

ПРОБЛЕМЫ И ОПАСНОСТИ ПУБЛИЧНОГО ОБЩЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ

Сотников А.А., Артюшина Е.А.¹

¹ ФГБОУ ВО «Пензенский государственный технологический университет», Пенза
e-mail: eart@penzgtu.ru

В настоящей работе рассматриваются главные проблемы и потенциальные опасности, которые можно выявить в процессе коммуникации пользователей социальных сетей. Под социальной сетью понимается веб-сайт или онлайн-сервис, предназначенный для поддержания социальных взаимоотношений в виртуальной форме при помощи Интернета. Оказываемое влияние, стремительный рост популярности и открытый доступ к контенту привлекли к социальным сетям внимание правительств, финансовых организаций и исследователей. Анализ и обработка полученных из сетей данных помогает исследователям усовершенствовать знания об информационных потоках, а результаты такого анализа имеют немаловажное прикладное значение. Также в данной статье излагается суть существующих на текущий момент основных видов сетевых манипуляций. К ним относятся: распространение недостоверной общественно значимой информации, коммерческое использование социальных профилей пользователей сети без их ведома и согласия, сбор компрометирующих материалов владельцами платформ с долгосрочными неблагоприятными целями, неявное склонение детей и подростков к вступлению в сообщества с крайне опасным контентом. В качестве меры предотвращения подобного рода сетевых манипуляций в статье поддерживается идея обеспечения безопасного Интернета и защита пользователя социальных сетей от потенциально вредного контента на системном уровне.

Ключевые слова: социальные сети, анализ социальных профилей, опасный контент, защита от сетевых манипуляций, безопасный Интернет

PROBLEMS AND DANGERS OF PUBLIC COMMUNICATION IN SOCIAL NETWORKS

Sotnikov A.A., Artyushina E.A.¹

¹ Penza State Technological University, Penza
e-mail: eart@penzgtu.ru

This paper discusses the main problems and potential dangers that can be identified in the process of communication between users of social networks. A social network is a web site or online service designed to maintain social relationships in a virtual form using the Internet. The influence, the rapid growth of popularity and open access to content attracted the attention of governments, financial organizations and researchers to social networks. Analysis and processing of data obtained from networks helps researchers improve their knowledge of information flows, and the results of such analysis are of no small practical value. Also, this article outlines the essence of the currently existing main types of network manipulation. These include: the dissemination of untrue socially significant information, the commercial use of social profiles of network users without their knowledge and consent, the collection of incriminating materials by platform owners with long-term unseemly goals, the implicit inducement of children and adolescents to join communities with extremely dangerous content. As a measure to prevent this kind of network manipulation, the article supports the idea of providing a secure Internet and protecting a user of social networks from potentially harmful content at the system level.

Keywords: social networks, analysis of social profiles, dangerous content, protection against network manipulations, secure Internet

Введение. Социальные сети уверенно вошли в современную жизнь и занимают в ней значимую часть, активно воздействуя на поведение, предубеждения, ценности и намерения своих пользователей. Оказываемое влияние, стремительный рост популярности и открытый доступ к контенту привлекли к социальным сетям внимание правительств, финансовых организаций и исследователей. Оперативный анализ и обработка полученных из сетей данных помогает исследователям усовершенствовать знания об информационных потоках, о

формировании и распространении мнений, о связи ценностей и предубеждений пользователя и генерируемого им контента.

Цель исследования. В настоящей работе рассматриваются главные проблемы и потенциальные опасности, которые можно выявить в процессе взаимодействия пользователей социальных сетей. Предпринимается попытка исследования социальных сетей как популярного средства коммуникации и обмена информацией, имеющего свою специфику использования.

В частности, контент конкретного пользователя в новостных лентах социальных сетей достаточно быстро «тонет» и теряет свою актуальность. Так, в сети Facebook обсуждение публикации по среднему информационному поводу продолжается около 5–6 часов, получая за столь краткое время до 95% всей возможной реакции целевой аудитории. При этом поиск по своим собственным текстам для пользователя Facebook сильно затруднен.

В сети Вконтакте участники имеют некоторые возможности для отслеживания собственных действий с помощью отметок «понравилось», «поделиться», комментариев, обновлений и т.п., но полноценные средства поиска в ней также отсутствуют. Поэтому активные пользователи быстро теряют контроль над своим контентом, размещенным в сети всего лишь неделю или месяц назад. Безвозвратно «тонут» в лентах и чужие публикации.

Постоянно растущие объемы информационных потоков в социальных сетях создают широкие предпосылки для разного рода манипуляций. Так публикация и распространение заведомо недостоверной общественно значимой информации (фейки, вбросы) до последнего времени могли беспрепятственно повторяться с заданной периодичностью, в некоторых случаях намеренно усиливая напряженность в социуме [1,2,9].

Очевидно, что информация теряется лишь для активного пользователя сети, но не для соответствующей программной платформы. В социальных медиа любые публикации, отметки, приватные сообщения (в том числе – paste) неуничтожимы и могут храниться неопределенно долго.

Материал и методы исследования. При целенаправленном сборе и анализе сведений о пользователе социальной сети практикуемая система отметок формирует его психологический и социальный портрет, с высокой степенью точности определяет вкусы и личные предпочтения [3,4].

Наглядным примером может служить распределение основных типов профилей использования Интернет с учетом национального менталитета из таблицы 1, полученное на основании исследовательских данных.

Как отмечено в источнике [3], исследование проведено в рамках мирового исследовательского проекта «World Internet Project». Использовались данные

формализованного интервью в России (2013 г., N = 1600 чел., выборка репрезентативна по полу и возрасту) и Швеции (2012 г., N = 2743, выборка репрезентативна по полу и возрасту). Данные интервью обрабатывались с помощью SPSS for Windows 17.0 с применением одномерного, корреляционного, кластерного анализа (методом К-средних).

Таблица 1 – Распределение кластеров – профилей Интернет-пользователей в России и Швеции за 2014 г., в %

<i>Тип профиля пользователя</i>	<i>Россия</i>	<i>Швеция</i>
Человек информационный	5,9	12,8
Человек развлекающийся	33,4	8,8
Человек прагматичный	4,4	49,5
Человек традиционный	23,9	16,4
Человек не информационный	32,4	12,5
	100	100

Оперативный анализ социальных профилей пользователей сети, например, с помощью коммерческих пакетов типа Social Engagement, создает значительные конкурентные преимущества для всех заинтересованных лиц.

Результаты исследования и их обсуждение. Результаты оперативного анализа социальных профилей пользователей социальной сети в первую очередь используются в интернет-маркетинге для доставки адресной рекламы. Современные маркетинговые системы, активно обмениваясь социальными профилями, способны формировать соответствующие рекламные блоки не только по лингвистическому портрету пользователя от поисковых систем, но также на основе потоковых данных от мультимедийных устройств ввода/вывода. Конечная цель для всех видов интернет-маркетинга совпадает и состоит в увеличении коэффициента конверсии. Хотя при показе рекламных материалов сотнями миллионов копий % покупок и остается небольшим, тем не менее, за счет огромных объемов доставки адресная реклама остается весьма прибыльным занятием [5].

Кроме популярных отечественных платформ (Вконтакте, Одноклассники), крупные национальные сети созданы и функционируют также в Китае (Renren Network, Qzone, Sina Weibo), в Бразилии (Orkut) и Японии (Mixi). Таким образом, сегодня владельцами абсолютного большинства социальных платформ (Facebook, Twitter, Instagram, видеохостинга Youtube и др.) являются США. Как отмечается в источнике [6], в соответствии с Патриотическим актом от 2001 г. большинство Web-сервисов продолжает передавать собранные данные Агентству национальной безопасности без постановления суда, в открытом

и нешифрованном виде.

Сбор сведений о пользователях Интернет может осуществляться неявными способами, например, в процессе их авторизации на Web-сайтах с помощью ресурсов социальной сети, например: аккаунтов Facebook, Twitter, кнопок для организации ссылок на Web-страницы и пр. В таком случае для соответствующей социальной платформы оказывается доступен трафик и траектории посетителей сайтов, в том числе – незарегистрированных, которых на текущий момент сама платформа идентифицировать неспособна.

С учетом охвата аудитории (≈ 10 млн. российских пользователей платформ Facebook, Google, Twitter), при целенаправленном узком анализе публикаций может быть достигнут значительный результат. Средствами мониторинга в таком случае могут являться бесплатные сервисы для оценки посещаемости сайтов Google Analytics, Яндекс.Метрика; специальные возможности поисковых систем, а также авторизация пользователей на Web-сайтах через соответствующие аккаунты.

Таким образом, о пользователе социальной сети может быть собрана компрометирующая его негативная информация, например, об употреблении ПАВ, промискуитете и др. В тоже время – позитивный контент, не относящийся к категории развлечений, как правило, не слишком востребован. Компрометирующие материалы могут быть задействованы и через длительный период времени, в подходящей ситуации, например, когда пользователь займет ключевой пост в крупной компании, государственной организации, станет журналистом СМИ и т.д. По аналогии с интернет-маркетингом, если % конверсии окажется высоким и компромат будет найден хотя бы на 1-го из 1000 пользователей сети, возникнут оптимальные условия для создания «точки влияния». В масштабах целой страны достаточно создать нескольких тысяч таких точек, чтобы существенно влиять на принятие стратегически невыгодных для государства решений. Как видно, именно этот процесс с достаточной долей вероятности и происходит сегодня в странах ЕЭС [5,7].

Социальные сети в настоящее время широко используются не только для публикаций, но и для общения с родственниками и друзьями. Рядовой пользователь сети далеко не всегда осознает, что процесс общения является публичным и содержимое его персональной страницы или микроблога доступно не только узкому кругу друзей или подписчикам, но и всей глобальной сети, в том числе – соответствующим системам мониторинга.

В зависимости от уровня социального интеллекта пользователь способен поддерживать в сети от 10 до 30 «сильных связей» – полноценных дружеских или родственных контактов, а также иметь множество «слабых связей» для нерегулярного и, обычно, виртуального взаимодействия. В целом, социальные сети часто создают для своего пользователя иллюзию дружеского общения, подменяя «сильные» связи большим количеством «слабых». Именно

такой стиль общения характерен для нового поколения.

По результатам исследований MediaScore, приведенных в таблицах 2, 3 легко определить предпочтения пользователей при выборе социальной сети с учетом их возраста.

Таблица 2 – Российская аудитория социальных сетей с учетом возрастной группы, февраль 2019 г., в % от населения

<i>Социальная сеть</i>	<i>Возрастная группа</i>		
	<i>I 12-24</i>	<i>II 25-34</i>	<i>III 35-64</i>
ВКонтакте	92	86	59
Instagram	73	66	47
Facebook	36	43	46
Одноклассники	34	47	44
Snapchat	9	4	2
TikTok	9	3	2
Мой мир	7	6	12
Google+	4	3	6

Таблица 3 – Среднее время в сети с учетом возрастной группы пользователей Рунета, март 2019 г., в минутах за день

<i>Возрастная группа</i>	<i>Среднее время в сети</i>
<i>I (12-24)</i>	194
<i>II (25-34)</i>	185
<i>III (35-64)</i>	178

Также интересными представляются результаты исследований на базе платформы Brand Analytics, приведенные ниже на рисунке 1. Платформа анализирует активность пользователей в социальных сетях, причем сообщением в исследованиях называется любой открытый пост или комментарий. Вовлеченность пользователя оценивается как сумма комментариев, отметок «понравилось» и «поделиться». Автором считается пользователь, оставивший хотя бы одно сообщение за месяц.

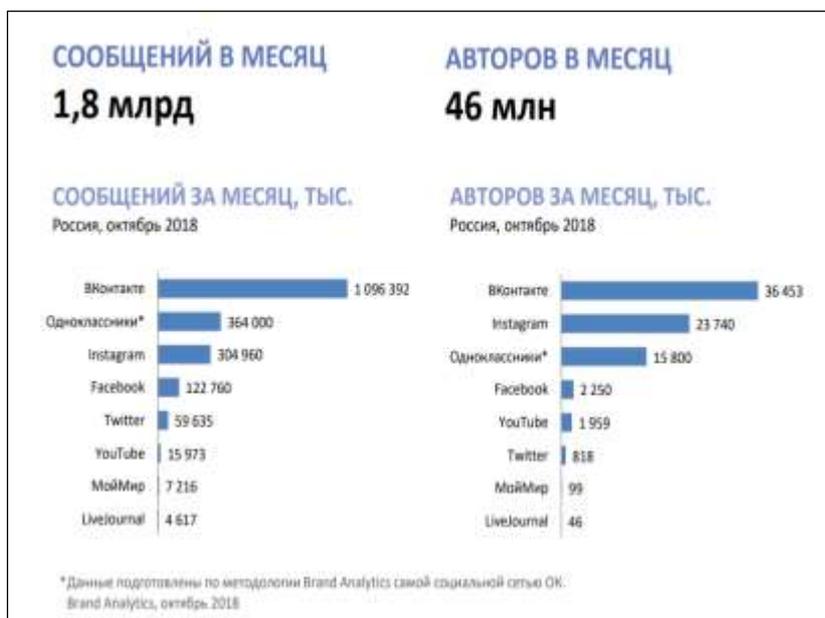


Рисунок 1 – Объемы информационных потоков в социальных медиа Рунета

Как следует из вышеприведенных данных, особенно рискованным становится бесконтрольный доступ к социальным сетям для современных детей и подростков. Такие стандартные возрастные проблемы, как неумение общаться на конкретные темы, трудности в восприятии юмора и сарказма без соответствующих подсказок (эмодзи, стикеры), постоянный поиск развлечений с целью избавления от скуки иногда приводят несовершеннолетних к вступлению в сообщества с крайне опасным контентом, такие как «группы смерти», «колумбайн-сообщества» и т.п.

К интеллектуальным особенностям поколения «большого пальца» (i-finger) уже традиционно относят: выносные знания – оперативная проверка всей получаемой информации через поисковые системы типа Google, Яндекс; слишком короткое «окно» внимания, преимущественная работа кратковременной памяти; потребление максимально гранулированного контента в виде коротких сообщений и ограниченного по объему медиа; мультизадачность в процессе потребления информации из сети, низкий уровень концентрации при решении конкретных задач [7,8].

В этой связи одной из серьезных опасностей, угрожающей поколению подростков с таким новым «клиповым» типом мышления, является малая устойчивость к манипуляциям, открывающая широкие возможности для внешнего управления.

Выводы и заключение. Как показывает практика, всевозможные настройки, фильтры и прочие средства родительского контроля для обеспечения безопасного Интернета применяют лишь 1-2% взрослых пользователей сети. Остальные либо не имеют достаточных знаний для этого, либо элементарно пренебрегают доступными способами защиты своих детей от потенциально вредного контента.

Поскольку иммунитет против сетевых манипуляций у детей и подростков чаще всего отсутствует, особенно актуальной становится проблема обеспечения безопасного общения в соцсетях, а также защита от опасного контента на системном уровне [9].

Список литературы

1 Распопова С.С., Богдан Е.Н. Фейковые новости: учебное пособие для вузов. Издательство: Аспект Пресс. – 2018. – 112 с.

2 Что такое фейковые новости и как за них будут наказывать? //Новости сайта Государственной Думы федерального собрания РФ от 7 марта 2019 г. URL: <http://duma.gov.ru/news/29982/> (дата обращения: 04.02.2020).

3 Бродовская Е.В., Домбровская А.Ю. Профили пользователей интернета и национальный менталитет в России и Швеции: результаты сравнительного кластерного анализа // Фундаментальные исследования. – 2014. – № 11-3. – С. 661-664; URL: <http://fundamental-research.ru/ru/article/view?id=35580> (дата обращения: 04.02.2020).

4 Мартышкин А.И., Сальников И.И., Пашенко Д.В. Этапы сбора и представления больших данных для построения социального профиля человека // Известия Тульского государственного университета. – 2018. – № 9. – С. 617-628; URL: <https://elibrary.ru/item.asp?id=36394798> (дата обращения: 04.02.2020)

5 Ашманов И.С. Оптимизация и продвижение в поисковых системах / 4-е издание – Издательство: «Прогресс книга», Серия «IT для бизнеса» – 2019. 512 с.

6 Романовская О.В. Акт о свободе: Ограничения прав человека в США в целях противодействия терроризму // Электронный научный журнал «Наука. Общество. Государство» 2017.– Т.5 №3(19); URL: <https://esj.pnzgu.ru/page/39536> (дата обращения: 04.02.2020)

7 Ашманов И.С. Мастер-класс: Социальные сети – оружие информационной войны. [Электронный ресурс] Высшая школа современных социальных наук (факультет) МГУ им. М. В. Ломоносова URL:

<http://vshssn.msu.ru/%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D0%B0%D1%8%D0%BB%D0%B5%D0%BA%D1%86%D0%B8%D1%8F%D1%81%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5-%D1%81%D0%B5%D1%82%D0%B8-%D0%BE%D1%80%D1%83%D0%B6/>

(дата обращения 06.03.2020)

8 Сотов М. Поколение большого пальца – образование [Электронный ресурс] // Российская газета № 3733 от 31 марта 2005 г. URL: <https://rg.ru/2005/03/31/literatura.html> (дата обращения 04.02.2020)

9 Роскомнадзор ограничит доступ к ресурсам, распространяющим фейк-ньюс о коронавирусной инфекции в России. [Электронный ресурс] // Новости сайта Федеральной службы по надзору в сфере связи информационных технологий и массовых коммуникаций (Роскомнадзор) от 4 марта 2020 г. URL: <https://rkn.gov.ru/news/rsoc/news72182.htm> (дата обращения 06.03.2020)