как и прочие ИКТ, сами по себе не являются источником и причиной социальных волнений, как показали революционные события на Ближнем Востоке. Роль социальных сетей в общественно-политических трансформациях в событиях в арабских странах не была ни монопольной, ни преобладающей среди других средств коммуникации.

Более того, социальные сети не оформились и в качестве негосударственных акторов, подобных ТНК, которые четко осознавали бы свои интересы и возможные стратегии в событиях, подобных *Арабской весне*. Наконец, по тем же причинам лишены оснований утверждения о причастности США к организации и режиссуре *арабских революций*.

В общем и целом социальные сетевые сервисы едва ли представляют угрозу безопасности как на уровне отдельных государств, так и на международном уровне. Соответственно, дискуссия относительно того, как следует реагировать на вызовы безопасности, исходящие от социальных сетей, представляет собой не совсем корректную постановку вопроса. Этот посыл может быть актуален для политического руководства РФ при дальнейшем рассмотрении ими проблематики социальных сетей в плоскости национальной и международной безопасности.

2. Социальные сетевые сервисы могут оказывать деструктивное влияние на международную безопасность в качестве инструментов для проведения того или иного политического курса. Практическим примером такого рода является подход США, в рамках которого указанные сервисы адаптируются с целью подрыва режимов в авторитарных странах, а также для задач шпионажа и военной разведки. Инициативы Соединенных Штатов, направленные на использование социальных сетевых сервисов в таких целях, должны встретить адекватное противодействие международного сообщества, включая РФ. Частью этого процесса должно стать усиление внимания к данной проблематике со стороны ключевых российских ведомств, и в первую очередь МИД, на организационном и структурном уровнях. Верным, но недостаточным шагом в этом направлении является учреждение поста Специального координатора по вопросам политического использования ИКТ в МИД РФ. Процессу расширения соответствующих структурных подразделений МИД должна сопутствовать активизация механизмов межведомственных комиссий. Донесение до международного сообщества российской позиции по использованию социальных сетей в деструктивных целях также является задачей экспертного сообщества, которое должно активизироваться в данном направлении.

3. Одной из приоритетных задач для России в рамках повестки вызовов безопасности в связи с развитием ИКТ должно стать развитие новых проектов в сфере идентификации пользователей, а также анализ зарубежного опыта в этой области.

Необходимо тщательно изучить опыт разработки и ход внедрения проектов комплексного обеспечения безопасности интернета и идентификации пользователей, таких как *Экосистема идентичности*. Данный проект является перспективным примером комплексного подхода к проблеме идентификации. Частично он мог бы стать ориентиром при выработке отечественного системного подхода к идентификации пользователей. Учитывая ограниченность нормативной и концептуальной базы, которой на сегодняшний день располагает в данной сфере Россия,

нам незачем прокладывать свой путь *с нуля*, тратя на это дефицитные ресурсы. Однако, для того чтобы успешно изучить и адаптировать опыт США, российским органам власти необходимо преодолеть нынешний ограниченный подход и скептицизм к американским инициативам в данной сфере. Вместе с тем, разумеется, речь не может идти о механическом копировании американских инициатив — возможным объектом для адаптации здесь выступает сам принцип системных и многоуровневых решений в области идентификации, а отнюдь не конкретные положения концепции *Экосистемы.*

Наработка решений для отечественных проектов подобного рода требует реализации принципов мултистейкхолдеризма с активным и приоритетным участием общественных объединений, бизнеса и горизонтально-вертикальных сетей государственных органов различного уровня. В свою очередь, для осознания актуальности данных принципов российским властям нужен четкий импульс со стороны экспертного сообщества. В число *генераторов* такого импульса мог бы в перспективе войти и ПИР-Центр.

4. Социальные сетевые сервисы могут служить интересам национальной и международной безопасности в областях, не связанных с решением задач международно-политического и военного характера.

На сегодняшний день перспективы имеют как минимум три таких направления:

а) противодействие недружественным информационно-пропагандистским кампаниям;

б) оповещение и информирование населения о чрезвычайных ситуациях и иных угрозах безопасности, сбор и обработка информации о таких угрозах;

в) отслеживание и пресечение противоправной деятельности, включая экстремизм и терроризм.

Выход на устойчивое взаимодействие со структурами интернет-сообщества, которые могут быть полезны в развитии данных направлений, должен стать приоритетной задачей МЧС, МВД, ФСБ, Минобороны РФ и других органов, ответственных за обеспечение безопасности. На данный момент взаимодействие государства с интернет-сообществом развивается, но недостаточными темпами. В числе факторов, препятствующих его развитию, консерватизм и закрытость госструктур в сфере безопасности, отсутствие у них достаточных навыков и мотивации для взаимодействия с интернет-сообществом и гражданским обществом в целом, а также недопонимание технологий социальных сервисов, недооценка их потенциала.

Вместе с тем, по отдельным направлениям, таким как осмысление роли и потенциала ИКТ и глобальных СМИ в контексте деятельности силовых структур, за последнее время достигнут определенный прогресс. Позитивная динамика такого рода должна быть поддержана частным сектором, экспертами и интернет-сообществом и в других областях, связанных с использованием ИКТ и конкретно социальных сетевых сервисов для укрепления национальной безопасности РФ. Определенный вклад в этом направлении, как представляется, может внести и ПИР-Центр.

Примечания

[1] Материал доработан на основе статьи: Демидов О. Социальные сетевые сервисы в контексте международной и национальной безопасности. *Индекс Безопасности*. 2011, Зима. № 4 (99). С. 59–76.

[2] Boyd, D., Ellison, N. Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*. 2007. No 13 (1). http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (последнее посещение — 27 августа 2012 г.).

[3] Policy and Legal Challenges of VirtualWorlds and Social Network Sites — Holger M. Kienle, Andreas Lober, Hausi A. Muller, IEEE Computer Society Washington, DC, USA ©2008.

[4] См. подробнее: The Role of Information Communication Technologies in the «Arab Spring» — Implications beyond the Region. PONARS — Ekaterina Stepanova. Eurasia Policy Memo No. 159. May 2011.

[5] Морозов Е. Цена вопроса. *Газета «Коммерсантъ».* 2011, 9 марта, http://www.kommersant.ru/doc/1595762/print (последнее посещение — 27 августа 2012 г.).

[6] Rachman G. Reflections on the Revolution in Egypt. Financial Times. 2011, February 14, http://www.ft.com/cms/s/0/bc459dfc-3880-11e0-959c-00144feabdc0.html (последнее посещение — 27 августа 2012 г.).

[7] Дмитрий Медведев провел во Владикавказе заседание Национального антитеррористического комитета. Президент России. 2011, 22 февраля, http://kremlin.ru/news/10408 (последнее посещение — 27 августа 2012 г.).

[8] Арабские беспорядки и революции беспокоят Москву. Le Monde, Франция. *ИноСМИ.ру*. 2011, 24 февраля, http://www.inosmi.ru/politic/20110224/166817328.html (последнее посещение — 27 августа 2012 г.).

[9] Корпорация по присвоению имен и номеров в интернете (*англ.* Internet Corporation for Assigned Names and Numbers). Подробнее см. статью в этом номере *Индекса Безопасности*: Якушев М. Интернет–2012 и международная политика. Политические и геополитические аспекты глобального управления интернетом. *Индекс Безопасности*. 2013. Весна. № 1 (104). С. 29–42.

[10] Department of Defense Strategy for Operating in Cyberspace. July 2011. US Department of Defense Official Website. http://www.defense.gov/news/d20110714cyber.pdf (последнее посещение — 27 августа 2012 г.).

[11] Стратегический наступательный твиттер. *Газета.ру.* Александр Артемьев. 2011, 16 февраля, http://www.gazeta.ru/politics/2011/02/16_a_3527294.shtml (последнее посещение — 27 августа 2012 г.).

[12] Следует сразу оговориться в отношении *Wikileaks*. Некоторые эксперты, включая, например, Е.А. Степанову (см. например, исследование The Role of Information Communication Technologies in the «Arab Spring» — Implications Beyond the Region, Ponars — Ekaterina Stepanova. Eurasia Policy Memo No. 159. May 2011) отмечают противоречия в риторике Белого дома о свободе в интернете в свете резко негативной реакции Вашингтона на проект Джулиана Ассанжа. Однако масштабная утечка конфиденциальной переписки дипломатов не смогла ни нанести США действительно серьезный ущерб, ни заставить Белый дом провести ревизию базовых посылов своего курса, оставшись периферийным, хотя и ярким эпизодом в повестке американской политики в отношении киберпространства за последний год. Таким образом, ситуация с *Wikileaks*, хоть и обнаружила наличие двойных стандартов в политике Вашингтона, не привела к отказу Белого дома от борьбы за свободу в интернете во всемирном масштабе.

[13] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. Human Rights Council. Seventeenth session. Agenda item 3. General Assembly. 2011. 16 May. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A. HRC.17.27_en.pdf (последнее посещение — 27 августа 2012 г.).

[14] Стратегический наступательный твиттер. *Газета.ру*. 2011, 16 февраля, http://www.gazeta.ru/politics/2011/02/16_a_3527294.shtml (последнее посещение — 27 августа 2012 г.).

[15] Glanz James, Markoff John. U.S. Underwrites Internet Detour Around Censors. *The New York Times.* June 12, 2011. http://www.nytimes.com/2011/06/12/world/12internet.htm?_r=2&scp=2&sq=shadow%20internet&st=cse (последнее посещение — 27 августа 2012 г.).

[16] В северо-западной части КНДР, на границе с Китаем, распространенной практикой среди жителей, желающих передать во внешний мир ту или иную информацию, является передача сообщений и звонков по мобильным телефонам, которые ловят сигнал с китайских вышек, расположенных в холмах через границу.

[17] Белянинов К. Демократию скачают из интернета. *Газета Коммерсантъ.* 2011. 14 июня. № 105/В (4646). http://www.kommersant.ru/doc/1659553?isSearch=True (последнее посещение — 27 августа 2012 г.).

[18] Там же.

[19] Черненко Е. Военные США плетут паутину. *Коммерсантъ*. 2011. 20 июля. № 131 (4672). http://www.kommersant.ru/doc/1682038 (последнее посещение — 27 августа 2012 г.).

[20] Там же.

[21] Алексей Сидоренко. Интервью с автором. 2011.

[22] Там же.

[23] Howe J. The Rise of Crowdsourcing. *Wired.* 2006, June 14, http://www.wired.com/wired/archive/14.06/crowds.html (последнее посещение — 27 августа 2012 г.).

[24] Выступление Государственного секретаря США Хиллари Клинтон по вопросу свободы интернета. Официальный сайт Посольства США в Москве. 2010, 21 января, http://russian.moscow.usembassy.gov/tr_hrc012110.html (последнее посещение — 27 августа 2012 г.).

[25] Встреча с представителями интернет-сообщества. Президент России. 2011, 29 апреля, http://kremlin.ru/news/11115 (последнее посещение — 27 августа 2012 г.).

[26] Генпрокуратура изучит сайты о подпольных казино. *РБК*. 2011, 15 марта, http://top.rbc.ru/society/15/03/2011/559564.shtml (последнее посещение — 27 августа 2012 г.).

[27] Встреча с представителями интернет-сообщества. Президент России. 2011, 29 апреля, http://kremlin.ru/news/11115 (последнее посещение — 27 августа 2012 г.).

[28] Институт современного развития (ИНСОР) создан с целью объединения лучших экспертов для подготовки предложений и выработки документов по важнейшим направлениям государственной политики.

[29] Вражина А. Первая блогерская. Осетинская война в блогосфере. *Lenta.ru.* 2008, 13 августа. http://www.lenta.ru/articles/2008/08/13/blogs/(последнее посещение — 27 августа 2012 г.).

[30] Концептуальные взгляды на деятельность Вооруженных сил Российской Федерации в информационном пространстве. Информационная безопасность по-русски. *Персональные данные, информационная безопасность и ИТ-инновации*. 2012, 10 февраля, http://www.tsarev.biz/innovation/konceptualnye-vzglyady-na-deyatelnost-vooruzhennyx-sil-rossijskoj-federacii-v-informacionnom-prostranstve/(последнее посещение — 27 августа 2012 г.).

[31] Продвижение в Twitter — вперед, за синей птицей. *Блог ORZ.* 2011, 26 июня, http://blog.orz.com.ua/?p=1251 (последнее посещение — 27 августа 2012 г.).

[32] US Social Network Usage: 2011 Demographic and Behavioral Trends. By Debra Aho Williamson March 2011. 17 Pages, 28 Charts. E-Marketer. emarketer.com/Reports/All/Emarketer_2000777.aspx (последнее посещение — 27 августа 2012 г.).

[33] *ВКонтакте* привлекли к суду из-за песен МакSим. *Lenta.ru*. 2011, 25 апреля, http://lenta.ru/news/2011/04/25/maksim/(последнее посещение — 27 августа 2012 г.).

[34] Чумаченко А. Правильный выбор площадки для продвижения бренда в социальных сетях. *Блог Netpeak*. 2011. 28 апреля. http://netpeak.ua/blog/choose-your-network (последнее посещение — 27 августа 2012 г.).

[35] Банковских карт не оказалось у половины россиян. *Lenta.ru*. 2011. 1 марта. http://www.lenta.ru/news/2011/03/01/cards/(последнее посещение — 27 августа 2012 г.).

[36] *Одноклассники* разрешили «привязывать» к аккаунтам банковские карты. *MoneyNews*. 2011, 6 июля, http://moneynews.ru/News/15271/(последнее посещение — 27 августа 2012 г.).

[37] National Strategy for Trusted Identities in Cyberspace. Creating Options for Enhanced Online Security and Privacy. The White House Official Website. 2010, June 25, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (последнее посещение — 27 августа 2012 г.).

[38] Там же.