УДК 32.019.57

ГЛОБАЛЬНЫЕ «ГИБРИДНЫЕ» АКТОРЫ ИНФОРМАЦИОННОГО ВМЕШАТЕЛЬСТВА В СОВРЕМЕННЫЕ ПОЛИТИЧЕСКИЕ ПРОЦЕССЫ

С. В. Володенков

Московский государственный университет им. М. В. Ломоносова,
Российская Федерация, 119991, Москва, Ленинские горы, 1

Статья посвящена вопросам, связанным с изучением актуальной практики трансформации Интернета в условиях его технологической эволюции. Показано, что на современном этапе развития цифрового пространства формируются глобальные акторы, функционирующие в гибридных режимах и предпринимающие попытки установления тотального контроля над информационно-коммуникационными потоками в онлайн-среде. Разнообразие взаимоотношений подобного рода акторов определяет актуальную практику информационного противоборства в политической сфере, характеризующуюся активным внедрением в Интернете технологий манипуляции массовым сознанием, основанных на сборе конфиденциальных пользовательских данных и анализе их «цифровых следов». Анализируются не только традиционные государственные акторы, но и такие современные акторы, как крупные IT-корпорации, а также террористические организации. В условиях конкуренции за право доминирования в публичном цифровом пространстве и при возможности получения прямого коммуникационного доступа к онлайн-пользователям подобные структуры игнорируют наличие суверенных национальных сегментов Интернета, осуществляя экстерриториальное вторжение в национальные информационные системы. Это приводит к формированию новых типов угроз национальной безопасности в ситуации широкого разнообразия конкурентных отношений в цифровой среде и борьбы в информационно-коммуникационной сфере. На современном этапе технологической эволюции интернет-пространства существуют серьезные риски возникновения системы глобального контроля и манипулятивного доминирования со стороны акторов нового «гибридного» типа, преследующих различные интересы, что непосредственным образом может влиять на изменение традиционных способов информационно-коммуникационного противоборства в пространстве глобальной политики.

Ключевые слова: политическая манипуляция, общественное сознание, интернет-технологии, политическая коммуникация, политический контроль, информационное противоборство.

Анализ актуальной практики развития современных информационно-коммуникационных ресурсов и технологий позволяет констатировать наличие такой угрозы, как трансформация Интернета в монополизированное коммуникационное пространство, находящееся под управлением небольшой группы глобальных акторов, контролирующих сетевую коммуникационную ин-

https://doi.org/10.21638/11701/spbu23.2019.304

фраструктуру, включая каналы массовой коммуникации и информационные ресурсы. Данные акторы обладают потенциалом для определения форматов использования интернет-технологий в политической сфере, а также влияния на процессы генерации и трансляции политического контента по каналам интернет-коммуникации как в содержательном, так и в технологическом аспектах. Кроме того, подобные акторы имеют доступ к любой пользовательской информации, что обеспечивает возможности выявления политической лояльности конкретных пользователей и моделей их политического поведения, а также применения различных административных и политических санкций по отношению к протестным сетевым аудиториям независимо от принадлежности к конкретному государству.

Реализация такого сценария развития с высокой долей вероятности может привести к появлению *кибердейтократии* — глобальной информационной элиты, контролирующей сетевое пространство. Помимо этого, данный сценарий предполагает формирование потенциала для возникновения нового типа глобального политического устройства, основанного на тотальном доминировании кибердейтократии в мировом политическом пространстве, а также на возможностях вмешательства в политические процессы любого современного государства, не обладающего соответствующим потенциалом и инфраструктурой для противодействия и защиты.

Элементы реализации данного сценария со стороны соответствующих интересантов мы можем наблюдать уже сейчас, когда ведущие информационные ресурсы и каналы массовой коммуникации находятся в управлении небольшого числа представителей политической элиты одного государства.

Сегодня потенциал влияния на общественное сознание монополизируется посредством продвижения в глобальном интернет-пространстве таких ресурсов, как *YouTube*, *Facebook*, *Twitter*, *Google*, *Dropbox*, *Instagram*, *Yahoo*, которые могут быть использованы как для политического воздействия на общественное сознание в общемировом масштабе посредством управления и контроля контента, формирующего политическую псевдореальность для миллиардов интернет-пользователей, так и для тотального контроля за пользовательским контентом и сетевой активностью любого отдельно взятого человека.

Такого рода глобальные сетевые ресурсы активно участвуют в программах слежки за интернет-пользователями независимо от их национальной и территориальной принадлежности, что было продемонстрировано в рамках деятельности Агентства национальной безопасности США, осуществляющего общемировой контроль за коммуникационной активностью сотен миллионов пользователей.

Кроме того, большинство подобных ресурсов находятся под контролем представителей политической элиты США. Так, в 2014 г. в состав совета директоров компании *Dropbox*, предоставляющей услуги сетевого хранения данных и имеющей почти 300 млн пользователей по всему миру, вошла бывший глава Госдепартамента США Кондолиза Райс.

Отдельное внимание необходимо обратить на возможности формирования моделей восприятия политической реальности и моделей поведения, основан-

ных на анализе личных данных и персональной сетевой активности конкретных пользователей и сообществ.

Так, служба национальной разведки США с 2011 г. реализует проект анализа публичных данных и записей социальных медиа, включая социальные сети и блогосферу, популярные новостные интернет-ресурсы, для последующего прогнозирования общественно-политических трендов и кризисов.

Одновременно Управление перспективных разработок Министерства обороны США инициировало разработку программного обеспечения для мониторинга и анализа информационных потоков в интернет-пространстве в рамках изучения влияния публичной сетевой информации на поведение людей.

В июне 2013 г. глава национальной разведки США Джеймс Клэппер признал: власти страны получают данные о тех пользователях интернет-компаний, которые не являются американцами, что позволяет спецслужбам изучать электронные письма, фотографии и другие документы таких пользователей (Director James R. Clapper…, 2013).

По сообщениям *Washington Post*, американские спецслужбы имеют прямой доступ к серверам девяти крупнейших интернет-компаний — *Google*, *Facebook*, *Yahoo*, *PalTalk*, *AOL*, *Skype*, *Microsoft*, *Apple*, *YouTube* (данная программа спецслужб носит название PRISM) (Gellman, Poitras, 2013).

Однако не только США единолично стремятся поставить под контроль пользовательские данные. Так, организация «Пять глаз» (*Five Eyes*), созданная для взаимодействия в сфере обеспечения технической интероперабельности военно-морских сил США, Великобритании, Канады, Австралии и Новой Зеландии, на прошедшей в 2018 г. встрече *Five Country Ministerial* (FCM) потребовала от любых технологических компаний предоставить доступ к зашифрованным данным и устройствам всех их пользователей. Примечательно, что, согласно опубликованному постановлению, «конфиденциальность не является абсолютной», «государственные органы должны иметь возможность иметь доступ к частной информации», а ответственность за обеспечение доступа к «законно полученным данным», включая содержание сообщений, лежит как на правительственных организациях, так и на технологических компаниях (Five country ministerial 2018).

«Правительства “Пяти глаз” поощряют поставщиков услуг в области информационных и коммуникационных технологий добровольно устанавливать законные решения для доступа к своим продуктам и услугам, которые они создают». Иными словами, все технологические компании, связанные со сферой массовой коммуникации, начиная от производителей электроники наподобие *Apple* и *Samsung* и заканчивая сервисами наподобие *Facebook* и *WhatsApp*, должны оказывать «помощь» спецслужбам: «Если правительственным службам по-прежнему будут препятствовать в законном доступе к информации, необходимой для защиты граждан наших стран, мы можем применять технологические, принудительные, законодательные или другие меры для получения законного доступа» (Five country ministerial 2018). По своей сути *Five Eyes* — военно-разведывательный альянс пяти государств, обеспечивающий сбор разведывательной информации по всему миру.

Попытки установить глобальный контроль над интернет-пространством сегодня оправдываются и под прикрытием противостояния угрозе внешнего информационного вмешательства, для чего необходимо создание и расширение возможностей противодействия иностранному вмешательству и дезинформации: «Мы также все чаще наблюдаем использование онлайн-пространств для распространения дезинформации, разделения и подрыва наших демократических институтов. Распространение вмешательств и дезинформации подрывает доверие граждан к онлайн-коммуникациям и информации, сводя на нет преимущества и возможности, которые создают коммуникационные и социальные медиаплатформы… Мы призываем оправдать ожидания общественности в отношении безопасности в Интернете путем разработки и внедрения возможностей для предотвращения загрузки нелегального и незаконного контента, а также для выполнения срочного и немедленного удаления в случае невозможности предотвратить загрузку» (Five country ministerial 2018). Кто при этом будет определять легальность и законность контента, в документе не указывается, что подразумевает наличие у глобальных акторов права самостоятельно определять, какой контент в «свободном и открытом Интернете» соответствует закону, а какой нет.

Учитывая глобальный характер осуществляемого контроля, данные о сетевой активности российских пользователей также становятся доступными заинтересованным внешним службам. Подобная информация о поведении интернет-пользователей представляет практический интерес для организации эффективного внешнего влияния на них независимо от принадлежности к тому или иному государству.

В связи с этим обращают на себя внимание слова, произнесенные исполнительным директором *Google* Эриком Шмидтом в Лондоне в одном из его выступлений, посвященных скорому наступлению такого мира, в котором *Google* накопит так много личной информации о его пользователях, что будет в состоянии формировать каждый аспект их жизни. Шмидт заявил: «Мы не нуждаемся в том, чтобы вы нажимали на все клавиши в вашем компьютере. Мы знаем, где вы находитесь и где вы были. Мы можем узнать в общих чертах, о чем вы думаете. Мне кажется, что большинство людей не хочет, чтобы *Google* отвечал на их вопросы, а им хочется, чтобы он указал им, что они должны делать… Мы знаем все, что вы делаете, и правительство может за вами наблюдать. Мы узнаем, где вы находитесь в районе 50 см, и мы сократим это расстояние до нескольких сантиметров… Ваша машина будет вести вас сама, и это неправильно, что машины были изобретены до компьютеров… Вы никогда не бываете одни, и вам не скучно» (Watson, Jones, 2013).

Сегодня большинство глобальных сетевых ресурсов, посредством которых люди по всему миру ищут необходимую им информацию и коммуницируют друг с другом, собирают пользовательскую информацию, позволяющую определять особенности конкретного пользователя и выдавать ему персонализированный контент, что, с учетом огромных потоков информации в Интернете, не поддающихся самостоятельному анализу, способно влиять на формирование у конкретного человека специализированного мировосприятия, а также поведения.

По сути, данная практика становится технологией «мягкого вторжения» в сознание массового гражданина.

С появлением персонализированного поиска в *Google* каждый пользователь по одному и тому же поисковому запросу получает отличную от других пользователей информацию, формируемую с учетом индивидуальных особенностей личности, которые поисковик выдает на основе анализа поведения пользователя. Алгоритмы поисковой выдачи во многом непрозрачны и закрыты от постороннего взгляда, а возможности манипуляции информационным потоком помещены в своего рода «черный ящик», на выходе из которого мы и получаем конечный контент. Существует значительное число примеров того, что поисковая выдача *Google* оказывается «смещенной». Например, получив запрос «три белых подростка», поисковик *Google* выдавал стоковые изображения улыбающихся и веселых тинейджеров, в то время как на запрос «три чернокожих подростка» появились фотографии чернокожих молодых людей, задержанных полицией, что многими было воспринято как проявление расизма.

Подобных примеров искажения поисковой выдачи можно привести достаточно много, в том числе и тех, которые имеют непосредственное отношение к России. Так, в 2017 г. исполнительный директор *Google* Эрик Шмидт на форуме по международной безопасности в Галифаксе заявил, что *Google* снизит выдачу сайтов с «российской пропагандой»: «Мы стараемся перенастроить систему и предотвратить это [влияние российской пропаганды]». Поисковик намерен бороться с российскими сайтами, попадающими в поисковую выдачу *Google News*, в первую очередь с телекомпанией *RT* и агентством *Sputnik*.

Таким образом, даже на основе официальных заявлений можно сделать вывод о том, что поисковая выдача *Google* будет в определенной мере «смещена» и управляема, по крайней мере в отношении российских ресурсов (хотя на самом деле масштаб проблемы значительно шире). С учетом того, что *Twitter* запретил *RT* и *Sputnik* публиковать на своей площадке рекламу, о равных возможностях для различных новостных ресурсов в интернет-пространстве говорить не приходится.

В том же 2017 г. *Google* объявил о глобальном запуске механизма проверки новостей на фейки и вбросы *FactCheck* (Fact Check…, 2017). В итоге результаты поисковой выдачи будут сразу снабжаться оценкой «правдивости», которая может варьироваться от «правда» до «ложь» с несколькими промежуточными стадиями. Однако самое примечательное заключается в том, что работа по «оценке правдивости» передана на аутсорс некоему «международному сообществу репортеров», включающему 115 активных организаций по всему миру (при этом ни одной из России). Правдивость же сообщений о конфликте в Донбассе должны оценивать четыре украинские организации, что, безусловно, сделает информацию о реальных событиях ангажированной и смещенной к украинской версии. Аналогичная ситуация и с конфликтом в Южной Осетии в 2008 г. — результаты поисковой выдачи по данному вопросу должна проверять грузинская организация, финансируемая европейскими фондами и посольством США в Грузии.

Кроме того, большинство наиболее популярных ресурсов, помимо *Google*, в том числе *Facebook*, *Gmail* и *YouTube*, активно используют так называемые идентификационные *cookie*-файлы и персональные веб-маяки, позволяющие отслеживать персональную сетевую активность и индивидуальные предпочтения пользователя. По сути, речь идет о создании глобальной системы шпионажа в интернет-пространстве.

Не случайно в последние годы деятельность по обработке персональных данных интернет-пользователей стала высокодоходным направлением бизнеса. В данном сегменте появились глобальные игроки *BlueKai* и *Acxiom*, хранящие персональные данные сотен миллионов пользователей, касающиеся их поведения и предпочтений в сети.

Посредством использования полученных данных формируются возможности тотального управления общественным сознанием в мировом масштабе. В этих целях осуществляется принудительное конструирование персонализированной информационной картины мира для каждого пользователя интернет-ресурсов. Кроме того, на основе анализа огромного массива информации отслеживаются политические тренды любого государства для последующего использования полученной информации в интересах субъектов глобального политического управления.

В качестве примера можно привести резонансный секретный эксперимент *Facebook* (Facebook conducted..., 2014), в рамках которого 689 тыс. пользователей без их ведома видели на своих страницах специально сформированную персональную ленту новостей, имевшую различную эмоциональную окраску. В дальнейшем исследовались реакция пользователей и их поведенческая активность в собственных аккаунтах с целью выявления поведенческих зависимостей от типов эмоциональной окраски новостных сообщений.

Очевидно, что подобного рода эксперименты по изучению различных моделей информационно-коммуникационного воздействия на поведение пользователей в дальнейшем будут активно применяться и другими социальными сервисами для разработки наиболее эффективных методик управления индивидуальным сознанием.

Таким образом, технологии управления выдачей контента начинают влиять непосредственно на сознание людей, принимающих решения и осуществляющих действия на основе полученных в Интернете данных. Манипулятивные возможности современных глобальных онлайн-ресурсов весьма высоки. Выдача контента, заранее отрегулированная в интересах определенных акторов, приведет к превращению многих соцмедиа и поисковиков в глобальные инструменты манипуляции и пропаганды. С их помощью крупные политические и экономические игроки смогут оказывать прямое влияние на массовое сознание в онлайн-пространстве. Многие пользователи активно потребляют готовую информацию и зачастую не способны критично воспринимать контент.

Появление глобальных акторов, обладающих технологическим потенциалом, развитой информационно-коммуникационной инфраструктурой и соответствующими компетенциями, ставит вопрос о возможном вмешательстве

в суверенные политические системы (включая такую их составляющую, как избирательный процесс) совершенно в иной плоскости, отличной от традиционных конфликтов «государство — государство». Не случайно последней «жертвой» активности подобных акторов стал Президент США Дональд Трамп, который выступил с обвинением *Google*, *Facebook* и *Twitter* в необъективности и подтасовке результатов поисковой выдачи и публикаций в новостной ленте. Он написал в своем *Twitter*-аккаунте: «*Google* и другие подавляют голоса консерваторов, скрывают хорошую информацию и новости. Они контролируют то, что мы можем и не можем видеть. Это очень серьезная ситуация…» (Donald Trump's Twitter account, 2018).

Глобальные акторы могут функционировать в новых «гибридных» форматах и представлять интересы не только конкретного государства, но и группы государств, а также крупных корпораций и частных лиц, включая неинституциональных акторов, имеющих собственные политические цели. К числу подобных акторов мы относим и международные террористические организации, действующие благодаря экстерриториальности современных информационно-коммуникационных технологий по всему миру. Оказываемое террористическими структурами пропагандистское воздействие на массовое сознание впоследствии может напрямую влиять и на модели электорального поведения, на уровень поддержки радикальных и экстремистских организаций, претендующих на участие в публичном политическом процессе.

Говоря о высоком уровне информационно-коммуникационной активности террористических организаций в онлайн-пространстве, следует сослаться на выложенную *Wikileaks* дипломатическую переписку, согласно которой пропагандистская деятельность «Аль-Каиды» и «Талибана» в Интернете, включая работу в социальных медиа, создание информационных сайтов, размещение видеоматериалов на портале *YouTube* с использованием современных технологий продвижения контента, не уступает по своим масштабам информационно-коммуникационным программам США (Wikileaks…, 2019). Еще в октябре 2008 г. спецслужбы США стали рассматривать *Twitter* как возможную площадку для контакта террористов (304th Military*…,* 2008).

Подобное размывание традиционных агентов внешнего вмешательства предъявляет новые требования к обеспечению национальной информационной безопасности современных государств, сталкивающихся с новыми потенциальными «гибридными» оппонентами, определение активности которых становится отдельной важной задачей.

Не случайно президент США отметил в своем *Twitter*-аккаунте: «Я никогда не говорил, что Россия вмешивалась в выборы. Я говорил, что это могла быть Россия, Китай или любая другая страна или группа. Это мог быть гений в четыреста фунтов, сидящий в спальне и играющий на компьютере» (Vazques, 2018). Данное высказывание Трампа наглядно демонстрирует сложности с детектированием источников угрозы в условиях появления новых глобальных акторов вмешательства в национальные политические процессы.

Подведем итоги. На современном этапе технологической эволюции интернет-пространства конструируется система глобального контроля и мани-

пулятивного доминирования со стороны акторов нового «гибридного» типа, преследующих различные интересы, что самым непосредственным образом влияет на эволюцию традиционных способов информационно-коммуникационного противоборства в режиме *state vs state*. Интернет сегодня уже не может рассматриваться как открытое пространство для демократического транзита, что было характерно для первых стадий развития онлайн-коммуникаций. Он представляет собой в первую очередь высококонкурентное поле глобального информационного противоборства между технологически развитыми акторами, претендующими на тотальное доминирование в цифровой среде без учета каких-либо национальных границ и суверенных онлайн-сегментов в современных государствах.

Литература/References

304th Military Intelligence Battalion Open Source Intelligence Team. *Sample Overview: al Qaida-Like Mobile Discussions & Potential Creative Use*. October 16, 2008. Available at: http://www.fas.org/irp/eprint/mobile.pdf (accessed: 21.02.2019).

Director James R. Clapper interview with Andrea Mitchell. *Office of the Director of National Intelligence*. June 8, 2013. Available at: https://www.dni.gov/index.php/newsroom/speeches-interviews/speeches-interviews-2013/item/874-director-james-r-clapper-interview-with-andrea-mitchell (accessed: 21.02.2019).

Donald Trump's Twitter account. August 28, 2018. Available at: https://twitter.com/realDonaldTrump/status/1034456273306243076 (accessed: 21.02.2019).

Five country ministerial 2018. *Australian Government. Department of Home Affairs. National security*. Available at: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018 (accessed: 21.02.2019).

Gellman B., Poitras L.U.S. British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*. June 6, 2013. Available at: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (accessed: 21.02.2019).

Facebook conducted secret psychology experiment on users' emotions. *The Telegraph*. June 28, 2014. Available at: http://www.telegraph.co.uk/technology/facebook/10932534/Facebook-conducted-secret-psychology-experiment-on-users-emotions.html (accessed: 21.02.2019).

Fact Check now available in Google Search and News around the world. April 7, 2017. Available at: https://blog.google/products/search/fact-check-now-available-google-search-and-news-around-world/ (accessed: 21.02.2019).

Vazques M. *Trump: 'They are laughing their asses off in Moscow' over how US handled Russia investigations.* February 18, 2018. Available at: https://edition.cnn.com/2018/02/18/politics/trump-russia-laughing-moscow-tweets (accessed: 21.02.2019).

Watson P.J., Jones A. Google-Berg: Global Elite Transforms Itself For Technocratic Revolution. *Infowars.com*. May 13, 2013. Available at: http://www.infowars.com/google-berg-global-elite-transforms-itself-for-technocratic-revolution/ (accessed: 21.02.2019).

Wikileaks. WarDiaries. 2019. Available at: https://wardiary.wikileaks.org/search/?q=Taliban+Broadcast&sort=date&type_=Non-Combat%20Event (accessed: 21.02.2019).

Володенков Сергей Владимирович — д-р полит. наук, доц., проф.; s.v.cyber@gmail.com

Статья поступила в редакцию: 22 февраля 2019 г.;

рекомендована в печать: 25 июня 2019 г.

Для цитирования: *Володенков С.В.* Глобальные «гибридные» акторы информационного вмешательства в современные политические процессы // Политическая экспертиза: ПОЛИТЭКС. 2019. Т. 15, № 3. С. 383–391. https://doi.org/10.21638/11701/spbu23.2019.304

GLOBAL "HYBRID" ACTORS OF INFORMATION INTERFERENCE IN THE CONTEMPORARY POLITICAL PROCESSES

Sergey V. Volodenkov

Moscow State University named after M. V. Lomonosov,
1, Leninskie gory, Moscow, 119991, Russia; s.v.cyber@gmail.com

This article is devoted to issues related to the study of the current practice of the Internet transformation in terms of its technological evolution. The paper shows that at the present stage of development of the digital space, global actors are functioning and operating in hybrid modes, and attempting to establish total control over information and communication flows in the online environment. The diversity of relationships of this kind of actors forms the current practice of informational confrontation in the political sphere, characterized by the growing implementation of mass consciousness manipulation technologies on the Internet based on collecting confidential user data and analyzing their "digital traces". The article analyzes not only traditional state actors but also such modern actors as large IT corporations, as well as terrorist organizations. Under the conditions of competition for dominance in the public digital space and the possibility of obtaining direct communication access to online users such structures ignore the presence of sovereign national segments of the Internet, carrying out an extraterritorial intrusion into national information systems, which creates new types of threats to national security in a highly diverse competitive relationship in the digital environment for the right to dominate in the information and communication sphere. The paper concludes that at the present stage of the technological evolution of the Internet space there are severe risks of forming a system of global control and manipulative dominance on the part of the actors of the "hybrid" type pursuing different interests, which can directly affect the transformation of traditional formats of information and communication confrontation in the global policy space.

Keywords: political manipulation, public consciousness, Internet technologies, political communication, political control, information confrontation.

Received: February 22, 2019

Accepted: July 25, 2019

For citation: Volodenkov S. V. Global "Hybrid" Actors of Information Interference in the Contemporary Political Processes. *Political Expertise: POLITEX*, 2019, vol. 15, no. 3, pp. 383–391. https://doi.org/10.21638/11701/spbu23.2019.304 (In Russian)