Хакеры, цифровые активисты и блогеры: к вопросу привлечения к противодействию экстремистской и террористической деятельности в интернете

Статья рекомендована И.Ю. Алексеевой 14.03.2019.

ВЛАДИМИРОВА Татьяна Валерьевна
Доктор философских наук, доцент, профессор кафедры социологии Новосибирского государственного университета экономики и управления

Аннотация
Развитие технологий, используемых экстремистскими и террористическими группами, идет на опережение по сравнению с возможностями государственных спецслужб, занятых в противодействии информационным угрозам. В информационном противостоянии растет значение новых социальных групп. В противодействии информационным угрозам определенную роль должны играть представители социальных групп хакеров, блогеров и цифровых активистов. Автор предлагает более пристально отнестись к изучению особенностей деятельности хакеров, цифровых активистов и блогеров с тем, чтобы обратиться к разработке способов взаимодействия с ними с целью противодействия информационным угрозам национальной безопасности.

Ключевые слова:
интернет, противодействие информационным угрозам, хакеры, цифровые активисты, блогеры, изучение особенностей новых социальных групп, национальная безопасность.

Интернет является усложняющейся реальностью, продуцирующей все новые угрозы экстремистской и террористической направленности. Это динамичная среда, контролировать которую уже нелегко на данном этапе. Принимаемые государствами меры в определенной мере снижают террористическую и экстремистскую активность в Сети, однако появляются все новые методы и пути обхода этого контроля.

Развитие технологий, используемых экстремистскими и террористическими группами, идет на опережение по сравнению с возможностями служб, занятых в противодействии. Это необходимо признать с тем, чтобы искать новые способы противодействия угрозам экстремизма и терроризма. Речь идет о противодействии призывам к насилию в обществе, распространению идеологии насилия, оправданию национальной, этнической и религиозной нетерпимости и вражды, склонению к сотрудничеству с террористическими и экстремистскими организациями. Важно становиться более информированным о различных способах использования интернета и более приспособленным для контроля и для противодействия действиям преступников и их пособников. Считаем, что в помощь решению подобных задач является изучение особенностей новых социальных групп интернета и взаимодействие с ними.

Ключевыми силами государства в информационном противодействии экстремизму и терроризму в сети Интернет являются МВД России и ФСБ России, а также Минкомсвязь России и подведомственный министерству Роскомнадзор. Но сложно не согласиться с тем, что также «важную роль в системе ИПТ (информационного противодействия терроризму — прим. автора) в сети Интернет должны играть негосударственные субъекты — общественные объединения, СМИ, владельцы

и администраторы интернет-сайтов, блогеры и иные пользователи интернета» [1, с. 85–103]. Мы разделяем мнение И. Ю. Сундиева, А. А. Смирнова, которые отмечают, что роль государства состоит не в дирижировании деятельностью негосударственных акторов (это невозможно в силу их численности), а в активном сотрудничестве с ними в рассматриваемой сфере деятельности, применении методов стимулирования общественно полезной гражданской активности [1, с. 100].

Помимо этого, «в связи с заведомой ограниченностью эффективности мер фильтрации информации в интернете наиболее важное значение в системе мер ИПТ имеют методы пропаганды и контрпропаганды в киберпространстве. Они включают в себя распространение официальных информационных сообщений в сети Интернет, проведение брифингов или пресс-конференций для интернет-СМИ, создание специализированных интернет-сайтов антитеррористической направленности, подготовку и распространение контента контрпропагандистского характера, участие в дискуссиях на форумах и в социальных сетях» [1, с. 103].

В обществе сформировалась такая социальная группа как хакеры. Хакеры по своим возможностям в Сети вероятно сопоставимы с нетократией [2]. Нетократия или цифровая элита: в различных источниках эта социальная группа называется по-разному. Это те, кто владеют современными цифровыми мессенджерами, социальными сетями, задают основные тренды сетевых информационных потоков. И хакеры, и представители нетократии находятся «за гранью понимания» с точки зрения традиционной системы обеспечения национальной безопасности. И те, и другие являются представителями «антисистемы», они вне государства или над государством, поскольку сама Сеть, по сути, явление глобальное, не приемлющее традиционных границ.

Если Марк Цукерберг, Майкл Делл, Сергей Брин, Павел Дуров и другие (сегодня их называют цифровой элитой), владеющие сетями киберпространства, являются личностями в большей мере известными, они имеют и политические и экономические конфигурации, которые осваиваются и спецслужбами государств, и транснациональным капиталом, то хакеров условно можно отнести к прекариату [3] — тем, «кому нечего терять ...». В условиях роста атомизации общества такие люди более других расположены к маргинальному состоянию. Среди них много фрилансеров, временных работников, представителей креативной индустрии.

Спецслужбы мира развивают практику найма известных хакеров. Пожалуй, здесь можно провести аналогию с тем, как в свое время государства в борьбе за морское могущество негласно нанимали вольных торговых людей — пиратов. Пираты XVII–XVIII вв. часто контролировали основные морские пути — единственные эффективные коммуникации тех времен.

Можно сказать, что сегодня на смену морским пиратам пришли пираты цифровые. Одним из способов захвата лидирующих позиций в борьбе с террористической угрозой в интернете становится развитие искусного взаимодействия с хакерами, привлечение их на свою сторону, что является довольно сложной задачей. Для того чтобы подойти к ее решению, необходимо обратиться к исследованию особенностей этой социальной группы, понять основные мотивы ее деятельности, изучить образ жизни таких людей.

Часто хакеров различают на виды, из которых двумя основными являются White hat («белая шляпа») и Black hat («чёрная шляпа»). Черными шляпами называют киберпреступников, тогда как белыми шляпами — прочих специалистов

по информационной безопасности (в частности специалистов, работающих в крупных IT-компаниях) или исследователей IT-систем, не нарушающих закон. Есть еще Grey hat («серая шляпа»). О серых шляпах говорят, когда сталкиваются со случаями мелких нарушений закона или отсутствием нарушений законодательства, но нарушением внутренних правил какого-либо интернет-сервиса [4].

Как социальную группу хакеров сложно локализовать и выделить. Но уже появляются исследования в ключе специфики их субкультуры, значения их деятельности для развития технологий в контексте позитивного или деструктивного влияния на процессы в обществе (М. Кастельс, Е. С. Ларина, П. Химанен, О. Б. Скородумова, М. С. Букин, М. С. Вершинин, Е. В. Осипов, В. П. Терин и др.). Конечно же, необходимо уделять отдельное внимание таким исследованиям.

Некоторые авторы называют хакеров Робин Гудами Информационной Эпохи [5]. Известный исследователь информационного общества М. Кастельс считает хакерами Дж. Ассанджа, участников WikiLeaks и целую плеяду последователей этой организации. Он отмечает, что они работают на идею и их целью является представлять гражданам доступ к важнейшей информации о поведении и стратегиях облеченных властью людей и организаций, которые принимают важнейшие в мире решения [6, с. 24]. В своей работе «Власть коммуникации» (2013) теоретик отмечает, что «в условиях беспощадных атак на WikiLeaks и заточения Ассанжа в стенах посольства Эквадора в Лондоне созданная WikiLeaks информационная модель была воспринята рядом новых организаций эпохи свободной цифровой коммуникации, таких как Friends of WikiLeaks — социальная сеть, кто поддерживает WikiLeaks, запущенная в декабре 2011 г., Brussels Leaks — сеть активистов и журналистов, провозгласивших своей задачей “вывести теневые взаимодействия внутри Европейского Союза в публичную сферу”, Trade Leaks, созданный Русланом Коганом в Австралии с целью ”делать в сфере бизнеса то, что WikiLeaks делает в политике”. Существует также RuLeaks, который стремится воспроизвести модель WikiLeaks в России. ... На практике буквально каждый месяц возникают альтернативные новостные организации» [6, с. 27].

Насколько можно разделять такую точку зрения о хакерах как о Робин Гудах — остается неоднозначным вопросом. Мы бы рассматривали подобные организации и хакеров, поддерживающих их деятельность, как отдельную группу, поскольку особенности их деятельности являются несколько иными по сравнению с общепринятыми представлениями о хакерах. Главное отличие идейных хакеров или цифровых активистов — в их поддержке или участии в различных сетевых организациях, которые объединяют участников под социально актуальными целями.

Известный эксперт в области конкурентной разведки Е. С. Ларина вслед за зарубежными исследователями выделяет группу цифровых активистов [7]. В нее входят наиболее политически активные пользователи. Цифровые активисты могут включать в себя и политических хакеров, и политически активных блогеров. Еще в 1998 году ряд известных исследователей, связанных с американским разведывательным сообществом, сделали прогноз о скорейшем превращении интернет-активистов в мощную трансграничную и локальную политическую силу. К концу нулевых годов численность интернет-активистов по миру стала измеряться уже сотнями тысяч человек. Эти сотни тысяч людей являются уже не разрозненными, атомизированными индивидуумами и враждующими между собой группами. Они

становятся все более организованными — связанными между собой сетевыми коммуникациями, образующими разные по длительности и интенсивности сети.

Цифровые активисты — убежденные сторонники групповых и коллективных действий. Они строят свою деятельность, опираясь на малые группы, небольшие общины и массовые движения, состоящие из локальных подразделений.

С другой стороны, именно цифровые активисты, актуализирующие проблемы и вопросы жизни общества, в состоянии успешно осуществлять пропаганду и контрпропаганду в киберпространстве, отстаивая национальные интересы своей страны. Считаем, что возможности социальных сетей, других интернет-платформ организаций цифровых активистов составили бы существенный вклад в развитие практик противодействия призывам к политическому насилию, оправданию насилия по национальному, религиозному признаку.

Е. С. Ларина отмечает, что «в Соединенных Штатах, Канаде, Скандинавии, странах Балтии, Бенилюксе действуют онлайн и оффлайн курсы и школы для цифровых активистов, регулярно проводятся открытые конференции и закрытые встречи по теме цифрового активизма. В России же по состоянию на лето 2016 г. не проведено ни одной конференции, не издано ни одной книги, не существует ни одного научно-практического центра, специализирующегося на цифровой активности» [7, с. 77].

Еще одной группой «цифровых пиратов» свободного, усложняющегося интернет-пространства, которые многое могли бы сделать для профилактики и противодействия экстремизму и терроризму в киберпространстве, можно назвать блогеров. Они также имеют безграничные возможности влияния на сетевые коммуникации, но не в техническом, а социально-смысловом аспекте. В отличие от хакеров они находятся в легальном, публичном пространстве. В отличие от цифровых активистов охват ими тем и аудиторий более широк и многообразен. Их деятельность сравнима с деятельностью средств массовой информации. Они формируют, аккумулируют общественное мнение в социальных сетях.

Блогеры не так хорошо владеют архитектоникой интернет-пространства, но искусно занимают внимание и предпочтения тысяч и миллионов пользователей. Ресурсы блогера определяются объемом, конфигурацией и плотностью сети его подписчиков. Под их влиянием находятся большие социальные сети. В интернете публикуются рейтинги популярности блогеров. К примеру, в 2017 году первые три позиции занимают блогеры с интернет-проектами, на которые подписано более 7,5 млн человек, 5 млн и 4 млн. — соответственно [8].

Особенности блогосферы, в частности, блоговые посты (отдельные сообщения, опубликованные для публичного чтения) изучаются различными социальными науками: политологией — К. О. Квятковский, К. А. Крайнова, Д. С. Мартьянов, Е. С. Крестинина, Ю. Г. Чернышов и др., журналистикой — Е. Л. Вартанова, В. В. Коломина, Е. В. Лазуткина, А. А. Никитенко и др., культурологией — Г. М. Агеева, Н. В. Кузнецова, Е. А. Осипова и др. [9]. Исследователи фиксируют особенности строения блогосферы, ее актуальные тенденции, отражающие текущее состояние современного общества. Изучение наработок социальных наук в сфере исследования блогосферы является значительной задачей в развитии аналитики спецслужб государства.

Выводы

Количество пользователей и коммуникаций в киберпространстве становится все больше и государство уже не в состоянии контролировать процессы, происходящие в Сети. В таких условиях государственные службы обращаются к методам стимулирования общественно полезной гражданской активности в интернете, к работе с агентами политических коммуникаций. Считаем, что среди негосударственных субъектов в противодействии информационным угрозам экстремизма и терроризма определенную роль должны играть представители социальных групп хакеров, блогеров и цифровых активистов.

Если до сих пор исследователи и практики-специалисты в обеспечении национальной безопасности в большей мере рассматривали только вопросы противодействия деятельности представителей этих групп, то автор призывает более пристально отнестись к изучению особенностей жизни и деятельности хакеров, цифровых активистов и блогеров и начать разрабатывать методы и способы взаимодействия с ними с целью противодействия информационным угрозам национальной безопасности.

Изучение особенностей этих социальных групп, дальнейшее выстраивание взаимодействия с ними должно привести к более эффективной борьбе с терроризмом и экстремизмом в интернете, в частности, профилактики этих угроз. Государство не должно «использовать» представителей этих групп. Оно должно рассматривать их как граждан, как субъектов в противодействии угрозам, обращаться к их сетям и платформам как к организациям-представителям гражданского общества.

Важно заметить, что российское государство значительно уступает сегодня в работе с политически активными хакерами, блогерами и цифровыми активистами США и другим западным странам. Между тем, в мире уже созданы специальные интерфейсные структуры, которые перенацеливают усилия цифровых активистов с внутриполитических проблем западных стран на борьбу с государственными органами власти России, Китая и Ирана. Аналитики отмечают, что в США сложился военно-разведывательно-высокотехнологический комплекс. В состав комплекса входят компании, типа Google, Facebook, IBM, значительное число благотворительных фондов нового поколения, созданных на деньги высокотехнологичных компаний и их учредителей, инвестиционные фонды, университеты, организационные структуры разведывательных сообществ западных стран [7, 10, 11].

По поводу цифрового активизма Е. С. Ларина отмечает, что «на наших глазах из независимой, набирающей могущество, молодой силы чем дальше, тем больше цифровой активизм превращается в неявно управляемый и используемый инструмент» [7, с. 78]. Новые социальные группы интернета, их возможности с успехом осваиваются спецслужбами и политическими силами западного мира. В последнее время их силы используются не столько в борьбе с экстремизмом и терроризмом, сколько во взращивании экстремистских настроений в других государствах. В подобном контексте сложно не согласиться с тем, что если государством и общественными организациями не будет вестись работа по эффективному взаимодействию с технически и профессионально продвинутой молодежью,

не будут предоставляться дополнительные возможности и ресурсы, то все это будет сделано другими.

Задачи эффективного взаимодействия, предоставления возможностей для продвинутой молодежи отсылают нас, в том числе, к такой области политики государства как работа с молодежью. Речь идет о дальнейшем развитии патриотического воспитания в образовательных организациях, о поддержке волонтерских движений, о доступности занятий спортом, музыкой, другими сферами досуга. Отдельной задачей в этом списке стоит дальнейшее изучение социальных трансформаций, охватывающих информационное пространство и ведущих к появлению новых моделей цифрового поведения молодых людей.

ЛИТЕРАТУРА

1. СУНДИЕВ И. Ю., СМИРНОВ А. А. **Информационное противодействие терроризму в сети Интернет** // Вестник Национального антитеррористического комитета. 2015.— № 1 [12] — С. 85–103.

2. АЛЕКСАНДР БАРД И ЯН ЗОДЕРКВИСТ. **Netократия. Новая правящая элита и жизнь после капитализма** URL: http://www.rulit.me/books/netokratiya-read-124507-1.html.

3. СТЭНДИНГ Г. **Прекариат: новый опасный класс.** / М.: Ад Маргинем Пресс, 2014.— 328 с.

4. СМ.: URL: **https://ru.wikipedia.org/wiki/**

5. ХИМАНЕН П., КАСТЕЛЬС М. **Информационное общество и государство благосостояния: Финская модель.** / М.: Логос, 2002.— 224 с.

6. КАСТЕЛЬС М. **Власть коммуникации: учеб. пособие** / Пер. с англ. Н. М. Тылевич, под науч. ред. А. И. Черных.— М.— 2017. 591 с.

7. ЛАРИНА Е. С. **Феномен цифрового активизма: риски, угрозы, возможности** // Информационные войны. 2016.— № 3 (39) — С. 71–78.

8. **Topkin.ru** . URL: topkin.ru/best/lyudi/samyie-populyarnyie-bloggeryi-rossii/

9. КОЧЕТКОВА М. О. **Жанровая динамика дискурса блогосферы: социолингвистический аспект:** дис. … д-ра филос. наук / М. О. Кочеткова.— Томск., 2016.— 252 с.

10. АКОПОВ Г. Л. **Хактивизм в процессе информационно-политических конфликтов** // Вопросы безопасности.— 2014.— № 1.— С. 24–32.

11. ГРИНЯЕВ, С. Н. **Взгляды военных экспертов США на ведение информационного противоборства** / С. Н. Гриняев // Зарубежное военное обозрение.— 2001.— № 8.— URL: http://psyfactor.org/infowar1.htm.