УДК 32.019.51

ПРОБЛЕМЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО МАНИПУЛИРОВАНИЯ В ПРОСТРАНСТВЕ СЕТИ FACEBOOK

А. В. Курилкин

Московский государственный университет имени М. В. Ломоносова

Поступила в реакцию 12 марта 2019 г.

Аннотация: *в статье рассматривается вопрос об использовании различных механизмов работы социальной сети Facebook для проведения информационно-психологических операций. Автор приходит к выводу, что в настоящее время в социальной сети Facebook представляется возможным четко выделять целевую аудиторию и воздействовать на нее различными инструментами информационно-психологических операций.*
Ключевые слова: *Facebook, информационно-психологическая операция, манипуляция.*

Abstract: *this paper examines the question about the use of various mechanism of Facebook for information and psychological operations. The author comes to the conclusion that at the present time in the social network Facebook it is possible to clearly identify the target audience and influence it with various information and psychological methods.*
Key words: *Facebook, information operation, psychological operation, manipulation.*

Непрекращающаяся с 2016 г. по настоящее время череда политических скандалов, связанная с социальной сетью Facebook, продемонстрировала ряд уязвимостей социальной сети и широкие возможности проведения информационно-психологических операций.

На сегодняшний день проблема манипулирования настроениями и предпочтениями пользователей в Интернете в целом и в Facebook в частности достаточно популярна в американских исследовательских кругах, но внимание западных исследователей приковано к проблеме борьбы в киберпространстве [1; 2], fake-news [3; 4] и хакерским атакам [5; 6]. В отечественной же политической науке данный вопрос исследуется в рамках более общей темы информационно-психологических операций [7; 8], информационно-психологического воздействия [9–12], предвыборной агитации [13], политической психологии [14], защиты от нежелательной информации в Интернете [15; 16].

В то же время вопросы информационно-психологического воздействия в самой массовой на сегодняшний день социальной сети мира и одной из самых популярных социальных сетей на постсоветском пространстве изучены недостаточно, особенно с учетом раскрывшейся в последнее время информации. При этом публикации зарубежных ученых на тему манипулирования пользователями социальных сетей зачастую политически ангажированы.

Автор данной статьи ставит перед собой несколько задач: изучить методы формирования информационного потока для конкретного пользователя и механизмы выделения целевой аудитории для проведения рекламной кампании; оценить роль преднамеренного размещения и продвижения поддельных информационных и пропагандистских сообщений для информационно-психологического воздействия на пользователей.

Утечки данных и выделение целевой аудитории информационно-психологической операции

За 15 лет существования в социальной сети Facebook зарегистрировалось более двух миллиардов пользователей, причем во многих западных странах эта соцсеть является самой популярной. По данным социологических опросов, для значительного числа американцев именно Facebook служит главным источником новостей.

Более того, изменения на рынке СМИ, произошедшие в результате стремительного развития Интернета и IT-технологий, заставили многие издания перейти в онлайн и социальные сети.

Вследствие этого изменился рынок рекламы, и для социальных сетей он стал основным источником заработка. Facebook, как и многие другие соцсети, поставляет данные сторонним компаниям для размещения рекламы [17].

Помимо этого, социальная сеть позволяет собирать данные и сторонним компаниям. Первым этой возможностью в политических целях воспользовался

предвыборный штаб тогда еще кандидата в президенты Барака Обамы в 2008 г.

Разработанное по заказу предвыборного штаба приложение для сторонников Обамы собирало личные данные как о собственных пользователях, так и об их друзьях в Facebook. При этом, как рассказала бывшая сотрудница предвыборного штаба Обамы [18], в 2008 г. скандала не случилось из-за того, что многие сотрудники соцсети поддерживали кандидатуру Обамы и по факту закрыли глаза на утечку данных.

В 2018 г. стало известно об утечке данных 87 миллионов человек [19; 20]. Сбор данных через различные развлекательные приложения организовала британская консалтинговая компания Cambridge Analytica для более точного размещения политической рекламы в поддержку кандидатуры Дональда Трампа в президентской гонке.

Аналогичные инструменты, по мнению ряда западных специалистов, использовались и во время агитационной кампании в Великобритании перед референдумом о выходе из Евросоюза и в ряде европейских стран в период выборов. Таким образом, на сегодняшний день, несмотря на попытки Facebook ограничить доступ к персональным данным, данные пользователей доступны для получения сторонними организациями.

Личные данные нужны были во всех случаях для более точного таргетирования и определения как политических предпочтений, так и интересов пользователя с целью продвижения определенных рекламных постов в его «ленте новостей». Стоит отметить, что Facebook разработал достаточно подробный механизм маркировки пользователей – каждому зарегистрировавшемуся в социальной сети присваивается как минимум 96 рекламных тегов [21]. При этом они необязательно носят коммерческий характер – летом 2018 г. стало известно [22], что поисковые алгоритмы соцсети отметили тегом «treason» (т. е. измена родине) профили 65 тысяч россиян. Впоследствии компания заявила, что данный тег удален, однако вопрос о причинах появления такой метки остался без ответа.

Широкие возможности рекламных механизмов Facebook, а также возможность получить личные данные пользователей значительно упрощают подготовку информационно-психологической операции, а также позволяют более эффективно размещать агитационные и пропагандистские материалы для воздействия на целевую аудиторию операции.

Отсутствие четкой верификации рекламодателей и зачастую отсутствие контроля за аномальным ростом подписчиков публичных страниц позволяет проводить операции под «чужим флагом» на просторах социальной сети. Ярким примером подобной операции является «Алабамский эксперимент» [23].

В 2017 г. американские СМИ сообщали, что кандидата от партии Республиканцев Роя Мура в социальных сетях продвигают аккаунты «российского происхождения». В итоге общественное мнение склонилось на сторону его соперника, кандидата от партии демократов, Дага Джонса.

Спустя год, в декабре 2018 г., стало известно, что никакие «русские тролли» кандидатуру республиканца не поддерживали, а продвигающие Роя Мура аккаунты были созданы в рамках секретного эксперимента Twitter и Facebook. Свои извинения принес и финансировавший работу New Knowledge миллиардер Рид Хоффман.

Как объяснили в Facebook, эксперимент проводился с целью сбора эмпирических данных для анализа якобы имевшего места вмешательства Российской Федерации в президентские выборы в США. Однако по факту компания самостоятельно вмешалась в предвыборный процесс и использовала механизмы «черного пиара» для воздействия на избирателей.

Спустя несколько месяцев после завершения выборов и поражения Мура представители социальной сети заявили, что особого влияния на избирательный процесс эксперимент не оказал, но признали, что компания провела «операцию под чужим флагом» – один из классических элементов информационно-психологической войны.

Действия модераторов социальной сети в отношении материалов СМИ также можно назвать ангажированными – в частности, в разгар скандала с «fake-news» и якобы имевшего место вмешательства России в президентские выборы в США руководство социальной сети попыталось составить список «достоверных» и «качественных» СМИ, но в итоге подверглось критике за выбор изданий преимущественно левой идеологии и игнорирование изданий правого политического толка. При этом в отношении ряда СМИ руководство социальной сети занимает жесткую позицию и удаляет все аккаунты, связанные с работой средств массовой информации – в частности, подобной цензуре подверглись страницы российского информационного агентства Sputnik, американского ресурса InfoWars и украинского журналиста и блогера Анатолия Шария.

Важным фактом является и то, что сам механизм формирования ленты новостей пользователя приводит к возникновению «эхо-камеры» [24] и, в конце концов, благодаря алгоритмам социальной сети, конкретный пользователь получает только информацию, соответствующую его точке зрения, и не может сформировать более-менее полноценную картину

происходящего и, следовательно, укореняется в навязанных ему однажды взглядах и установках.

В итоге легкодоступность личных данных пользователей вкупе с развитым механизмом таргетирования пользователей, как показал опыт избирательных кампаний в США, позволяет создавать и продвигать для целевых групп информационно-психологической операции необходимые материалы. Важным при этом является тот факт, что, однажды «лайкнув» подобный материал, пользователь будет в дальнейшем получать аналогичный контент благодаря алгоритму формирования ленты новостей и, таким образом, укореняться в навязываемой ему позиции. При этом, как показывает опыт «Алабамского эксперимента», преднамеренное искажение информации позволяет создавать информационные поводы для публикаций в СМИ, которые потом, в связи с активной SMM-политикой современных СМИ, размещаются на пространстве социальной сети.

В целом же, политическая предвзятость руководства социальной сети, легкодоступность личных данных пользователей и широкие возможности проведения политических рекламных кампаний и продвижения нужной информации в социальной сети, а также развитой механизм таргетирования пользователей приводят к тому, что пространство социальной сети легко может использоваться и используется для проведения информационно-психологических операций.

ЛИТЕРАТУРА

1. World War Web / ed. G. Rose // Foreign Affairs. – 2018. – № 97.

2. The future of war / ed. J. Tepperman // Foreign Policy. – 2018. – № 4.

3. *Vosoughi S.* The spread of true and false news online / Soroush Vosoughi, Deb Roy, Sinan Aral // Science. – 2018. – № 359.

4. *Kornbluh K.* The Internet's Lost Promise / K. Kornbluh // Foreign Affairs. – 2018. – № 97.

5. *Buchanan B.* The Cybersecurity Dilemma : Hacking, Trust, and Fear Between Nations / B. Buchanan. – Oxford University Press, 2017.

6. *Clark R. A.* Cyberwar. The Next Threat to National Security and What to Do About It / R. A. Clark, R. K. Knake. – Ecco, 2013.

7. *Манойло А. В.* Основы теории современных информационных войн / А. В. Манойло // Информационные войны. – 2017. – № 4 (19).

8. *Павлова М. П.* Социальные медиа и сети – новые инструменты для террористических организаций / М. П. Павлова // Информационные войны. – 2017. – № 4 (19).

9. *Володенков С. В.* Интернет-технологии как инструмент воздействия на современные национальные политические режимы / С. В. Володенков // Дискурс-Пи. – 2017. – Вып. 28, № 3.

10. *Володенков С. В.* Интернет-технологии как современный инструмент виртуализации массовой политической реальности / С. В. Володенков // Вестник Московского университета. Сер. 12: Политические науки (ранее: Теория научного коммунизма; Социально-политические исследования). – 2017. – № 2.

11. *Володенков С. В.* Потенциал и особенности технологий интернет-пропаганды в современном политическом управлении / С. В. Володенков // Информационные войны. – 2017. – № 2 (42).

12. *Ромашкина Н. П.* Социальные сети : новые возможности или угрозы? / Н. П. Ромашкина // Информационные войны. – 2017. – № 3 (43).

13. *Роговский Е.* Выборы США : успех технологических инноваций / Е. Роговский // Международная жизнь. – 2017. – № 3.

14. *Евгеньев Т. В.* Психологические особенности формирования оппозиционной повестки в сети Интернет / Т. В. Евгеньев, В. А. Губченко // Политическая наука. – 2017. – Спецвыпуск.

15. *Тумбинская М. В.* Системный подход к обеспечению защиты от нежелательной информации в социальных сетях / М. В. Тумбинская // Вопросы кибербезопасности. – 2017. – № 2 (20).

16. *Чесноков В. О.* Применение алгоритма выделения сообществ в информационном противоборстве в социальных сетях / В. О. Чесноков // Вопросы кибербезопасности. – 2017. – № 1 (19).

17. *Dance G. J. X.* As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants / G. J. X. Dance, M. LaForgia, N. Confessore // The New York Times. – Mode of access: https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html

18. *Davidsen C.* Personal twitter account / C. Davidsen // Twitter. – Mode of access: https://twitter.com/cld276/status/975568130117459975

19. *Хабибрахимов А.* Facebook сообщила об утечке данных 87 млн пользователей в скандале с Cambridge Analytica / А. Хабибрахимов // VC.RU. – Режим доступа: https://vc.ru/flood/35815-facebook-soobshchila-ob-utechke-dannyh-87-mln-polzovateley-v-skandale-s-cambridge-analytica

20. *Грассегер Х.* Как Big Data и пара ученых обеспечили победу Трампу и Brexit / Х. Грассегер, М. Крогерус ; пер. The Insider. – Режим доступа: https://theins.ru/politika/38490

21. *Devey C.* 98 personal data points that Facebook uses to target ads to you / C. Devey // The Washington Post. – Mode of access: https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/?noredirect=on&utm_term=.b08ea5abfba5

22. Facebook labels Russian users as ‘interested in treason’ // The Guardian. – Mode of access: https://www.the-

guardian.com/technology/2018/jul/11/facebook-labels-russian-users-as-interested-in-treason

23. *Shane S.* Secret Experiment in Alabama Senate Race Imitated Russian Tactics / S. Shane, A. Blinder // The New York Times. – Mode of access: https://www.nytimes.com/2018/12/19/us/alabama-senate-roy-jones-russia.html

24. *Поцелуев С. П.* О факторах политической радикализации в сетевой коммуникации посредством «Эхокамер» / С. П. Поцелуев, Т. А. Подшибякина // Научная мысль Кавказа. – 2018. – № 2.

Московский государственный университет имени М. В. Ломоносова

Курилкин А. В., выпускник аспирантуры факультета государственного управления

E-mail: anton.kurilkin@gmail.com

Moscow State University named after M. V. Lomonosov

Kurilkin A. V., Post-graduate Student of the School of Public Administration

E-mail: anton.kurilkin@gmail.com