УДК 32.019.5

ВЫБОРЫ В США: ТРИУМФ ЦИФРОВОЙ ДЕМОКРАТИИ?

© 2017 г. **Е.А. Роговский***

Статья поступила в редакцию 28.12.2016

Применение информационных технологий в ходе кампании по выборам президента США в 2016 г. носило особенный характер. Круг соответствующих приложений вышел далеко за рамки традиционных направлений, типичных для кампании 2008 г. Каждая сторона для реализации целей своей предвыборной стратегии заручилась поддержкой мощных ИКТ-корпораций (Х. Клинтон – "Гугл" (Google), Д. Трамп – "Фейсбук" (Facebook) и применила уникальные технологии ("Гугл" – манипуляции с помощью своего поискового механизма[1]; "Фейсбук" – выявление подсознательных политических предпочтений на уровне конкретных избирателей – пользователей своей социальной сети). Проведенное исследование объясняет эффективную победу Д.Трампа, одновременно вскрывая качественно новые проблемы информационной безопасности.

Ключевые слова: *Д. Трамп, Х. Клинтон, выборы 2016 г. в США, "Гугл" (Google), "Фейсбук" (Facebook), манипуляции с помощью поисковых механизмов.*

Политики и военные в США осознали возможность использования интернета против интересов страны

Многочисленные публикации представителей спецслужб, военных и политиков свидетельствуют, что в США прекрасно знают о возможностях использования сетевых технологий против интересов страны[2]. В этих публикациях подчёркивается, что террористы могут использовать социальные сети для рекрута новых членов своих организаций, планирования террористических актов и политических провокаций, сбора информации, распространения слу-

* **Роговский Евгений Александрович, руководитель Центра военно-промышленной политики Института США и Канады РАН (ИСКРАН)**. Российская Федерация, 121069 Москва, Хлебный пер., 2/3. (rogowski@rambler.ru)

[1] "Гугл" (*Google*) – сетевая монополия, которая используется для поиска в большинстве стран мира (кроме России и Китая) и которая решает, что покупают, во что одеваются, куда поедут путешествовать её пользователи, а также формирует отношение к кандидатам на выборах. Она покажет пользователям всё, что захочет ***сама***. "Гугл" сама ранжирует страницы в поисковой выдаче, в зависимости от того, какое мнение по тому или иному вопросу она хочет сформировать. Это и есть манипуляционный эффект поисковой системы (*Search Engine Manipulation Effect – SEME*), и "Гугл" покажет результаты поиска в том порядке, в каком захочет (http://goldenfront.ru/articles/view/google-eto-cifrovoj-kgb-uchenyj-protiv-internet-poiskovika/).

[2] Weimann Gabriel. How Modern Terrorism Uses the Internet. SPECIAL REPORT 116, March 2004. Available at: http://www.usip.org/pubs/specialreports/sr116.html (accessed 21.12.2016).

хов и ложных сведений, а также для того, чтобы посеять панику, ввести кого-нибудь в заблуждение, очернить отдельных лиц, группы людей или компании.

Когда уровень доступных террористам технологий превысил уровень противодействия со стороны ФБР, Б. Обама обратился к инноваторам Кремниевой долины с настоятельной просьбой предпринять что-нибудь, чтобы предотвратить использование террористами онлайновых социальных сетей для радикализации общества и мобилизации рекрутов, т.е. использовать против интересов США те "технологические возможности, которые предоставило нам современное цивилизованное общество". В своём обращении к нации в январе 2016 г. (после теракта в Сан-Бернандино), Президент США настоятельно просил лидеров высокотехнологичных компаний затруднить террористам использование высоких технологий "для ухода от правосудия"[3].

Информационная безопасность – неотъемлемая часть национальной безопасности

Ещё в начале 2015 г. Обама объявил, что сферу кибербезопасности его администрация считает приоритетной, и подчеркнул: "Из-за угроз в киберпространстве наша критически важная инфраструктура продолжает находиться в состоянии риска… Наш долг состоит в обеспечении безопасности киберпространства, поддержании интернета в открытом, взаимодействующем, безопасном и надежном состоянии"[4].

Но как показали выборы 2016 г., американское общество сильно поляризовано и конфликтно. Специфика острой политической борьбы заставляет относиться к противнику как к врагу, и соответственно, применять против него все доступные средства. Отсюда рождается спрос на весьма изощрённые сценарии дискредитации того или иного кандидата. Фактически, с помощью онлайновых социальных сетей создан удобный и эффективный способ пропаганды ненависти, инспирирования насилия и раздувания конфликтов, который сегодня интенсивно используется и террористами, и политиками. Доступ широких масс населения к новым информационным технологиям отражает явно дестабилизирующую зависимость – чем сильнее поляризовано общество, тем шире новые технологии используются в нём для "усугубления" ситуации.

Несмотря на неоднократные авторитетные предупреждения, самым громким из которых можно считать известный бестселлер М. Гудмана "Будущие преступления" [Goodman M., 2015], ***состояние избирательной системы США накануне президентских выборов 2016 г. с организационно-технической точки зрения оставалось весьма уязвимым.***

В ходе предвыборной кампании крупнейшие интернет-гиганты, такие как "Гугл", "Фейсбук" и др., систематически нарушали правила. В ходе президент-

[3] White House Wants Silicon Valley to Help Stop Terrorist Recruitment January 08, 2016. Available at: http://abc7news.com/technology/white-house-wants-silicon-[3]valley-to-help-stop-terrorist-recruitment-/1152288 (accessed 20.12.2016).

[4] Washington raises pressure on Silicon Valley in fight against terrorism. Available at: http://www.latimes.com/business/technology/la-fi-obama-silicon-valley-20160109-story.html (accessed 20.12.2016).

ских выборов они столкнулись с растущей критикой, вызванной наличием на их сайтах поддельной (лживой) информации[5]. Такие новости уже стали в США реальной политической проблемой.

Надо заметить, что электоральная система США находится в компетенции властей штатов. Она никогда не относилась к критически важным объектам стратегической инфраструктуры, а потому усилия федералов по киберзащите таких объектов затрагивали избирательный механизм лишь косвенно. По оценкам Разведывательного сообщества США никакое государство и никакой хакер, не могут модифицировать с помощью кибератаки результаты голосования – это чрезвычайно сложно[6].

Тем не менее, в своём совместном заявлении о безопасности выборов представители властей высказали убеждённость в том, что электоральная система США уязвима.

В этой системе можно выделить четыре сферы применения современных технологий (прежде всего интернета):

1) использование онлайновых социальных сетей для сбора средств и агитационного воздействия на избирателей;

2) онлайновые методы регистрации избирателей;

3) онлайновые процедуры голосования;

4) подсчёт поданных голосов[7].

О применении информационных технологий командами Х. Клинтон и Д. Трампа

Мысль о том, что современная Америка готова отказаться от некоторых демократических принципов проведения выборов близка известному канадскому журналисту и политику Д. Агню (*David Agnew*), который считает, что: "Умные правительства смотрят на интернет не как на угрозу [демократии], а как на потенциально позитивный инструмент вовлечения граждан в работу по управлению обществом"[8]. Старая – Джефферсоновская – демократия была на практике демократией не народа, а элиты и, соответственно, не для народа, а для элиты (*Democracy by and for an elite*).

В сложившемся в настоящее время в США напряжённом политическом противостоянии попытка увеличения "количества демократии в американском обществе" за счёт увеличения количества голосующих с помощью перехода к системе электронного голосования, может привести к обратному результату,

---

[5] Nick Wingfielg, Mike Isaac, Katie Benner. Google and Facebook Take Aim at Fake News Sites. Available at: http://www.nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html (accessed 10.12.2016).

[6] Joint DHS and ODNI Election Security Statement. Director of National Intelligence. Wash., DC 20511, October 07, 2016. Available at: https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement?tmpl=component&format=pdf (accessed 10.12.2016).

[7] Травкина Н.М., Роговский Е.А.. Цифровая демократия" и президентская кампания – 2016. Available at: http://www.rusus.ru/?act=read&id=505 (accessed 10.12.2016).

[8] Digital democracy. Stand by for online voting, and more. Economist. June 22nd 2000.

т.е. к сокращению "количества демократии", обусловленному существенным искажением воли избирателей, принявших участие в голосовании.

Как на Х. Клинтон работали "Гугл" и Центр новой американской безопасности

Демократы использовали сетевые технологии прежде всего для сбора денег и тенденциозной онлайновой агитации.

Корпорация "Гугл" когда-то относилась к политическому лоббированию весьма пренебрежительно. Однако при президентстве Б.Обамы эта корпорация обрела опыт мобилизации миллионов своих пользователей на политическую борьбу (как это было сделано в ходе противодействия закону "О безопасной онлайновой конфиденциальности" (*Secure Online Privacy Act – SOPA*) и постепенно превратилась в опытного мастера вашингтонского лоббирования[9]. Её сотрудники активно участвовали в работе таких элитных либеральных экспертных структур как Като институт (*Cato Institute*), "Компетитив энтерпрайз институт" (*Competitive Enterprise Institute*) и "Нью Америка фаундейшн" (*New America Foundation*), а бывший генеральный директор "Гугл" Э. Шмидт лично участвовал в разработке технологической системы президентской кампании Х. Клинтон.

Одной из важнейших особенностей предвыборной кампании Х.Клинтон можно считать исключительно лидерское поведение Обамы в социальных сетях[10]. Демократы, используя контекстную рекламу и другие возможности платформы "Гугл", "давили" на рядовых пользователей, забывая о непосредственной обратной связи с избирателями. Команда Х. Клинтон использовала поисковую систему "Гугл" весьма тенденцизно.

Что такое "эффект манипуляции"

Исследователь Р. Эпштейн из Института исследования поведения и технологий (*American Institute for Behavioral Research and Technology*)[11] предложил метод, позволяющий выявить в механизме сетевого поиска так называемый "эффект манипуляции" (*Search Engine Manipulation Effect – SEME*). Речь идёт о выявлении намеренного смещения результатов поиска вверх (к началу списка), т.е. о завышении оценки соответствия между вопросом пользователя и представленных ему результатов поиска.

---

[9] Google, once disdainful of lobbying, now a master of Washington influence. Available at: http://www.washingtonpost.com/politics/how-google-is-transforming-power-and-politicsgoogle-once-disdainful-of-lobbying-now-a-master-of-washington-influence/2014/04/12/51648b92-b4d3-11e3-8cb6-284052554d74_story.html?wpisrc=nl_hdln (accessed 18.12.2016).

[10] Here's how the first president of the social media age has chosen to connect with Americans. Available at: http://www.washingtonpost.com/news/politics/wp/2015/05/26/heres-how-the-first-president-of-the-social-media-age-has-chosen-to-connect-with-americans/?lkjadf (accessed 18.12.2016).

[11] Epstein Robert. How Google Could Rig the 2016 Election. millions of votes to a candidate with no one the wiser. August 19, 2015. Available at: http://www.politico.com/magazine/story/2015/08/how-google-could-rig-the-2016-election-121548 (accessed 18.12.2016).

Проверка с помощью этого метода различных онлайновых поисковых механизмов (в том числе "Гугл") позволила исследователям сделать выводы, существенные с точки зрения избирательного процесса: пристрастное ранжирование результатов поиска в интернете может существенно сместить преференции вплоть до 20% неопределившихся избирателей, и это ранжирование может быть замаскировано так, чтобы избиратели не осознают наличие какой-либо манипуляции.

В последствии выяснилось, что пристрастное ранжирование результатов интернет-поиска может предоставить корпорации "Гугл" чуть ли не право "решающего голоса" на президентских выборах в США. В самом деле, половина президентских выборов в США завершалась с разницей не более, чем в 7,6% голосов. Это выглядит как здоровая конкуренция, однако в эпоху интернета близость количества набранных кандидатами голосов представляется опасно уязвимой. Такая ситуация означает, что манипуляция с голосами "неопределившихся избирателей" может легко склонить чашу весов в пользу интересов манипулятора. (По мнению авторов этой работы, даже если только 60% населения того или иного штата имеет доступ к интернету и только 10% избирателей окажутся "неопределившимися", – этого может быть достаточно для достижения контролируемого результата выборов с победной маржой, достигающей 1,2%).

По мере того, как всё больше людей присоединялись к онлайновым социальным сетям, а влияние эффекта тенденциозного ранжирования на предпочтения избирателей росло, пропорционально возрастал и авторитет людей, контролирующих поисковые системы в социальных сетях. И поскольку абсолютное большинство людей результатам онлайнового поиска слепо доверяют, противодействовать этому практически невозможно. Такие люди искренне верят в то, что именно "Гугл" будет решать, кто станет американским президентом[12].

Таким образом, с точки зрения соблюдения демократических принципов избирательного процесса, неконтролируемый обществом онлайновый поисковый механизм в предвыборный период может представлять весьма существенную угрозу, которую следует отнести к сфере информационной безопасности. Угрозы национальной безопасности США для Х. Клинтон подготовил "Центр новой американской безопасности"; они содержатся в докладе его руководителя М. Флурнуа "Девять уроков по навигации национальной безопасности" (2016)[13].

Для того чтобы справиться с предстоящими проблемами, Америка должна восстановить доверие к своим действиям и вернуть глобальное лидерство.

С практической точки зрения в предвыборной кампании демократов в качестве рабочей стратегии последовательно использовался "китайский" политический принцип – "превратить плохое дело в хорошее". Так, трактуя уязвимость американского киберпространства на уровне государственных и партий-

[12] Rogers Adam. Google's Search Algorithm Could Steal the Presidency. Available at: https://www.wired.com/2015/08/googles-search-algorithm-steal-presidency/ (accessed 20.12.2016).

[13] "Nine Lessons for Navigating National Security". Available at: https://www.cnas.org/publications/reports/nine-lessons-for-navigating-national-security (accessed 20.12.2016).

ных организаций, поддержанная спецслужбами (!) Х. Клинтон представила её как результат злого умысла.

Администрация Обамы ставила задачу предотвратить использование глобальной информационной инфраструктуры против интересов США, но решить её не смогла.

В сентябре 2016 г. "демократическая элита" наконец-то признала, что Америка не может гарантировать "честность" проведение президентских выборов. Тут политически нейтрального Ассанжа или бывшего разведчика Сноудена было мало. Тут не подходят ни террористы ИГИЛ, ни даже весь Китай. ***Требовался самый крупный враг.*** По версии журнала "Форбс" – это В.В. Путин!

Судя по всему, последней каплей, спровоцировавшей публикацию 7 октября 2016 г. совместного заявления Министерства внутренней безопасности США и ЦРУ[14], стала идея дискредитации сразу всех разоблачений "независимых" источников, "запятнав их связями с Москвой"[15]. (Видимо именно эту идею министр иностранных дел РФ С.В. Лавров назвал "истерикой".)

"Нестерпимо" насущной такая дискредитация стала на фоне августовских (2016 г.) сообщений о том, что у АНБ украли важный шпионский код[16]. Это означало, что теперь против США может быть применено их собственное кибероружие, созданное для вмешательства во внутренние дела других стран! Руководство охватил страх, похожий на панику фокусника, у которого украли его волшебный ящик с зайцами, лентами и иными причиндалами.

Кого-то надо было срочно уличить в хакерских атаках, дискредитирующих президентские выборы. "Виновники" были тут же названы. Президент Обама стал "изображать жертву", демонстрируя уверенность в том, что за кибератаками на сервер Демократической партии США стоит российское государство. Эта идея стала стратегической "фишкой" всей предвыборной кампании Х. Клинтон.

Команда Трампа, на которую работали корпорация "Фейсбук" и Центр долгосрочной кибербезопасности (*Center for Long-Term Cybersecurity*) Калифорнийского университета в Беркли, придерживалась сугубо коммерческой стратегии организации предвыборной кампании.

Трамп считал, что цена голоса каждого выборщика резко возросла. Соответственно, следуя своему имиджу успешного бизнесмена, Трамп поставил своей команде задачу – сформировать стратегию его предвыборной кампании так, чтобы победу обеспечили не огромные деньги, а новейшие технические инновации, резко снижающие цену завоёванного голоса.

---

[14] Joint DHS and ODNI Election Security Statement. DIRECTOR OF NATIONAL INTELLIGENCE. WASHINGTON, DC 20511. October 07, 2016 Available at: https://www.dni.gov/алindex.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement?tmpl=component&format=pdf (accessed 11.12.2016).

[15] США заподозрили Россию в передаче украденных данных Wikileaks. Available at: https://news.mail.ru/politics/27443191/ (accessed 11.12.2016).

[16] The National Security Agency's primary mission is to spy on the electronic communicatins of countries and people overseas Available at: http://www.pbs.org/newshour/bb/analyzing-nsa-code-breach-context-recent-cybersecurity-events/ (accessed 11.12.2016).

Д. Трамп выступил против общения с избирателями с помощью гаджетов. После его знаменательной ноябрьской (2015 г.) встречи с избирателями в Спрингфилде (штат Иллинойс) Д. Трамп и его зять Дж. Кушнер пришли к заключению, что в их предвыборной кампании явно недооценены возможности социальных медиа. И Трамп попросил зятя заняться возможностями корпорации "Фейсбук". Кушнер позвонил в компанию (он в ней раньше работал) и попросил "просветить" его в отношении использования в сети методов "микротаргетирования"[17]. В результате бизнес-принципы корпорации "Фейсбук" были адаптированы под избирательную кампанию Д. Трампа.

По правде говоря, влияния сети "Фейсбук" на избирательный процесс, было тестировано задолго до выборов. Ещё в 2015 г. специальный тест показал, что надпись "голосуй", добавленная на экраны 61 млн. пользователей сети, привела к избирательным урнам дополнительно около 340 тыс. человек[18]. Некоторые специалисты отмечали, что если бы "Фейсбук" захотела "подтолкнуть" тех избирателей, кто благоволил конкретному кандидату, она легко могли бы взвинтить результаты выборов в нужную сторону[19]. Ещё за два года до президентских выборов "Вашингтон пост" обращала внимание своих читателей на то, что Республиканская партия проводит систематическую работу по согласованию списка своих избирателей со списком пользователей "Фейсбук".

В феврале 2014 г. "Фейсбук" отмечал своё десятилетие. К этому времени сеть имела более 1 млрд. пользователей и более 200 млрд. посещений, стала хостом для более 400 млрд. фото и в настоящее время регистрирует более 6 млрд. "лайков" в день. За четыре года, с 2013 по 2016 г., доля пользователей этой социальной сетью, назвавших её главным источником новостей, выросла с 47 до 66%. Сеть "Фейсбук" охватила всю территорию США и фактически сегодня является одним из высших форумов для политических дискуссий. Она изменила способы, которыми избиратели связываются друг с другом, изменила коммуникации с организациями, и даже с находящимися в Вашингтоне конгрессменами, которые ежедневно обновляют свои странички в этой социальной сети. Фактически за время своего существования "Фейсбук" успела превратиться в мощный политический инструмент[20].

Абсолютное большинство людей, "мигрировавших в цифровое пространство "Фейсбук", не хочет замечать своей информационной небезопасности. Эти люди не задумываются о том, что современные технологии больших баз данных (big data), используя сведения об их (поведении в сети, могут раскрыть весьма чувствительную персональную информацию, в том числе многие

---

[17] "Microtargeting: Knowing the Voter Intimately". // Winning Campaigns Magazine, Vol. 4, No.1.

[18] Zittrain "Facebook could decide an election without anyone ever finding out". Available at: http://www.newstatesman.com/politics/2014/06/facebook-could-decide-election-without-anyone-ever-finding-out (accessed 12.12.2016).

[19] How Facebook plans to become one of the most powerful tools in politics. Available at: http://www.washingtonpost.com/blogs/the-fix/wp/2014/11/26/how-facebook-plans-to-become-one-of-the-most-powerful-tools-in-politics/ (accessed 12.12.2016).

[20] How Facebook has changed the way we govern. Available at: http://www.washingtonpost.com/business/technology/how-facebook-has-changed-the-way-we-govern/2014/02/04/663cfc78-8dc5-11e3-833c-33098f9e5267_story.html?wpisrc=nl_headlines (accessed 12.12.2016).

"атрибуты личности" (от сексуальной ориентации до политических предпочтений). В рамках президентской гонки "Фейсбук" позволила команде Д. Трампа создать прецедент политического "микротаргетирования" американских избирателей, которыми в своём подавляющем большинстве "оказались" пользователи этой онлайновой социальной сети.

Что такое "микротаргетирование"

"Микротаргетирование" – это механизм точной настройки и использования социальных медиа для работы с целевой аудиторией. Это понятие предполагает "интимное знание" пользователей социальной сетью (в том числе избирателей). Задача микротаргетирования – побуждение избирателя голосовать за того или иного кандидата, – существенно сложнее задачи коммерческой рекламы – традиционного маркетингового таргетирования клиентов.

Для того, чтобы предсказать поведение конкретного избирателя на выборах, необходимо составить целостное представление о его личности. Для этого отдельных сведений о человеке (его доход, пол, раса, другие демографические параметры, марка машины, которую он водит, сорт кофе, который пьёт и проч., и проч.) недостаточно; такие сведения характеризуют человека лишь частично и не позволяют составить о нём достаточно точное представление как об избирателе. Здесь надо подобрать многосложный комплекс факторов, позволяющий надёжно прогнозировать, за кого проголосует тот или иной человек. Надо оперативно использовать мощные компьютерные технологии, позволяющие: 1) хранить в цифровом виде и архивировать гигантские массивы исходных данных, 2) наращивать количество и качество информации, поступающей из широкого спектра источников, 3) интегрировать разнородные массивы данных (информацию о результатах предшествующих голосований, географические данные, погоду и проч.), и 4) создавать аналитические инструменты обнаружения новых значимых структур и отношений, имеющих стратегическую и тактическую ценность.

В противостоянии с Х. Клинтон команда Д. Трампа в работе с избирателями полагалась не столько на СМИ (практически все они были против него), сколько на значительно более дешёвые мобильные сообщения (в том числе "лайки" и "смайлики"), появляющиеся перед глазами конкретного избирателя в любом месте, в любое время суток. При этом команда Д. Трампа рассылала свои сообщения с учетом индивидуальных профилей пользователей (*message tailoring*), прибегала к манипуляции их эмоциональным состоянием (*sentiment manipulation*) и даже применяла элементы искусственного интеллекта.

Так, "Фейсбук" позволил команде Трампа опробовать на своей платформе новые американские аналитические технологии "больших баз данных". Ставка на "Фейсбук" обеспечила предвыборной кампании Д. Трампа беспрецедентно высокую эффективность. Онлайновая социальная сеть, обрабатывая огромные массивы информации, успевала практически в реальном времени улавливать мельчайшие сдвиги в настроении избирателей и выдавать действенные рекомендации.

В сочетании с обычной рассылкой сообщений, взятое Дж. Кушнером на вооружение "микротаргетирование" показало своё явное превосходство. Если в начале предвыборной кампании Д. Трампа бейсболок и прочих вещей в день продавалось на 8 тыс. долл., то затем в день собиралось уже по 80 тыс. долл. Когда Кушнер занялся продвижением видеовыступлений тестя, удалось добиться 74 миллиона просмотров (при затратах всего в 160 тыс. долларов).

Фактически "Фейсбук" стал ключевым инструментом распространения не только пропагандистских сообщений Трампа, но и привлечения новых потенциальных сторонников. ***Речь идёт не о российских, а именно об американских инновационных технологиях, которые применялись гражданами США с помощью компьютеров, находящихся на территории этой страны! Именно это более всего раздражает демократов, придумавших иную причину своего поражения – внешнее вмешательство в американские выборы!***

Ключевые предвыборные ориентиры Д. Трампа

Геополитика XXI века признала появление нового информационного пространства (киберпространства), ставшего геостратегически важным. Это заставило задуматься о том, что в таком пространстве и у "банановой страны" и у великой державы могут быть одинаковые уязвимости в обеспечении информационной безопасности (в этом отношении великая держава может оказаться даже более уязвимой!). Настало время задуматься о киберугрозах, не только в рамках того или иного сиюминутного предвыборного спектакля, но и в контексте качественно новых угроз, которые могут возникнуть уже в ближайшем будущем.

В этой связи уместно вспомнить о сценариях, изложенных в документе "Будущее кибербезопасности 2020" (*Cybersecurity Future 2020*), подготовленном Центром долгосрочной кибербезопасности (ЦДКБ) в 2016 году[21].

Этот центр был специально создан для того, чтобы на основе долгосрочного прогноза киберугроз, адекватных развитию интернета и цифровых технологий в целом, определить новые направления работ в области кибербезопасности. Такой прогноз включает ряд новых вопросов глобальной безопасности, возникших на пересечении технологических и социальных аспектов развития информационных технологий[22].

Ещё совсем недавно некоторые учёные полагали, что в реальной жизни (оффлайн) люди слишком прочно связаны рамками различных социальных отношений, которые так или иначе ограничивают их возможности самовыражения, и что именно киберпространство предоставляет человеку анонимность и, следовательно, возможность свободного выбора политической идентичности [Бондаренко, 2005, с. 76-92]. Увы, теперь это не так! Киберпространство утеряло анонимность и приобрело ту самую прозрачность, которая мешает совпа-

[21] Cybersecurity Future 2020. Center for long-term cybersecurity. Available at: https://cltc.berkeley.edu/scenarios/ (accessed 13.12.2016).

[22] Exclusive Interview: How Jared Kushner Won Trump The White House. Available at: http://www.forbes.com/sites/stevenbertoni/2016/11/22/exclusive-interview-how-jared-kushner-won-trump-the-white-house/#39cbb47c2f50 (accessed 13.12.2016).

дению "латентной политической самоидентичности индивида" с его декларациями о поддержке тех или иных политических принципов. Теперь, опираясь на косвенные данные о поведении пользователя в онлайновой социальной сети, с помощью современных информационных технологий можно достаточно точно охарактеризовать его скрытую ("латентную") политическую самоидентичность.

Вопросам роста информационной уязвимости пользователей социальной сети "Фейсбук" посвящена статья автора[23], в которой упоминается новая бизнес-стратегия: ***свободу самовыражения пользователей не надо ограничивать, её надо использовать, извлекая прибыль из "неразумения и оплошностей", допускаемых всеми обитателями киберпространства***. Именно эти "оплошности" и стали экономическим ресурсом не только для нового, современного этапа развития ИКТ-бизнеса, но и для политики.

В отличие от демократов, команда Трампа осознавала уязвимость американского киберпространства на уровне конкретных пользователей; она тоже признавала необходимость "превратить плохое дело в хорошее" и преуспела в этом. Люди из "Фейсбук" точно знали, от кого, прежде всего, зависит информационная безопасность их клиентов. Эти люди отнюдь не призывали к защите конфиденциальности пользователей, их предвыборная стратегия преследовала противоположную цель – воспользоваться дефицитом конфиденциальности пользователей в собственных политических интересах.

Предвыборная стратегия Трампа имела два ключевых ориентира: большие базы данных и оптимизация расходов:

1) для привлечения максимального числа избирателей на свою сторону, избирателям надо говорить только то, что те хотят услышать. Такая информация готовилась на основе точной политической идентификации пользователей социальной сети "Фейсбук", (в том числе в региональном разрезе).

2) при планировании избирательных митингов надо было ориентироваться на "правильных" избирателей и предоставлять им обработанную информацию как можно дешевле.

Соответственно, эту кампанию можно разбить на пять этапов.

1. Выявление подсознательных предпочтений конкретных избирателей (технологии косвенной политической идентификации личности) на основе обработки представительного массива данных о пользователях сети "Фейсбук".

На этом этапе надо было "пропустить через детектор" как можно больше избирателей и зафиксировать их персональную реакцию ("лайки") на различные новости. Особого внимания заслуживало содержание предвыборного информационного трафика (ложь, провокационные вбросы, дезинформация, поддельные новости и проч.).

По мере приближения к дате президентских выборов масштабы распространения ложных сведений обеими конкурирующими сторонами нарастали. Так, демократы были замечены в систематическом распространении дезинформации на очень высоком пропагандистском уровне (неоднократные заявле-

[23] Роговский Е.А. Нужна ли анонимность в демократическом обществе. Available at: http://www.rusus.ru/?act=read&id=361 (accessed 12.12.2016).

ния в прессе руководителей спецслужб[24] и самой Х. Клинтон о вмешательстве России в американскую избирательную кампанию). Республиканцы же "работали на нижних этажах" – на уровне избирателей. Например, в сети "Facebook" быстро нарастал объём распространяемых поддельных новостей. Так, если в феврале – апреле 2016 г. 20 самых "горячих" новостей привлекли 12 млн. пользователей "Фейсбука", а поддельные новости – 3 млн. ("счёт" – 12 : 3), то ко дню выборов соотношение сил изменилось на 7,3 : 8,7[25]!

2. Разработка методики применения технологии косвенной политической идентификации личности для подготовки и проведения предвыборной кампании. (В том числе оценка представительности выборок – согласование списков зарегистрированных избирателей по избирательным участкам и округам с перечнем пользователей "Фейсбук". Статистическое обоснование надёжного агрегированного показателя, характеризующего средний уровень политического предпочтения для больших контингентов населения).

3. Расчёт показателей, характеризующих средний уровень политического предпочтения для массы зарегистрированных избирателей (по штатам);

4. Заблаговременное планирование (оптимизация) и проведение предвыборной кампании на основе полученных оценок, главное: в каких штатах может быть достигнут наилучший показатель "прибыли" (т.е. количества голосов в коллегии выборщиков) на инвестированный капитал? Заметим, что по сообщению Федеральной избирательной комиссии, к середине октября на предвыборную кампанию Трампа было затрачено примерно вдвое меньше средств, чем на кампанию Клинтон.

5. Систематический контроль (верификация) полученных оценок и оперативная корректировка планов проведения предвыборной кампании.

Как мы сегодня знаем, поставленная цель предвыборной стратегии была достигнута – Дональд Трамп на выборах победил. Но какой ценой?!

Фактически, его предвыборная кампания отняла у рядовых американцев право на тайное голосование, нанесла колоссальный ущерб всей системе американской демократии, дискредитировала её. Можно сказать, что против американского народа изнутри было применено самое современное информационное оружие ("Фейсбук"-сканирование и технологии больших баз данных), подрывающее веру избирателей в совместимость принципов демократии и интернета. Победу, добытую ценой изменения конституционных основ (отказ от права на тайное голосование), трудно признать юридически полноценной. Это пиррова победа. Без веры в демократию и её икону – интернет, Америка уже очень скоро станет совершенно иной страной.

---

[24] Office of the Director of National Intelligence. Available at: https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement?tmpl=component&format=pdf (accessed 13.12.2016).

[25] Silverman Craig. This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook. Available at: https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.ciG1W7qod#.rjD2pxLgA (accessed 13.12.2016).

Сценарии будущего развития

Быстрое развитие технологий заставляет задуматься о новых реальных киберугрозах, которые могут возникнуть уже в ближайшем будущем (и не только в рамках сценария той или иной заранее спланированной провокационной ситуации) и породить в системах информационной безопасности качественно новые опасные уязвимости.

Технологии развиваются очень быстро. Во второй декаде XXI века появились "Облака", "Интернет вещей", технологии больших баз данных, новые сенсоры, аналитика, а также экспериментальные проекты "искусственного интеллекта" (над созданием приложений для "облачных" технологий работают 5,4 млн. специалистов, а над созданием технологий обработки больших баз данных и продвинутой аналитики 6 миллионов[26].

Особенностью научно-технического развития США является то, что **секретная по своей сути технология – выявление подсознательных политических предпочтений на уровне конкретных избирателей – создана в коммерческой сфере.**

Для того, чтобы государство получило возможность регулировать использование той или иной коммерческой технологии, её надо засекретить. По мнению сенаторши Д.Фейнстейн (*Dianne Feinstein*), вице-председателя Сенатского комитета по разведке, сейчас эта система сломана[27]. Видимо, для начала должны получить политическую оценку угрозы распространения такой технологии, в том числе экспорта, причём потенциальные угрозы должны учитывать не только внешнеполитические, но также технические и социальные тенденции и факторы!

Как уже отмечалось выше, для победы команде Трампа надо было построить надёжные сценарные прогнозы поведения избирателей, соответствующие потенциальным тенденциям развития интернета и цифровых технологий в целом. Такая сложнейшая задача нашла своевременное решение. Уже 18 ноября 2016 г. в Вашингтоне были обнародованы рекомендации, изложенные в ранее подготовленном и уже упоминавшемся документе "Будущее кибербезопасности 2020".

Разработанные сценарии – это некие эвристические конструкции-прогнозы, опирающиеся на три базисных гипотезы:

1. Развитие современной экономики нельзя объяснить только "технологией", человеческим поведением, государственным регулированием или какой-то бизнес-моделью, – воздействие всех этих значимых факторов наслаивается друг на друга.

---

[26] Columbus Louis . 2016 Big Data, Advanced Analytics & Cloud Developer Update. Available at: http://www.forbes.com/sites/louiscolumbus/2016/10/16/2016-big-data-advanced-analytics-cloud-developer-update-5-4m-developers-now-building-cloud-apps/#2228ad4368f4 (accessed 20.12.2016).

[27] Feinstein Dianne. How to rethink what's 'top secret' for the Internet age. Available at: https://www.washingtonpost.com/opinions/how-to-rethink-whats-top-secret-for-the-internet-age/2016/12/16/57835e0e-bccd-11e6-94ac3d324840106c_story.html?utm_term=.5f5cd9aa60be&wpisrc=nl_headlines&wpmm=1 (accessed 20.12.2016).

2. Быстрое изменение социально-экономических условий, как правило, обусловлено непредвиденными сдвигами в структуре, казалось бы, несвязанных между движущих факторов, которые сопряжены с динамикой ситуации в совершенно различных сферах, – охране здоровья, на рынках, в нормах социального поведения, и прочих.

3. Новые важные стратегии разрабатываются независимо от созданных ранее моделей; в них внимание акцентируется на том, как будущее может отличаться от настоящего существенными, хотя, вероятно, и нежизнеспособными (в долгосрочном аспекте) формами.

Сценарный подход включает ряд новых вопросов глобальной безопасности, возникших на пересечении технических и социальных аспектов развития информационно-коммуникационных технологий. В рамках такого подхода кибератаки на компьютерные устройства (и/или сети таких устройств) и, соответственно, их защита, представляют собой только часть проблемы.

Прогноз информационной безопасности к концу полномочий администрации Трампа

Уже в недалёком будущем само понятие "кибербезопасности" в очень существенной степени будет зависеть от выбора той или иной стратегии технического, социального и политического развития международной обстановки.

По этой причине авторы упомянутых выше сценариев полагают, что круг такого рода исследований в области кибербезопасности уже очень скоро значительно расширится, а потому так важно попытаться заранее обозначить новые существенные факторы (и угрозы!), тесно связанные с этим понятием.

В сложившейся ситуации Америке жизненно необходим новый, причём тщательно регулируемый поток лжи и дезинформации.

Будет очень печально, если американское руководство (как на интернет-бирже!) не сможет успевать контролировать поток соответствующих инноваций и своевременно предотвращать использование лжи во вред интересам страны.

Надо научиться своевременно и надёжно (быстро и точно) отличать ложь от правды в онлайновых социальных сетях (например, встраивая в информационный трафик автоматизированные программы типа "детектор лжи"). Это трудно, но такого рода программы уже разрабатываются[28].

Логично поставить вопрос, а какие проблемы кибербезопасности могут стать актуальными в конце полномочий администрации президента Трампа, скажем, в 2020 г. в ходе следующих президентских выборов? Это могут быть не только физическая и противовирусная защита всех стационарных и мобильных компьютеров, используемых в системах голосования и подсчёта голосов, но также и своевременное распознавание и дискредитация дезинформации, предотвращение её возможных тяжёлых последствий (например, разо-

[28] Newton Casey . Facebook is patenting a tool that could help automate removal of fake news. Available at: http://www.theverge.com/2016/12/7/13868650/facebook-fake-news-patent-tool-machine-learning-content (accessed 20.12.2016).

блачение параноидальных подозрений или наоборот, недооценка потенциала террористов).

Часть ответов на эти вопросы содержится в сценариях, разработанных группой междисциплинарных экспертов ЦДКБ. В подобном сценарии на основе будущих возможностей развития "взаимосвязей между человеком и технологиями" допускается модификация самого понятия "безопасности". Например, так: "безопасность – это такое состояние, когда человек должен точно знать, что рядом с ним нет ни одного человека, таящего преступные намерения".

Как известно, разработка различных стратегий обеспечения безопасности обычно опирается на сценарии потенциальных угроз, сформулированных в военно-политических доктринах. Однако в XXI веке многие серьёзные угрозы могут носить неявный характер и упоминаться доктринах только косвенно.

Уже в ближайшем будущем большинство людей и "вещей" будут соединены цифровыми сетями, а понятие "кибер" станет всеобщим. Соответственно, расширится содержание термина "безопасность", которое тоже надо будет переосмыслить (подобно расширению понятия "национальная безопасность", произошедшему после окончания "холодной войны").

В одном из таких сценариев предполагается, что сетевые устройства смогут тщательно контролировать не только местонахождение, но и эмоциональное состояние человека. В этой связи, Ст. Уэбер и Б. Купер в заметке в популярном американском интернет-издании "Хаффингтон пост"[29] задаются вопросом, а что если в 2020 г. портативные устройства смогут в реальном времени контролировать эмоциональное состояние человека (уровень гормонов, ритм сердца, выражение лица, оттенки голоса и проч.)? Тогда интернет может стать мощной системой "эмоционального считывания" параметров человеческой психологии, затрагивающих самые интимные стороны. В этом случае термин "персональных данных" придётся распространить и на параметры эмоционального состояния человека.

А что если инновационные технологии позволят киберпреступникам контролировать ментальное, эмоциональное и психическое состояние не только отдельных людей (в том числе политических лидеров), но и влиять на так называемую "пассионарность" больших контингентов населения, целых народов? В этом случае само понятие угрозы и задачи обеспечения кибербезопасности национального государства может существенно измениться.

Литература

Бондаренко С.В. 2005. Политическая идентичность в киберпространстве // Политическая наука, № 3, с. 76–92.

References

Bondarenko S.V. 2005. Politicheskaya identichnost' v kiberprostranstve [Political identity in cyberspace] // Political science, № 3, p.76-92.

Goodman M. Future Crimes. New York, 2015.

[29] Weber Steven, Cooper Betsy. It's the year 2020...how's your cybersecurity? Available at: http://www.huffingtonpost.com/the-conversation-us/its-the-year-2020hows-you_b_9821264.html (accessed 20.12.2016).

2016 Presidential Elections: Triumph of Digital Democracy?

(USA ❖ Canada Journal, 2017, No. 4, p. 5-19).
Received: 9.01.2017.

ROGOVSKIY Yevgeniy Aleksandrovich, Institute for U.S. and Canadian Studies, Russian Academy of Sciences (ISKRAN), 2/3 Khlebny per., Moscow, 121069, Russian Federation (rogowsky@rambler.ru).

The application of information technologies in the 2016 U.S. President election campaign had a special character. The range of relevant applications went far beyond the traditional areas typical for the 2008 campaign. For the purposes of its election strategy each party ensured the support of powerful IT-corporations (Google – by Hillary Clinton, Facebook – by D. Trump) and applied different technologies: Google – its own search mechanism (SEME); Facebook – the identification of subliminal political preferences at the level of the users of its social network. The study explains the effective victory of D. Trump and at the same time reveals a qualitatively new information security problems.

Keywords: *D. Trump, H. Clinton, 2016 elections, Google, Facebook, manipulations with the use of search engines.*

About the author:
ROGOVSKIY Yevgeniy Aleksandrovich, Candidate of Sciences (Economics), Head of the Center for Military-Industrial Policy Studies.