МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

ФАКУЛЬТЕТ ПОЛИТОЛОГИИ

Кафедра российской политики

На правах рукописи

Есиев Эльдар Таймуразович

Роль виртуальных технологий конфликтной мобилизации в противодействии политическому протесту

Специальность 5.5.2. Политические институты, процессы, технологии

Диссертация на соискание ученой степени
кандидата политических наук

Научный руководитель
доктор политических наук, с.н.с.
Манойло Андрей Викторович

Москва – 2023

Оглавление

Введение

Актуальность темы исследования определяется следующими факторами.

Во-первых, феномен конфликтной мобилизации в социальных сетях, встречающийся во внутриполитических конфликтах власти и общества – явление, подвергающее опасности целостность и суверенитет современных государств. Он определен в качестве угрозы национальной безопасности Доктриной информационной безопасности Российской Федерации (от 05.12.2016 г., п. 12)[1] как инструмент оказания информационно-психологического давления, направленного на дестабилизацию внутриполитической ситуации в России. Это означает, что государство видит необходимость бороться с этим явлением и технологиями, которые используются в ходе его реализации.

Во-вторых, эволюция технологий конфликтной мобилизации в социальных сетях привела к появлению новых подходов к противодействию данному феномену. Они уже применяются различными государствами, однако многие исследователи ставят вопрос об их эффективности. Это заставляет экспертное сообщество продолжать поиск наиболее рационального метода противодействия технологиям конфликтной мобилизации в Интернете.

В-третьих, современные обстоятельства продолжающейся гибридной войны против Российской Федерации со стороны ряда государств

[1] Указ Президента Российской Федерации от 5 декабря 2016 № №646 «Доктрина информационной безопасности Российской Федерации» // Российская газета URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 03.03.2022).

предполагают увеличение интенсивности применения виртуальных технологий конфликтной мобилизации с целью дестабилизации политической ситуации в России. В таких условиях изучение методов противодействия этим технологиям является ключевой задачей для обеспечения суверенитета государства.

Феномен политической мобилизации граждан может иметь и благоприятное воздействие на общественно-политическую жизнь. В том числе он позволяет проводить акции в поддержку общественных инициатив, способствующих развитию государства. Однако механизмы и инструменты этого феномена зачастую используются в антигосударственных целях, несут в себе задачу дестабилизации политической системы государства и требуют значительных усилий по противодействию им. В работе рассматривается феномен конфликтной мобилизации в кризисах, вызванных внешним влиянием для достижения политических интересов третьих стран или внутригосударственных сил. При этом исследование не затрагивает иных форм политического активизма, вызванных исключительно эндогенными факторами.

Степень научной разработанности темы исследования.

При исследовании феномена конфликтной мобилизации в социальных сетях было использовано значительное количество публикаций, выступлений, научных работ – как отечественных, так и зарубежных авторов. В целом, их следует разделить на шесть основных групп.

К **первой группе** относятся работы, посвященные феномену политической мобилизации. Авторы работ данной группы предлагают свои подходы к осмыслению этого феномена и оценки его роли в политическом процессе. Основными источниками информации в данном случае стали труды Гончарова Д.В., Мельвиля А.Ю., Лебона Г., Самсоновой Т.Н., Гурылиной М.В, Кремень Т.В.[2]. В этих работах представлены виды и формы

[2] Гончаров Д.В. Политическая мобилизация // Полис. Политические исследования. - 1995. - №6. - С. 129-137.; Политология: учеб. / А. Ю. Мельвиль [и др.]. - М.: Московский государственный институт

политической мобилизации, а также продемонстрированы примеры практического применения этого явления. Часть авторов данной группы отмечают, что термин «политическая мобилизация» не несет в себе какой-либо оценочной коннотации, а само явление должно исследоваться, как инструмент политического процесса.

Один из наиболее ярких примеров применения на практике феномена политической мобилизации связан с реализацией сценариев гибридной войны. Роль и место изучаемого первой группой авторов феномена в разрезе гибридного противостояния была изучена: Якуниным В.И., Цыганковым П.А., Слуцким Л.Э., Манойло А.В., Багдасаряном В.Э. и другими авторами[3].

Ко **второй группе** относятся работы, авторы которых анализируют виртуальные технологии конфликтной мобилизации. Данная группа делится на те труды, которые демонстрируют эффективность конфликтной мобилизации в социальных сетях, и на те, авторы которых скептически относятся к возможностям данного феномена. К первой подгруппе относятся работы Ушкина С.Г., Докуки С. В., Полата Р.К., Кана Р., Келнера Д., Джоста Дж., Барбера П., Бонно Р., Лангера М., Манойло А.В., Федорченко С.Н., Тастенова А., Устименко А.В., Априянца К.В.[4]. Ко второй подгруппе относятся работы Наима М., Баумана З., Морозова Е[5].

международных отношений (Университет) МИД России, ТК Велби, Изд-во Проспект, 2008. - 618 с.; Лебон Г. Психология народов и масс / Пер. с фр.; М.: ТЕРРА-Книжный клуб, 2008. - 272 с.; Самсонова Т.Н., Гурылина М.В. Основные тенденции политической мобилизации и политического участия граждан в современном российском обществе // Известия Тульского государственного университета. - 2016. - №4. - С. 41-46.; Кремень Т.В. Политическая мобилизация: объекты и субъекты // Историческая и социально-образовательная мысль. - 2013. - №5. - С. 146-149.

[3] Якунин В. И. Идеологические клише и мифы как инструмент внешней политики США // Российский журнал правовых исследований. - 2018. - №1(14) . - С. 9-19.; Цыганков П.А., Слуцкий Л.Э. Западный дискурс о «гибридной войне России против демократии»: новое вино в ветхие мехи // Вопросы политологии. - 2022. - №12 (88). - С. 4227-4238.; Манойло А.В. Информационная война в контексте специальной военной операции на Украине // Международная жизнь. - 2022. - №12 . - С. 74-83.; Багдасарян В. Э. Когнитивные матрицы манипулятивных технологий в войнах и революциях нового типа // Вестник МГОУ. Серия: История и политические науки. - 2020. - №1. - С. 8-23.

[4] Ушкин С.Г. Теоретико-методологические подходы к изучению сетевой протестной активности: от «умной толпы» к «слактивизму» // Мониторинг общественного мнения: экономические и социальные перемены. - 2015. - №3. - С. 3-11.; Докука С. В. Практики использования онлайновых социальных сетей // Социологические исследования. - 2014. - №1. - С. 137-145.; Polat, R. K. The Internet and Political Participation: Exploring the Explanatory Links // European Journal of Communication. - 2005. - № 20(4); Kahn, R., Kellner D. Oppositional Politics and the Internet: A Critical // Reconstructive Approach. Cultural Politics. - 2005. - № 1.; Jost, J. T., Barberá, P., Bonneau, R., Langer, M., Metzger, M., Nagler, J.Tucker, J. A. How Social Media Facilitates Political Protest: Information, Motivation, and Social Networks // Political Psychology. - 2018. - № 39; Манойло

Информацию об угрозах конфликтной мобилизации в социальных сетях можно найти у авторов **третьей группы работ**: Гончарова А.И., Хохлова А.А., Сивоволов Д.Л., Априянц К.В., Хабекирова З.С., Филатова О.Г., Рыдченко К.Д., Бугаев Д.В., Анисимов В.П., Смирнов Д.Н., Синельниковой Л.Н.[6]

Четвертую группу представляют собой работы, посвященные вопросам противодействия виртуальным технологиям конфликтной мобилизации. В рамках данной группы упоминаются следующие авторы: Бубнов А.Ю., Гаврилов С.Д., Гасанова В.С., Ибрагимова Г.Р, Сунг В.К., Дуай А., Ершов Н.А., Логунова Л.Ю. и ряд иных исследователей[7]. Авторы продемонстрировали на реальных примерах, как применяются интернет-технологии конфликтной мобилизации, и как в каждом из случаев такого

А.В. Цветные революции и технологии демонтажа политических режимов // Мировая политика. - 2015. - №1. - С. 1-19.; Федорченко С. Н. Государство-цивилизация в цифровой ойкумене // Журнал политических исследований. - 2023. - Т. 7, № 1. - С. 3-26.; Тастенов А. Устименко А.В.; Априянц К.В. Твиттер-революции»: микроблоги как инструмент выражения протестных настроений гражданского общества // Вестник ВГУ. Серия: Филология. - 2014. - №1. - С. 118-121.

[5] Наим М. Конец власти. От залов заседаний до полей сражений, от церкви до государства: почему управлять сегодня нужно иначе. - Corpus, - 2016. - 512 с.; Способны ли Facebook и Twitter помочь распространению демократии и прав человека? // Русский журнал URL: http://russ.ru/Mirovaya-povestka/Sposobny-li-Facebook-i-Twitter-pomoch-rasprostraneniyu-demokratii-i-prav-cheloveka (дата обращения: 03.03.2022).; Morozov E. The Net Delusion: The Dark Side of Internet Freedom. // NY: PublicAffairs, 2012.;

[6] Гончарова А.И. Применение социальных сетей в целях дестабилизации политической ситуации государства // Инновации. Наука. Образование. - 2022. - №53.; Хохлова А.А Особенности динамики социально-политической дестабилизации монархий БВСА до и после «арабской весны» // Азия и Африка сегодня. - 2022. - №3. - С. 50-58.; Сивоволов Д.Л. Новые угрозы национальному суверенитету России в сфере информационной безопасности // РАНХиГС М.: Социум и власть. - 2015. - №6. - С. 82-88.; Тастенов А. Устименко А.В.; Априянц К.В. Твиттер-революции»: микроблоги как инструмент выражения протестных настроений гражданского общества // Вестник ВГУ. Серия: Филология. - 2014. - №1. - С. 118-121.; Хабекирова З.С. Стратегия дискредитации и приемы ее реализации в политическом дискурсе демократической оппозиции // Вестник Адыгейского государственного университета. Серия 2: Филология и искусствоведение. - 2011. - № 2.; Филатова О.Г. Интернет-технологии политической мобилизации в современной России // Политическая экспертиза: ПОЛИТЭКС. - 2014. - Т. 10, - №4. - С. 57-67.; Рыдченко К.Д. Интересы и угрозы безопасности России в информационно-психологической сфере // Пробелы в российском законодательстве. - 2009. - №4.; Бугаец Д.В., Анисимов В.П. Доктрина информационной безопасности РФ - основа противодействия угрозам безопасности России в информационной сфере // Россия в XXI веке: новые тенденции развития. Материалы Международной научно-практической студенческой конференции. - 2017.

[6] Смирнов Д.Н. Реализация средств делигитимации в ходе «оранжевой революции» // Научные ведомости Белгородского государственного университета. Серия: История. Политология. Экономика. Информатика. - 2008. - Т.7. - № 5.; Синельникова Л.Н. Информационная война Ad infinitum: украинский вектор // Политическая лингвистика. - 2014. - № 2 (48).; - С. 95-101.; Шатилов А.Б. «Диванные войска» как новая форма информационно-пропагандистского сопровождения политических и военных конфликтов в начале XXI века // Власть. - 2014. - № 7. - С. 56-58.

[7] Ибрагимова Г.Р. Стратегия КНР в области управления интернетом и обеспечения информационной безопасности // Индекс безопасности. - 2013. - № 1 (104), - Т. 19.; Kim S. W., Douai A. Google vs. China's «Great Firewall»: Ethical implications for free speech and sovereignty // Technology in Society. - 2012. - № 34.

применения было оказано противодействие со стороны государственных структур. Изучение подобных примеров позволяет составить перечень примененных методов защиты от виртуальных технологий конфликтной мобилизации и классифицировать их.

К пятой группе относятся диссертации и авторефераты, относящиеся к тематике политической мобилизации, виртуальных технологий конфликтной мобилизации, а также методам противодействия им. К этой группе следует отнести работы: Володенкова С.В., Докуки С.В., Смирнова Д.Н.[8]

Источниковая база исследования состоит из аналитических и информационных публикаций информагентств РИА «Новости», ТАСС, статей в популярных отечественных газетах («Российская газета», «Коммерсант», «Ведомости» и т.д.), а также ресурсов в сети Интернет.

Нормативную базу исследования составляют:

- нормативные правовые документы, связанные с регулированием интернет-пространства в Российской Федерации. В частности, Федеральный закон от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»[9], утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 Доктрина информационной безопасности Российской Федерации[10], а также Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации», Указ Президента Российской Федерации от 09.11.2022 № 809 «Об утверждении Основ государственной

[8] Володенков С.В. Технологии интернет-коммуникации в системе Современного политического управления: дис. д-р. полит. наук: 23.00.02. - Москва, 2015. - 441 с.; Докука С.В. Коммуникация в социальных онлайн-сетях как фактор протестной мобилизации в России: дис. канд. социол. наук: 22.00.04. - Москва, 2014. - 150 с.; Смирнов Д.Н. Манипулятивные технологии и их применение в условиях смены политического режима: опыт оранжевой революции на Украине: дис. канд. полит. наук: 23.00.02. - Нижний Новгород, 2009. - 352 с.

[9] Федеральный закон от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс»

[10] Указ Президента Российской Федерации от 5 декабря 2016 № №646 «Доктрина информационной безопасности Российской Федерации» // Российская газета URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 03.03.2022).

политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей»;

- нормативные правовые документы Соединенных штатов Америки в области регулирования интернет-пространства. В частности, стратегия кибербезопасности США - The White House «National cyber strategy of the United States of America»[11];

- нормативные правовые документы Китайской Народной Республики в области регулирования интернет-пространства, в частности, Закон о национальной безопасности КНР от 2015 года, Национальная стратегия безопасности киберпространства КНР от 27.12.2016 г[12], стратегия Китая «Глобальная инициатива по безопасности данных»[13].

Объект исследования – конфликтная мобилизация общества в интернет-пространстве, осуществляемая в целях политической дестабилизации современных государств.

Предмет исследования – формы, методы, технологии конфликтной мобилизации в интернет-пространстве, применяемые для вовлечения граждан в политическую протестную деятельность (на материалах США, КНР и России).

Цель исследования – определить основные способы и методы противодействия технологиям конфликтной мобилизации в интернет-пространстве.

Из данной постановки объекта, предмета и цели вытекают следующие **задачи исследования**:

- выявить особенности и основные этапы эволюции виртуальных технологий конфликтной мобилизации;

---

[11] The White House «National cyber strategy of the United States of America» from 09.2018 whitehouse.gov. – 2018.

[12] Закон Китайской Народной Республики «О кибербезопасности» - Текст: электронный // pkulaw.com: [сайт]. – URL: https://pkulaw.com/en_law/4dce14765f4265f1bdfb.html (перевод был сделан автором самостоятельно посредством онлайн-инструментов, дата обращения: 11.02.2021).

[13] Китай предложил обеспечить глобальную безопасность данных // Коммерсант URL: www.kommersant.ru/doc/4483436 (дата обращения: 20.02.2022).

- выделить и классифицировать интернет-технологии конфликтной мобилизации;

- установить формы и методы применения технологий конфликтной мобилизации и управления протестом в КНР и США, определить их сходства и различия;

- определить основные подходы к организации противодействия виртуальным технологиям конфликтной мобилизации, применяемые в Российской Федерации;

- выработать эффективные методы противодействия интернет-технологиям конфликтной мобилизации, учитывая актуальное состояние международной политики.

- обозначить конкретные предложения для укрепления цифрового суверенитета Российской Федерации посредством развития системы противодействий интернет-технологиям конфликтной мобилизации.

Теоретико-методологическая основа исследования включает в себя системный, структурный и сравнительный подходы. Методология исследования определяется как его целью и задачами, так и научным подходом автора. При этом ключевыми принципами являются объективность исследования, его логичность и системность.

В настоящем исследовании используется сравнительный метод: автор сопоставляет подходы Китайской Народной Республики, Соединенных Штатов Америки и Российской Федерации к противодействию интернет-технологиям конфликтной мобилизации. Это позволило определить преимущества и недостатки каждого из подходов и выработать альтернативный метод, учитывающий слабые и сильные стороны подходов США и КНР. Выбор указанных государств в качестве сравнительных референтов определяется высоким уровнем технологического развития государств, что связано с возможностью противодействия виртуальным технологиям конфликтной мобилизации, а также отличием подходов этих государств к управлению виртуальной сферой. Задачей анализа опыта

приведенных государств является поиск нетривиальных решений, способных в перспективе укрепить российскую систему противодействия интернет-технологиям конфликтной мобилизации. При этом, автор не предполагает возможности полного копирования Россией подходов США и КНР в связи с явными социально-культурными, техническими и политическими причинами. Помимо этого, сравнительный метод использовался при анализе самого феномена сетевой конфликтной мобилизации, что позволило определить его роль в современном политическом процессе.

Структурный подход заключается в составлении классификации технологий сетевой конфликтной мобилизации. Были выделены критерии классификации, определенные, как платформы применения изучаемых технологий, скорость применения, источники. Данная классификация позволила определить цели каждой технологии, а также конкретные методы противодействия ей.

В рамках исследования также изучались реальные примеры применения технологий в США, КНР и Российской Федерации посредством контентного анализа публикаций в социальных сетях, выстраиванием хронологии действий организаторов протестов, а также замером уровня вовлеченности подписчиков в протестный контент, что позволило приобрести дополнительные знания об алгоритме реализации сценария конфликтной мобилизации в интернете. Исследование также включает в себя и использование методологии OSINT (Open source intelligence) или разведку по открытым источникам. Благодаря созданию специального аккаунта в социальных сетях и добавлению в группы для организации протестных акций в Гонконге, в мессенджере Telegram удалось выявить новые виртуальные технологии политической мобилизации – например, технологию геймификации протеста.

Научная новизна результатов исследования определяется, в первую очередь, исследованием ранее недостаточно изученных особенностей интернет-технологий конфликтной мобилизации:

- определены необходимые исходные социально-политические факторы, наличие которых делает возможным организацию конфликтной мобилизации в онлайн-пространстве. Одним из основных факторов является наличие виртуальной политической толпы, объединенной с помощью социальных сетей путем использования технологий формирования групповой идентичности и механизмов аутгрупповой агрессии;

- сформирована авторская классификация интернет-технологий конфликтной мобилизации. Она применима к каждому случаю использования таких интернет-технологий и позволяет рассматривать их по следующим критериям: где применяются, кто применяет, как долго применяет, на какую аудиторию, с помощью каких источников? В результате появления данной классификации удалось определить подходы организаторов протестов к использованию интернет-технологий конфликтной мобилизации, а также подходы государств к противодействию этим технологиям;

- выявлен ряд новых технологий конфликтной мобилизации, таких как геймификация протеста, позволяющая пролонгировать протестную активность и придать ей признаки игры. Также установлены и предложены методы противодействия данной технологии. Ценность выявления новых инструментов конфликтной мобилизации в интернете заключается в возможности оценки перспектив их практического применения во время протестных акций, а также в поиске технологий противодействия им;

- представлена авторская классификация для оценки подходов США, КНР в части противодействия интернет-технологиям конфликтной мобилизации. В результате анализа удалось определить подход США, заключающийся в создании единой системы управления информационным пространством, включающей партнерские отношения с крупнейшими социальными сетями и другими платформами, входящими в юрисдикцию государства. Такое партнерство делает возможным делегирование ряда задач государства по контролю за интернет-пространством этим компаниям. Также

определен подход КНР как подход централизованного государственного контроля, не дающий возможности внешним акторам использовать внутрикитайские интернет-площадки;

- выделено изменение подхода организаторов протестов в Российской Федерации к использованию интернет-технологий конфликтной мобилизации, что позволило автору исследования предложить актуальные рекомендации по противодействию данным технологиям; сделан важный вывод о перспективе появления в российском сегменте интернета обезличенных источников протестной информации, вокруг которых будет выстраиваться мобилизация пользователей; а также о росте использования такими источниками интернет-технологий конфликтной мобилизации краткосрочного и быстрого эффекта воздействия.

На защиту выносятся следующие положения:

1. Конфликтная мобилизации в онлайн-пространстве, как и классическая политическая мобилизация, возникает при следующих условиях: наличие реальных объективных проблем в экономической и политической жизни государства, депривация части населения, мобилизация ресурсов, наличие идентичности протестной группы, неэффективность функционирования системы правоохранительных органов. Отличием конфликтной мобилизации в интернете от других видов мобилизаций является возникновение виртуальной толпы, позволяющей администраторам страниц в социальных сетях координировать и управлять протестом в удаленном режиме. Конфликтная мобилизация в онлайн-пространстве определяется как сосредоточение и задействование субъектом политики методов и инструментов, применяемых в интернет-пространстве для организации, контроля и эскалации политического конфликта.

2. Ключевая роль в управлении процессами конфликтной мобилизации принадлежит администраторам сетевых групп и сообществ: администраторы групп в социальных сетях вызывают у пользователей чувство недовольства их собственным экономическим положением,

политическими правами и свободами, создают идентичность виртуальной группы путем противопоставления пользователей представителям власти, крупного бизнеса или иным акторам, демонстрируют эффективность виртуальной группы в реальной жизни с помощью проведения офлайн-политических акций.

3. В ходе проведенного исследования выявлены следующие виды технологий конфликтной мобилизации в пространстве сети Интернет: технологии социальных сетей, технологии видеохостингов, технологии мессенджеров, технологии микроблогов – по критерию интернет-платформы; открытые и скрытые технологии – по критерию субъекта мобилизации, вокруг которого происходит объединение пользователей; быстрые и долгосрочные технологии – по критерию скорости подготовки и продолжительности эффекта; локальные, государственные, межгосударственные технологии – по критерию радиуса воздействия технологий; централизованные или распределенные – по критерию акторов-передатчиков информации.

4. Выявлены подходы в применении интернет-технологий конфликтной мобилизации организаторами протестов США и КНР. В США используются технологии социальных сетей и форумов, открытые технологии, долгосрочные и быстрые по критерию скорости подготовки и продолжительности эффекта, локальные по критерию радиуса воздействия технологий и централизованные по критерию акторов-передатчиков информации. В КНР состав наиболее популярных технологий конфликтной мобилизации, согласно приведенной в диссертационном исследовании классификации, следующий: технологии социальных сетей, мессенджеров, видеохостигов, микроблогов, скрытые технологии – по критерию субъекта мобилизации, быстрые – по критерию скорости подготовки и продолжительности эффекта технологий, международные и локальные – по критерию радиуса воздействия технологий, а также распределенные – по критерию акторов-передатчиков информации.

5. В России организаторы протестов с помощью интернет-технологий конфликтной мобилизации преимущественно используют технологии социальных сетей, видеохостингов, микроблогов, мессенджеров, скрытые технологии – по критерию субъекта мобилизации, быстрые технологии – по критерию скорости подготовки и продолжительности эффекта, международные – по радиусу воздействия, распределенные – по критерию акторов-передатчиков информации.

Для укрепления цифрового суверенитета Российской Федерации необходимо, во-первых, использовать распределенные технологии политической мобилизации в международных интернет-площадках с целью развития позитивного образа власти и государства в российском сегменте интернета; во-вторых, повышать уровень доверия к государству во внутригосударственных и неангажированных международных социальных сетях, используя долгосрочные, централизованные и распределенные технологии; в-третьих, вести мониторинг и выявление новых технологий конфликтной мобилизации, учитывая риски использования организаторами политических акций новых быстрых инструментов; в-четвертых, стимулировать развитие российских социальных сетей, мессенджеров и иных платформ, поощрять их выход на международный уровень для укрепления возможностей Российской Федерации формировать через них международную повестку.

Теоретическая значимость полученных результатов определяется актуальностью темы исследования и состоит в сформулированных методах противодействия виртуальным технологиям конфликтной мобилизации странами: США и КНР, использующими отличные друг от друга подходы к купированию угрозы применения этих технологий; также представлена ретроспектива развития российского подхода к борьбе с виртуальными механизмами реализации сценариев конфликтной мобилизации, и отражены перспективы эволюции подхода Российской Федерации.

Методы противодействия онлайн-инструментам конфликтной мобилизации представлены в сравнении друг с другом благодаря разработке авторской классификации интернет-технологий этого феномена. Выделено 5 групп критериев, основанных на изучении применяемых на практике инструментов политического влияния в интернете. Каждая из групп определяет цели и задачи используемых технологий. Такая классификация позволила выявить динамику изменения подхода отдельных государств к противодействию интернет-технологиям политической мобилизации и выделить этапность сценария реализации экзогенного политического конфликта.

Практическая значимость результатов диссертационного исследования обусловлена тем, что органы государственной власти, некоммерческие и коммерческие структуры, занимающиеся формированием позитивного имиджа Российской Федерации за рубежом, а также те организации, деятельность которых ориентирована на повышение уровень доверия к государству внутри страны, могут использовать полученные результаты в своей работе, ориентируясь на классификацию интернет-технологий политической мобилизации при выборе методов реализации своих задач. Сформулированная классификация позволяет эффективно подобрать онлайн-инструменты в зависимости от уровня доступности интернет-площадок, наличия лидеров общественного мнения, сроков реализации задач, а также контрмер противоположной стороны при ее наличии.

Апробация результатов работы.

Основные идеи, материалы и положения диссертационного исследования нашли свое отражение в 6 статьях (общим объемом 5,02 п.л. / авторский вклад – 4,44 п.л.), из которых 4 статьи (объемом 3,74 п.л. / авторский вклад – 3,39 п.л.) опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности и отрасли наук.

Работа также была апробирована в рамках участия автора в научных и общественно-политических конференциях. В частности, на молодежной научной конференции «Ломоносов-2020» с темой «Виртуальные технологии конфликтной мобилизации в социально-экологическом конфликте «Шиес», Архангельская область». Отдельные главы работы были представлены в рамках программы конференции «Дни PR», организованной Российской ассоциацией связей с общественностью («РАСО») и в рамках научной конференции «Выборы в Государственную Думу 2021: повестка, стратегии и технологии» с темой «Мобилизационный потенциал Тикток: преимущества новой социальной сети для политиков».

Глава 1. Теоретико-методологические основания исследования феномена конфликтной мобилизации в интернет-пространстве

1.1 Эволюция понятий и представлений о феномене, формах и методах конфликтной мобилизации в интернет-пространстве

Конфликтная мобилизация – один из видов политической мобилизации. В свою очередь, под термином политическая мобилизация понимается сосредоточение и задействование субъектом политики различных материальных и людских ресурсов для достижения своих целей прежде всего путем создания массовой поддержки со стороны граждан, установления контроля над финансовыми и информационными источниками[14]. Таким образом, термин «конфликтная мобилизация» определяет характер методов и инструментов, используемых субъектами политики для создания массовой поддержки со стороны граждан. К таким методам относятся те, которые позволяют убедить людей в необходимости участия в протестных политических акциях, основу которых составляют насильственные действия. Конфликтная мобилизация реализуется с помощью комплекса средств и методов, направленных на работу с гражданами.

[14] Мельвиль А.Ю. Политология: учеб. / М.: Московский государственный институт международных отношений (Университет) МИД России. - Проспект, 2008. - 311 с.

В современной политике особое место занимают виртуальные технологии конфликтной мобилизации. К ним относятся инструменты информирования и убеждения, используемые в виртуальном пространстве, т.е. в интернете. Данные технологии значительно эволюционировали за последние двадцать лет. Так, во время «оранжевой революции» на Украине в 2004 году использование виртуальных технологий конфликтной мобилизации ограничивалось информированием о ходе политической борьбы в стране на специализированных профильных сайтах[15]. Для получения доступа к ним посетителю было необходимо пройти процедуру регистрации. Такой механизм значительно ограничивал возможности и потенциал виртуальных технологий конфликтной мобилизации. Однако с течением времени, с развитием интернета, социальных сетей эти технологии заняли особое место в процессе организации протестных акций. Уже в 2010-2012 годах в революциях, произошедших в государствах арабского мира (так называемая «Арабская весна») – Тунисе, Египте и Йемене – интернет использовался не как вспомогательная сила, но как основа противостояния общества и представителей власти[16]. Социальные сети сыграли ключевую роль в организации и контроле лидерами оппозиции протестных акций, приведших к отставкам президентов и сменам политических элит. Значимая роль интернета в этих революциях также отмечена исследователями, давшими им альтернативное название «Твиттерные революции» (Твиттер (Twitter – англ.) – американская социальная сеть, микроблог; активно использовалась для освещения протестных акций, а также их координации лидерами и участниками протеста во время революций «Арабской весны»). Виртуальные технологии конфликтной мобилизации используются в большинстве современных политических акций. В качестве еще одного

---

[15] Громова А. В. Роль СМИ в осуществлении «Цветных революций» // Вестник РУДН. Серия: Литературоведение, журналистика. - 2008. - №2.

[16] Панцерев, К.А. "Твиттерные революции" в странах Северной Африки - обратная сторона развития информационного общества // Азия и Африка сегодня. – 2016. - №4 (705),
Манойло А. В. Информационный фактор цветных революций и современных технологий демонтажа политических режимов // Вестник МГИМО. - 2014. - №6 (39).

примера можно привести антикоррупционные митинги в Москве и других крупных городах России в 2017 году, поводом для которых стал фильм-расследование оппозиционного политика А. Навального. Именно с помощью комплекса виртуальных технологий конфликтной мобилизации политику и его штабу удалось организовать и привлечь людей к несанкционированным митингам[17].

Виртуальным технологиям конфликтной мобилизации посвящено множество статей современных исследователей, написаны монографии, учебные пособия, а также изданы научно-популярные книги. Исследование виртуальных технологий конфликтной мобилизации основывается на 3 смысловых блоках:

1. Изучение различных теорий коммуникации.
2. Изучение современной информационной среды.
3. Изучение интернет-технологий конфликтной мобилизации.

Изучать феномен интернет-технологий, не затрагивая предшествующих ему смысловых блоков, невозможно. Это связано с тем, что исследования теорий коммуникации, а также современной информационной среды определяют изучение интернет-технологий, являющихся, в свою очередь, неотъемлемой частью как самого интернета, то есть информационной среды, так и технологий коммуникации, описанных в соответствующих теориях.

Однако прежде чем приступать к более глубокому анализу приведенных выше тезисов, посвященных феномену политической мобилизации, необходимо также и обозначить рамки феномена протеста, как конечной цели этой мобилизации.

Политический протест может быть интерпретирован с различных позиций. Согласно одному из подходов, под политическим протестом понимается публичное выражение недовольства, обиды, инакомыслия,

[17] Танцура М. С., Садовникова А. А. Исследование сетевой активности как инструмента политической мобилизации молодёжи (на примере антикоррупционных митингов 26 марта 2017 г.) // Известия Восточного института. - 2019. - №1 (41).

позволяющее снять накопившееся напряжение[18]. Иной подход говорит о том, что протест – организованная и скоординированная деятельность граждан, направленная на процесс принятия решений с целью повлиять на него[19]. Третий подход же говорит о том, что политический протест – действие, находящееся за рамками «нормальной» политики[20]. Автор данного подхода Ч. Тилли считает, что протестная активность подразумевает игнорирование сложившихся в обществе норм и разрушение правил допустимых форм политического действия. Данное определение наиболее близко к ситуациям политического конфликта власти и общества, рассматриваемым в рамках работы. Из этого определения становится возможным и формулирование рамок для объяснения, что такое противодействие политическому протесту. Это действия, направленные на сохранение сложившихся в обществе норм и правил организации допустимых форм политического участия граждан. Данное определение позволит конкретизировать спектр рассматриваемых протестных явлений и задачи исследования.

Основу феномена виртуальных технологий конфликтной мобилизации составляет политическая коммуникация. Данные технологии связаны с методами передачи информации от технологов пользователям и реакцией последних на эту информацию. Именно реакция пользователей социальных сетей на информацию, создаваемую заинтересованными политическими силами, определяет эффективность подобных технологий и, соответственно, влияет на политический процесс. Сами технологии являются эволюционным продолжением методов политической коммуникации. В связи с этим для понимания основных принципов виртуальных технологий конфликтной мобилизации необходимо углубиться в понимание феномена политической коммуникации.

---

[18] Travaglino G.A. Social sciences and social movements: the theoretical context / Contemporary Social Science. - 2014. - V.9. - N.1. - P. 1-14

[19] Piven F.F., Cloward R.A. Collective protest: a critique of resource mobilization theory / International Journal of Politics, Culture and Society. - 1991. - V.4, - N.4. - P 435-458.

[20] Tilly C. Food Supply and public order in modern Europe / The formation of national states in Western Europe. Princeton University Press. - 1975. - P. 380-455.

Изучение политической коммуникации началось в середине XX века. Г. Лассуэл в 1948 году в статье «Структура и функции коммуникации в обществе»[21] предложил определение термину «коммуникация», основанному на пяти ключевых его элементах:

- Кто?
- Что сообщает?
- По какому каналу?
- Кому?
- С каким результатом?

Отвечая на эти вопросы, по мнению Г. Лассуэла, мы понимаем, что такое коммуникация, и из чего она состоит. Помимо самого определения коммуникации Г. Лассуэл предложил модель, которая позволяет нам понять и основные принципы организации виртуальных технологий конфликтной мобилизации. Эта модель состоит из следующих компонентов: коммуникатор, сообщение, канал, реципиент, эффект. Коммуникатор создает сообщение, транслирует его через канал коммуникации, тем самым донося его до конкретного реципиента, получателя информации, а тот, в свою очередь, реагирует на сообщение, производя действия. Виртуальные технологии конфликтной мобилизации основаны на аналогичном алгоритме: технологи (коммуникаторы) создают сообщение (изначально направленное на появление острой политической реакции), транслируют его через социальные сети в интернете, доводя информацию до широкой аудитории пользователей социальных сетей, а последние, получая это сообщение, реагируют на него. При этом конечной задачей технологов является реакция пользователей не в виртуальной среде, а в реальном мире, на улицах городов.

Модель коммуникации Гарольда Лассуэла характеризуется также идеей манипулирования мнением реципиентов[22]. Однако она имеет ряд

---

[21] Lasswell H.D. The structure and function of communication in society // The communication of Ideas / Ed. By l. Bryson. N.Y. - 1948.

[22] Володенков С. В. Политическая коммуникация и современное политическое управление // Вестник Московского университета. Серия 12. Политические науки. - 2011. - №6.

недостатков. Во-первых, она демонстрирует лишь однонаправленное движение информации, сообщения. Она применима, если мы говорим про традиционные средства массовой коммуникации, например, газеты или радио, где у реципиентов нет возможности ответить коммуникатору. Однако, рассматривая интернет-технологии конфликтной мобилизации, следует отметить, что такая модель является неполной. Пользователи отвечают на сообщение коммуникатора, интерпретируя его по-своему. Данная особенность виртуальной среды является важной частью современных, сетевых моделей коммуникации. Во-вторых, модель Г. Лассуэла не принимает во внимание особенности самих каналов коммуникации. В частности, не были изучены различные «шумы», возникающие на этапе трансляции сообщения через каналы коммуникации и искажающие его изначальный смысл. Изучая виртуальную среду массовой коммуникации, следует сказать, что именно данный элемент является ключевым в интернете. Восприятие информации зависит от восприятия самого канала коммуникации (например, определенной информационной страницы в социальной сети, либо даже от имиджа самой социальной сети).

Несколько видоизмененная модель коммуникации была предложена ученными-математиками К. Шенноном и У. Уивером в статье «Математическая теория коммуникации»[23]. Ключевым отличием от теории Лассуэла является внимание к каналу коммуникации. К. Шеннон и У. Уивер добавили в модель Г. Лассуэла понятия «передатчик» и «декодер». Задача «передатчика» – интерпретация информации от коммуникатора для ее передачи по каналу коммуникации. В свою очередь задача «декодера» – расшифровка уже закодированной «передатчиком» информации для ее конечного получателя. Рассматривать «передатчик» и «декодер» можно как реальные технические средства, либо как роли тех или иных участников

[23] Shannon, Claude and Warren Weaver, The Mathematical Theory of Communication, Urbana, IL: The University of Chicago Press, 1949; Коммуникационные процессы в обществе: институты и субъекты. Монография / И.М. Дзялошинский. – М.: Издательство АПК и ППРО, 2012. - 592 с.; Дзялошинский И.М. Экология коммуникаций: учебное пособие / Дзялошинский И.М. — Саратов: Ай Пи Эр Медиа, 2019. — 443 с.

процесса коммуникации. Так, в частности, в социальной сети группа или сообщество могут быть «передатчиками» информации, которую подготовил коммуникатор, а человек, сделавший репост себе на страницу – «декодером», расшифровывающий эту информацию уже по-своему для своих подписчиков. При этом К. Шеннон и У. Уивер вводят понятие «шумов» – помех, внешних элементов, наличие которых влияет на интерпретацию изначального сообщения.

Таким образом, модель К. Шеннона и У. Уивера представляет собой следующий алгоритм: коммуникатор, источник информации, передает ее передатчику, который обрабатывает сообщение и отправляет его по каналу коммуникации, откуда декодер расшифровывает ее и передает уже конечному звену этой цепочки – приёмнику. При этом приёмник получает сообщение после воздействия на него «шумов», искажающих изначальный смысл этого сообщения. Однако и в этой цепочке также есть упущенные элементы. Например, также, как и в модели Г. Лассуэла, отсутствует ветка обратной связи от приемника до коммуникатора.

Значительное развитие модель коммуникации получила благодаря М. Де Флеру и его книге «Теории массовой коммуникации»[24]. Основной вклад в теорию коммуникации М. Де Флера связан с внедрением принципа обратной связи в ранее линейную модель. По своим элементам модель М. Де Флера аналогична той, которую создали К. Шеннон и У. Уивер. В ней также присутствуют: источник информации (коммуникатор), передатчик, канал связи, приёмник, получатель. При этом приёмник – аналог «декодера» в теории К. Шеннона и У. Уивера. Интерес вызывает цепочка движения сообщения в этой модели. Коммуникатор создает сообщение, отправляет его передатчику, тот кодирует сообщение, перенося его на язык определенного канала связи. Далее приемник получает сообщение посредством канала связи и декодирует его так, чтобы конечный получатель его смог принять. Однако движение сообщения на этом не заканчивается. Конечный получатель в свою

[24] Melvin L. De Fleur, Theories of Mass Communication, New York, Mckay, 1970.

очередь сам становится источником информации после получения сообщения. Он также запускает уже по-своему интерпретированное сообщение передатчику, и цепочка повторяется вновь. Особенность данной модели – ее цикличность. Модель характеризует массовую коммуникацию, как непрекращающееся движение информации, где получатель сообщения является в тот же самый момент и его источником. Еще одним отличительным признаком этой модели от предложенной К. Шенноном и У. Уивером является то, что «шумы» действуют не только на передатчика и декодера информации, а на все элементы цепочки. Тем самым, М. Де Флер отмечает помимо цикличности движения информации, ее постоянное искажение.

Данная модель ближе других характеризует движение информации в интернете. Современные возможности быстрого распространения информации основаны на совмещении роли получателя сообщения и его источника. Люди замечают публикацию в социальной сети, делают «репост» на свою страницу, становясь уже источником информации, а также добавляют к изначальному смыслу свою интерпретацию.

Принципы передачи информации в интернете позволяют определить схему ее распространения. При этом они не позволяют нам понять, как именно люди, пользователи начинают верить этой информации и руководствоваться ею во время принятия решения об участии в политическом протесте.

1.2. История изучения трансформации информационной среды как поля применения интернет-технологий протестной мобилизации

Создание интернета и его развитие стало поводом для ожидания глобальных изменений со стороны ученых и исследователей. Эти изменения должны были коснуться не только методов получения информации и методов общения, но и стабильности политических систем, их трансформации и изменения места государственных органов в новых системах. В своих работах многие исследователи уделяют внимание вопросам использования интернет-пространства, как инструмента воздействия на общественное мнение[25]. Данный вопрос относится к сфере убеждения, манипулирования мнением пользователей. Ряд авторов исследовали именно эту составляющую виртуальных технологий конфликтной мобилизации. Так, Роналд Дейберт[26], профессор кафедры политологии Университета Торонто, Канада, в своей книге «Пергамент, печать и гипермедиа: коммуникация во время трансформации мирового порядка» высказал мнение, что появление новых методов передачи информации всегда сопровождается глобальными социальными изменениями. Например, появление печатных книг стало причиной начала упадка церкви в Европе. Аналогичные по значимости процессы Р. Дейберт ожидал и от новых СМИ, в том числе и от интернета. По его мнению, «гипермедиа» (именно так он называл интернет) лишат правительства

[25] Егорова-Гантман Е. В. В тумане войны. Наступательные военные коммуникативные технологии. — Самара: ООО «Офорт»; М.: Группа компаний «Никколо М», 2010. — 432 с.; Манойло А.В. М Государственная информационная политика в особых условиях: М.: МИФИ, 2003. – 388 с.

[26] Deibert R.J. Parchment, Printing and Hypermedia: Communications in World Order Transformation. – N.Y.: Columbia University Press, 1997.

возможности совершать противоправные негуманные действия против своего населения. Открытый мир интернета должен обеспечить реализацию единых стандартов справедливости и свободы на территории всей планеты. Агентами же такого контроля, по мнению Р. Дейберта, должны стать некоммерческие организации (НКО). Автор отмечает, что реальная власть может отойти таким организациям, а в перспективе они могут даже заменить государства. Для этого необходимо уничтожение границ и создание единой «интернет-нации». Виртуальные технологии конфликтной мобилизации в контексте данной работы должны стать инструментом реализации подобной идеи.

Иного мнения придерживается Френсис Фукуяма в своей книге «Доверие»[27]. По мнению американского философа, новый информационный мир не сделает общество свободнее. Идея свободы, по мнению Ф. Фукуямы, в мире развитого интернета, связана с ожиданиями уничтожения существующей иерархии, в том числе политической. Несмотря на ликвидацию линейных типов коммуникации, акторы все равно сохранят желание контролировать других акторов, что вызовет необходимость сохранения этой иерархии. «Таким образом, ниоткуда не следует, что информационная революция оставит крупные иерархические организации в прошлом и на их месте возникнут добровольные человеческие сообщества. Поскольку объединение людей зависит от доверия между ними, а доверие, в свою очередь, обусловлено существующей культурой, следует сделать вывод, что в разных культурах добровольные сообщества будут развиваться в разной степени. Иными словами, способность компаний к переходу от крупной иерархической структуры к гибкой сети мелких фирм будет зависеть от степени доверия и социального капитала, характерного для общества в целом».

[27] Фукуяма Ф. Доверие: социальные добродетели и путь к процветанию: Пер. с англ. / Ф. Фукуяма. — М.: ООО «Издательство АСТ»: ЗАО НПП «Ермак», 2004. — 730, [6] с.

Одним из первых исследователей, обративших внимание на интернет-технологии протестной мобилизации в свете появления новой информационной среды, был Говард Рейнгольд. В своей работе «Умная толпа»[28] он впервые дал определение подобному феномену. «Сетевая война — это новый вид противоборства, где герои — от террористов и преступных группировок со стороны зла до воинственных общественных деятелей со стороны добра — используют сетевые формы организации, доктрины, стратегии и технологии с учетом требований информационного века». Г. Рейнгольд писал, что, несмотря на с виду демократические формы, новые сетевые технологии могут стать оружием в руках «вредных» элементов общества. «Большинство людей, пожалуй, надеются на появление новой формы организации во главе с «хорошими парнями», поступающими «правильно», набирающей все большую силу. Но события прошлого опровергают подобную точку зрения. В пору становления новой формы на первых ролях могут оказаться недовольные, никчемные люди или пройдохи, желающие воспользоваться открывшимися возможностями ради козней, наживы или власти». Основной идеей его работы является тезис, связанный с сетевой коммуникацией граждан – способность в условиях ограниченных временных ресурсов собирать толпы людей и синхронизировать их действия. Автор приводит пример флешмобов – акций, зачастую носящих рекламный характер, основанных на массовости и синхронности действий участников. Однако этот принцип находит отражение и в политике: например, в 2001 году в результате использования виртуальных средств коммуникации – SMS сообщений, которые содержали призыв к выходу на улицы г. Манила – удалось свергнуть президента Филиппин Дж. Эстраду[29]. Принципиальной идеей работы Г. Рейнгольда является тезис о децентрализации социальных связей – принцип коммуникации «от многих ко многим». Однако автор

[28] Рейнгольд Г. Умная толпа: новая социальная революция / Говард Рейнгольд. — Пер. с англ. А. Гарькавого. — М. : ФАИРПРЕСС, 2006. - 416 с.

[29] Ушкин С.Г. Теоретико-методологические подходы к изучению сетевой протестной активности: от «умной толпы» к «слактивизму» // Мониторинг общественного мнения: экономические и социальные перемены. - 2015. - № 3. - С. 3- 11.

придерживается мнения, что виртуальные средства коммуникации играют на руку не только технологам, желающим подорвать политическую стабильность государств, но и помогают самим властям контролировать общества, так как Интернет позволяет получать большие объемы информации о каждом человеке, зарегистрированным в той или иной социальной сети.

Развитие интернета и, в частности, социальных сетей определило появление существенных изменений не только в нашей бытовой жизни, но и в принципах коммуникации[30]. Это, в свою очередь, отразилось на появлении новых форм политической коммуникации. Результатом данного процесса стало повышение роли социальных сетей в политической жизни государств. Появились также интернет-технологии конфликтной мобилизации, с помощью которых акторы политического процесса задействуют пользователей социальных сетей в политических акциях. Как именно реализуются и применяются данные технологии – вопрос, которым задаются и который изучают многие исследователи.

[30] Шентякова А.В., Гришин Н.В. Мобилизация политического протеста молодежи и российские видеоблогеры: результаты когнитивного картирования // Galactica Media: Journal of Media Studies. - 2021. - Т. 3. - № 2. - С. 88-109.; Якунин В. И., Акаев А. А., Кочетков А. П. и др. Вызовы времени: Устойчивость государства в условиях современной трансформации // Вестник Московского университета. Серия 12: Политические науки. - 2021. - № 4.; Якунин, В. И., Кузнецов, И. И., Вилисов, М. В. Устойчивость государственных систем на постсоветском пространстве: контуры теоретической модели // Контуры глобальных трансформаций: политика, экономика, право. - 2020. - Т. 13. - №4. - С. 6–33.; Якунин, В. И. Идеологические клише и мифы как инструмент внешней политики США // Российский журнал правовых исследований. – 2018. - №1(14). - С. 9–19.

1.3. История изучения интернет-технологий конфликтной мобилизации

Одной из ключевых работ, посвященных изучению виртуальных технологий конфликтной мобилизации, является книга Э. Аронсона и Э. Партканиса «Эпоха пропаганды: Механизмы убеждения, повседневное использование и злоупотребление»[31]. Авторы уделяют внимание вопросам управления мнением людей с помощью различных техник и инструментов манипуляционного воздействия. В частности, Э. Арансон и Э. Партканис рассматривают интернет, как площадку, обладающую необходимыми возможностями для подобного воздействия. «Шагом вперед в распространении слухов и фактоидов является «флэйминг» (flaming) в Интернете. «Флэйминг» — это специальный интернетовский термин для злостных нападок и необоснованных слухов». Технология «флейминга», согласно Э. Арансону и Э. Партканису, является одной из виртуальных технологий конфликтной мобилизации. Авторы приходят к выводу, что вариаций методов воздействия, пропаганды в современном мире становится так много, что вырабатывать противодействие для каждого из них нерационально. Вместо этого предлагается обучать будущих профессионалов этой сферы аналогичным технологиям, руководствуясь принципом «лучшая защита – нападение». Более того, авторы уверены, что подобное обучение следует проводить не только для профессионалов, но и для масс, вырабатывая у них устойчивость к подобным технологиям. «Второй вариант техники, повышающей сопротивляемость убеждению по данной теме, —

[31] Аронсон Э., Пратканис Э. Р. Эпоха пропаганды: Механизмы убеждения, повседневное использование и злоупотребление. Перераб. изд. – СПб.: Прайм–Еврознак, 2003. –384 с.

прививка. Мы уже видели, что двухстороннее (включая опровержение) изложение данных более эффективно для убеждения определенных видов аудиторий, чем одностороннее преподнесение. Если людей предварительно подвергнуть воздействию краткого сообщения, которое они способны опровергнуть, потом они склонны демонстрировать «иммунитет» против последующего полномасштабного изложения тех же самых доводов — почти так же, как небольшое количество ослабленного вируса иммунизирует людей против настоящего вторжения этого вируса».

Одним из наиболее известных ученых, изучающих специфику социальных протестных движений в эпоху интернета, является Мануэль Кастельс. В своей работе «Власть коммуникации»[32] М. Кастельс формирует теорию сетевой коммуникации власти. Согласно данной работе источники власти, такие как убеждение, насилие, политическое доминирование, культурное фреймирование, сохранились и в настоящее время. Однако изменилась «область воздействия» власти – теперь она формируется преимущественно вокруг сетей. Сети могут формироваться и управляться как представителями власти, так и оппозиционными силами в зависимости от того, у кого процесс их программирования оказывается успешнее. Продолжение идеи книги «Власть коммуникации» нашлось в другой работе М. Кастельса «Сети возмущения и надежды - социальные движения в эпоху Интернета»[33]. Автор переносит сетевую теорию коммуникации на современную структуру интернет-коммуникации, выделяя в ней особенности развития и управления социальных движений: различных акций протеста, революций, митингов и т.д. Ключевым преимуществом интернета в вопросах имплементации и развития протеста является возможность создания «виртуальных сетей» – связей в киберпространстве, через которые люди идентифицируют себя и свои страхи, политическое недовольство, разделяя

[32] Кастельс, М. Власть коммуникации [Текст]: учеб. пособие / М. Кастельс ; пер. с англ. Н. М. Тылевич ; под науч. ред. А. И. Черных ; Нац. исслед. ун-т «Высшая школа экономики». — М. : Изд. дом Высшей школы экономики, 2016. — 564 с.

[33] Castells, Manuel (2012). Networks of outrage and hope – social movements in the Internet age. Chichester, UK: Wiley. – 298 pp.

их с другими. При традиционных типах коммуникации человек, недовольный действующей властью, противостоящий ей, в условиях отсутствия поддержки среди своего окружения воспринимается обществом, как маргинал. Такое фреймирование исключает любые возможности по организации этим человеком социального протеста. В условиях интернет-коммуникации гражданин таких взглядов из-за особенностей самого интернета, а именно, отсутствия локальных и временных ограничений, способен сконструировать «протестную сеть». Создаваемая виртуальная группа в конечном итоге идеологически объединяется с людьми, реально выходящими на улицы городов. Такое объединение М. Кастельс назвал «автономным пространством» – гибридом улицы и социальных сетей. При этом основное отличие интернет-коммуникации от других ее типов заключается в организационных и информационных возможностях интернета. «Автономное пространство» не ограничено влиянием властей, территориальными, а также временными ограничениями. У теории интернет-протеста М. Кастельса есть также предположение, что любая политическая активность, проводимая через интернет, вызвана не реальными причинами и спланированными действиями, а совокупностью совпадений. Причиной этого автор называет множество возможных акторов коммуникации, влияющих на формирование таких активностей. В связи с этим у политических активностей, имплементированных с помощью интернета, могут отсутствовать привычные временные рамки: начало и конец.

Помимо изучения общих особенностей политического протеста, организованного с помощью интернета, М. Кастельс также приводит схему формирования подобной активности. Решение об участии в политическом протесте пользователь принимает в зависимости от наличия 4 факторов:

1. Личного недовольства – убеждения в несправедливости существующих политической и социальной систем;

2. Личных возможностей – М. Кастельс пишет, что основой всех протестных политических активностей являются молодые, образованные, но

при этом нетрудоустроенные люди. Эта категория людей имеет как физические, так и психологические возможности для участия в протесте;

3. Виртуальной среды – наличием у потенциального участника протеста доступа к интернету и пониманию основ коммуникации в этой среде;

4. Идентификации себя, как представителя нового времени – М. Кастельс утверждает, что пользователи интернета ощущают себя не только гражданами своей страны, но и гражданами всего мира, и именно эта идентичность влияет на желание людей добиваться дополнительных прав и свобод у государства.

Целью виртуальных технологий конфликтной мобилизации является создание «виртуальной толпы»[34] – группы пользователей социальных сетей, объединённых интересом к определенной проблематике, транслирующих или создающих контент. «Виртуальная толпа» необходима для формирования идентичности у группы пользователей, которая в последствии заставляет их участвовать в реальных политических акциях на улицах городов. Феномен «виртуальной толпы» описал в статье «Новые социальные медиа: шанс или препятствие для диалога?» Г. Кехрель[35], профессор философии Инсбрукского университета (Австрия), президент Международной ассоциации за прогресс. Он выделил следующие характеристики «виртуальной толпы»:

1) передача информации в режиме реального времени;
2) передача информации в визуальной и аудиовизуальной формах;
3) интерактивность – участие всех акторов коммуникации;
4) коллективная виртуальная идентичность;
5) анонимность;
6) отсутствие понятного автора;
7) изменчивость тенденций;
8) ненадежность информации;

[34] Почепцов Г.Г. Информационно-политические технологии. - М.: Центр, 2003. - 381 с.
[35] Кёхлер Г. Новые социальные медиа: шанс или препятствие для диалога? – Полис. Политические исследования. - 2013. - № 4. - С. 75-87

9) прогрессия распространения информации – эффект «снежного кома»;

10) неустойчивость конструкции виртуальной толпы.

Г. Гехрель также задается вопросом – возможно ли в интернете выстроить диалог, или же это площадка лишь для навязывания мнения? Приводя аргументы, автор приходит к заключению, что любая массовая коммуникация, будь она между оратором и реальной или виртуальной толпой, основывается не на логических аргументах каждой стороны, а на эмоциональной составляющей тех доводов, которыми оперирует оратор. В связи с этим, интернет не может быть, по мнению автора, эффективной площадкой для истинно демократического диалога.

В России одним из первых потенциал интернета как среды организации протеста раскрыл Кузнецов И.И. в статье «РУНЕТ как часть российского электорального пространства»[36]. Рассматривая интернет, как территорию противостояния политиков во время электоральных процессов, автор отметил широкие возможности для организации так называемых информационных войн. «Особый фактор использования Сети в российских электоральных технологиях – создание и тиражирование компромата. Информацию в Интернете можно было публиковать анонимно, а затем цитировать как источник. Такой способ стал широко использоваться не только накануне общефедеральных и региональных избирательных кампаний, но и шире - в постоянно ведущихся политиками информационных войнах, ставших частью стратегий завоевания и удержания власти. Одним из первых сайтов такого рода стал «Коготь», на котором были «выложены» распечатки телефонных переговоров и пейджинговых сообщений представителей правящей «семьи». Эта информация стала основой нескольких публикаций в печатных СМИ». Описанное явление впоследствии получило широкое распространение и стало классической виртуальной

[36] Кузнецов И. И. РУНЕТ как часть российского электорального пространства // Общественные науки и современность. — 2003. — № 1. — С. 115–128.

технологией конфликтной мобилизации. Даже в отсутствии социальных сетей, Интернет в российской политике уже становился функциональным инструментом для решения политических задач. С появлением и развитием социальных сетей, в частности «Вконтакте», виртуальные технологии конфликтной мобилизации получили значительное развитие.

В поддержку тезиса эффективности интернет-технологий конфликтной мобилизации можно привести статью Докуки С.В. «Практики использования онлайновых социальных сетей»[37], в которой автор проводит исследование роли социальных сетей в процессе политической мобилизации и приходит к выводу, что эта роль действительно значима. В другой своей работе – диссертации на соискание ученное степени кандидата социологических наук «Коммуникация в социальных онлайн-сетях как фактор протестной мобилизации в России»[38] Докука С.В. демонстрирует динамику процесса сетевой политической мобилизации. В первую очередь, по словам автора, пользователи приобретают клиповое мышление, постоянно присутствуя в социальных сетях. Далее, когда технологам мобилизации необходимо привлекать людей, используются группы в социальных сетях и другие источники, распространяющие ангажированную информацию о том или ином политическом событии. Третий этап связан с образованием виртуальных протестных ячеек – групп протестной направленности в социальной сети, где люди, «обработанные» ангажированной информацией, делятся друг с другом мнениями, зачастую носящими конфликтогенный характер. Далее естественным образом у виртуального протестного сообщества формируется идентичность «мы-они», которая позволяет перенести процесс мобилизации на улицы городов. Пятый же этап, по мнению автора, отвечает за поддержку протестной активности в виртуальной среде уже после политической акции.

---

[37] Докука С. В. Практики использования онлайновых социальных сетей // Социологические исследования. - 2014. - № 1. - С. 137-145.

[38] Докука С.В. Коммуникация в социальных онлайн-сетях как фактор протестной мобилизации в России: дис. канд. социол. наук: 22.00.04. - Москва, 2014. - 150 с.

Вклад в изучение интернет-технологий конфликтной мобилизации внес также Володенков С.В. В диссертации на соискание научной степени доктора политических наук[39], в своей книге «Интернет-коммуникации в глобальном пространстве современного политического управления»[40] и в многочисленных статьях[41] по теме интернет-технологий политической коммуникации, автор проводит анализ эффективности подобных технологий как в российской, так и в международной политике и вводит новые научные термины в понятийный аппарат данной проблемы. Так, автор ввел понятие киберсимулякров – виртуальных конструкций, играющих ключевую роль в формировании массового восприятия пользователями политической реальности. Особую ценность представляет собой приведение в работах примеров реальных технологий интернет-коммуникации, влияющих на политический процесс. Так, например, предложена тринадцати-этапная модель организации «цветных революций», использующая виртуальные технологии протестной мобилизации. Помимо прочего, Володенков С.В. предлагает пересмотреть взгляд на интернет, как на территорию открытого диалога, утверждая, что социальные сети наоборот обладают существенно большим, чем традиционные СМИ, потенциалом для манипулирования общественным сознанием и мнением. Данная проблема, по мнению автора, вызывает необходимость выстраивания полноценной стратегии противодействия виртуальным технологиям конфликтной мобилизации. Эта задача государства воспринимается как приоритетная для защиты и сохранения суверенитета.

---

[39] Технологии интернет-коммуникации в системе современного политического управления: автореферат дис. доктора полит.наук : 23.00.02. - Москва, 2015. - 48 с.

[40] Володенков С. В. Интернет-коммуникации в глобальном пространстве современного политического управления. — Проспект Москва, 2018. — 271 с.

[41] Володенков С. В. Интернет-технологии как современный инструмент виртуализации массовой политической реальности // Вестник Московского университета. Серия 12. Политические науки. 2017. №2

Володенков С. В. Особенности интернет-коммуникации в современном политическом процессе // Вестник Московского университета. Серия 12. Политические науки. - 2014. - №2.

Володенков С. В. Медиатизация и виртуализация современного пространства публичной политики // Коммуникология. - 2016. - №4.

Володенков С.В. Роль информационно-коммуникационных технологий в современной политике // Антиномии. - 2018. - №2.

В поддержку значительного влияния социальных сетей на конфликтную мобилизацию можно найти множество работ социологов и политологов[42], однако существует и противоположная позиция[43]. Так, экс министр промышленности и торговли Венесуэлы, ныне известный журналист и политолог Мойзес Найм в книге «Конец власти. От залов заседаний до полей сражений, от церкви до государства: почему управлять сегодня нужно иначе» ставит под сомнение довод о влиянии социальных сетей на политику современных государств. «Власть приходит в упадок не под воздействием информационных технологий в целом и интернета в частности. Интернет и прочие средства коммуникации безусловно, меняют политику, массовую политическую активность, бизнес и, разумеется власть. Но их роль зачастую преувеличивают и недопонимают. Но обстоятельства, побудившие людей выйти на улицы, обусловлены ситуацией в страна и за рубежом, которая не имеет никакого отношения к новым средствам информации, оказавшимся в распоряжении у протестующих»[44]. Автор не разделяет позиции, согласно которой именно Интернет играет ключевую роль в процессе смены политических режимов. Автор верно замечает, что информационные технологии – не причина недовольства населения. Этот факт не вызывает сомнений. При этом суть Интернета в процессе дестабилизации политических режимов заключается в том, что он является инструментом политической мобилизации, цель которой – демонстрация гражданам проблем бытовой, социальной и политической жизни. В качестве защиты данной позиции можно привести пример, что протесты с использованием Интернет-технологий политической мобилизации проходят в государствах с различным социально-политическим состоянием: например,

---

[42] Сундиев И.Ю., А. Смирнов. М.: Русский биографический институт, Институт экономических стратегий, 2016. – 433 с.; Танина М.А., Юрасов И.А., Юдина В.А., Зябликова О.А., Юрасова О.Н. Цифровой протест в провинциальных городах России: структура, дискурс, модели. Пенза, 2021. – 124 с.; Шульц Э.Э. Технологии управления радикальными массовыми формами социального протеста в политической борьбе. М., 2018. – 248 с.; Etzioni A. The Active Society. A Theory of Societal and Political Processes. L., 1968.

[43] Mathis D., Grace H. Chronicling Civil Resistance. Washington, DC, 2021. Pinckney J. How to Win Well Civil Resistance Breakthroughs and the Path to Democracy. Washington, DC, 2021

[44] Наим М. Конец власти. От залов заседаний до полей сражений, от церкви до государства: почему управлять сегодня нужно иначе // Corpus, 2016; С. 29-30.

движение «желтых жилетов» в Париже и государственный переворот на Украине в 2014 году. Несмотря на различный социальный уровень граждан одной и другой территории, и те, и другие выходят на улицы с желанием дестабилизировать работу властей. В тот же самый момент на политической карте мира существуют государства с куда более низким уровнем жизни, нежели в указанных государствах, но за которыми не замечено активных протестных действий среди населения. Данный факт может поставить под сомнение тезис, согласно которому лишь уровень жизни играет ключевую роль в процессе дестабилизации политической жизни государства. Автор отрицает само существование феномена политической мобилизации, приводя указанное выше мнение.

Также к противникам тезиса эффективности Интернета в вопросе консолидации общества в политической борьбе можно отнести сторонников теории слактивизма. Главной идеей теории является тезис, что социальные сети не предполагают перехода протеста от виртуального состояния в реальное. Пользователи действительно заходят на протестные страницы в социальных сетях, активно участвуют в их жизни, однако в реальных политических акциях участия не принимают. Более того, социальные сети позволяют органам государственной власти выявлять и ликвидировать лидеров протеста, которые несут в себе опасность для государства. Сторонниками данных идей являются Е. Морозов[45] и З. Бауман[46]. Такая позиция неоднозначна. С одной стороны, безусловно, не все акции, организуемые через средства виртуальной среды, в дальнейшем переходят в реальный мир, а у властей действительно появляются рычаги воздействия на политических лидеров благодаря Интернету. Однако можно найти множество примеров, когда этот тезис не подтверждается. Рассматривая пример революции в Египте в 2011 году, можно заметить, что оба тезиса

[45] Morozov E. The Net Delusion: The Dark Side of Internet Freedom. – NY: PublicAffairs, 2012.
[46] Бауман З. Способны ли Facebook и Twitter помочь распространению демократии и прав человека? // Русский журнал. 2013 [Электронный ресурс]. URL: http://russ.ru/Mirovaya-povestka/Sposobny-li-Facebook-i-Twitter-pomoch-rasprostraneniyu-demokratii-i-prav-cheloveka (дата обращения: 02.02.2022)

авторов опровергаются реальными примерами. Во-первых, именно благодаря Интернету стала известна информация об убийстве молодого человека в Александрии органами правопорядка, что стало катализатором процесса политической мобилизации. Далее, опять же, благодаря протестным группам в социальных сетях, удалось организовать реальные политические акции в разных городах Египта и проводить их не один раз, а с относительной периодичностью. Кроме того, следует отметить, что в Египте времен Хосни Мубарака роль полиции и силовых структур была крайне высока, однако это не помешало Ваэлю Гониму – анонимному администратору протестной группы в социальной сети Facebook[47] – реализовать план политической дестабилизации и сыграть свою роль в революционных событиях 2011 года[48].

При этом важно обратить внимание на тот факт, что политическая мобилизация, как и ее разновидность в виде мобилизации в онлайн-пространстве, могут приносить государству пользу. С помощью таких технологию государства проводят агитацию по участию в выборах, выражение своей воли членами гражданского общества. Или же призывают людей участвовать в политических акциях в поддержку общегосударственных задач, митингов в поддержку политики государства. Использование политической мобилизации в позитивных целях позволяет сформировать или укрепить идентичность общества.

Приведенный выше анализ исследований, посвященных виртуальным технологиям конфликтной мобилизации свидетельствует о наличии противоположных подходов к восприятию этого феномена. Если одни исследователи воспринимают его, как настоящую угрозу, то другие придерживаются мнения, что интернет-технологии конфликтной мобилизации – исключительно инструмент и никакой опасности сами по себе не представляют. Одной из задач данной работы является описание феномена

---

[47] Социальные сети «Instagram» и «Facebook», принадлежащие компании Meta Platforms, признаны экстремистскими организациями и запрещены на территории России согласно решению Тверского суда, г. Москва.

[48] Кинаш Ю.С. Роль СМИ и «новых медиа» в современных политических конфликтах (на примере «Арабской весны» и Ливии): дис. канд. полит. наук: 23.00.06. - Москва, 2017. - 169 с.

конфликтной мобилизации в интернет-пространстве, как источника угрозы государственного суверенитета. Для достижения поставленной цели автор предлагает рассмотреть анализируемый феномен с позиций теории «секьюритизации». Согласно авторам данной теории, представляющим Копенгагенскую школу политической науки, для оценки того или иного явления в качестве угрозы, необходимо общественное одобрение такого восприятия. То есть само общество должно выработать единый подход по оценке феномена конфликтной мобилизации в онлайне, заключающийся в том, что инструменты этого феномена, имеющие признаки манипулятивного воздействия, несут экзистенциональную угрозу гражданам государства. Достижение такой общественной оценки позволит перейти к реализации конкретных мер противодействия этой угрозе. В случае же, если в обществе отсутствует консенсус в части указанного вопроса, то и попытки реализации программы противодействия ему будут неэффективны. Последующий анализ реальных примеров применения интернет-технологий конфликтной мобилизации, а также анализ текущего состояния программы противодействия им, применяемой Российской Федерацией, несет в себе задачу объяснения имеющихся угроз и рисков сферы информационной безопасности. Благодаря такому анализу возможно формирование интерпретационных моделей, необходимых для восприятия феномена конфликтной мобилизации в интернете обществом, как источника угроз.

Изучение интернет-технологий конфликтной мобилизации – актуальное направление в политологии и конфликтологии. Исследование этой темы включает в себя сразу несколько вопросов: действительно ли такие технологии эффективны в рамках конфликтной мобилизации населения, какие существуют разновидности данных технологий, как именно они влияют на решение пользователей участвовать в реальном политическом протесте. Поляризация мнений исследователей по этому вопросу связана с тем, что сам феномен интернет-технологий конфликтной мобилизации – молодое явление, существующее не более четверти века. Также проблемой

для понимания эффективности подобных технологий является их прямая зависимость от целого ряда факторов: среды их применения, причин применения, уровнем лояльности населения, качеством оппозиционных сил и т.д. Несмотря на наличие полярных подходов к вопросу эффективности интернет-технологий конфликтной мобилизации, можно, тем не менее, констатировать их наличие и их применение в политических акциях, проводимых по всему миру. Сам этот факт определяет необходимость и важность продолжения изучения этих технологий с целью поиска ответов на указанные выше вопросы.

Отдельно стоит отметить и ненасильственные технологии организации протестов. Они реализуются акторами посредством интернета, социальных сетей, а также традиционных СМИ. Одним из идеологов подобных ненасильственных механик реализации протестного сценария является Джин Шарп[49]. Согласно его подходу, существует 198 различных методов проведения ненасильственных акций, которые могут быть использованы для достижения политических, социальных и экономических изменений. Он исследует широкий спектр тактик и стратегий, которые люди могут использовать в борьбе против представителей порядка.

Шарп разделяет методы ненасильственных акций на три основные категории:

1. Процессы социального взаимодействия. Эти методы включают петиции, обращения, письма, декларации, речи, публичные митинги и другие формы выражения общественного мнения. Они направлены на обращение к обществу, правительству и другим сторонам, чтобы привлечь внимание к проблеме и вызвать реакцию противоположной стороны.

2. Методы экономического давления. Здесь рассматриваются методы, связанные с экономическими санкциями, бойкотами, забастовками, голодовками и т.д. Целью этих методов является давление на экономические

[49] Шарп Д. Политика ненасильственных действий. – 1973.

системы, предприятия или организации, чтобы достичь требуемых изменений.

3. Методы политического неповиновения. В этой категории рассматриваются такие методы, как гражданское неповиновение, отказ от уплаты налогов, отказ от сотрудничества с властями, уход в подполье и другие формы протеста, направленные на политические системы и власть.

Подобная классификация технологий протестного политического участия граждан применима и в случае интернет-технологий конфликтной мобилизации. Однако ее отличительной особенностью остаются форматы и механики реализации этих технологий. В связи с этим сохраняется актуальность формирования классификации интернет-технологий конфликтной мобилизации.

1.4. Классификация и типология технологий конфликтной мобилизации в интернет-пространстве

Определив специфику протестной активности в интернете, важно понять, как именно создается виртуальная протестная политическая толпа, и как она выводится на улицы городов. Реализуется этот сценарий с помощью определенных технологий, направленных на принятие человеком решения о своем политическом участии. Точное число таких технологий посчитать не представляется возможным, поэтому наиболее эффективный путь – предложить классификацию таких технологий, попытавшись охватить большинство из них.

В первую очередь, нужно разделить технологии конфликтной политической мобилизации на категории, исходя из того, на какой именно площадке в интернете они реализуются.

Наиболее популярными площадками в российском интернете являются следующие ресурсы: Youtube, Вконтакте, Одноклассники, Facebook[50] Telegram, WhatsApp, Viber, Instagram[51]. Можно сделать разделение этих сетей по следующим категориям: классические социальные сети (Вконтакте, Одноклассники, Facebook), видеохостинги (Youtube), мессенджеры (WhatsApp, Viber, Telegram) и медиасоцсети (Instagram, TikTok). Данное разделение необходимо для определения, какие технологии протестной мобилизации используются на каждой из приведенных

[50] Социальная сеть «Facebook», принадлежащая компании Meta Platforms, признана экстремисткой и запрещена на территории России согласно решению Тверского суда, г. Москва.
[51] Социальная сеть «Instagram», принадлежащая компании Meta Platforms, признана экстремисткой и запрещена на территории России согласно решению Тверского суда, г. Москва.

платформ. Классические социальные сети представляют собой наиболее функциональную площадку, так как их возможности обширны и эффективны. В них могут создаваться группы, публиковаться фото и видео контент, проводиться опросы, назначаться мероприятия, создаваться обсуждения и т.д. Характерными особенностями социальных сетей является то, что в них используются технологии территориальных сетей. В качестве примера можно привести протестные группы пользователей (рис. 1), выступавших против завоза твердых бытовых отходов из Москвы в Архангельскую область[52]. Технологи протеста создали целую сеть групп с похожим названием, одним оформлением, но с четкой территориальной привязкой, обеспечивающей большее внимание к группе со стороны местных

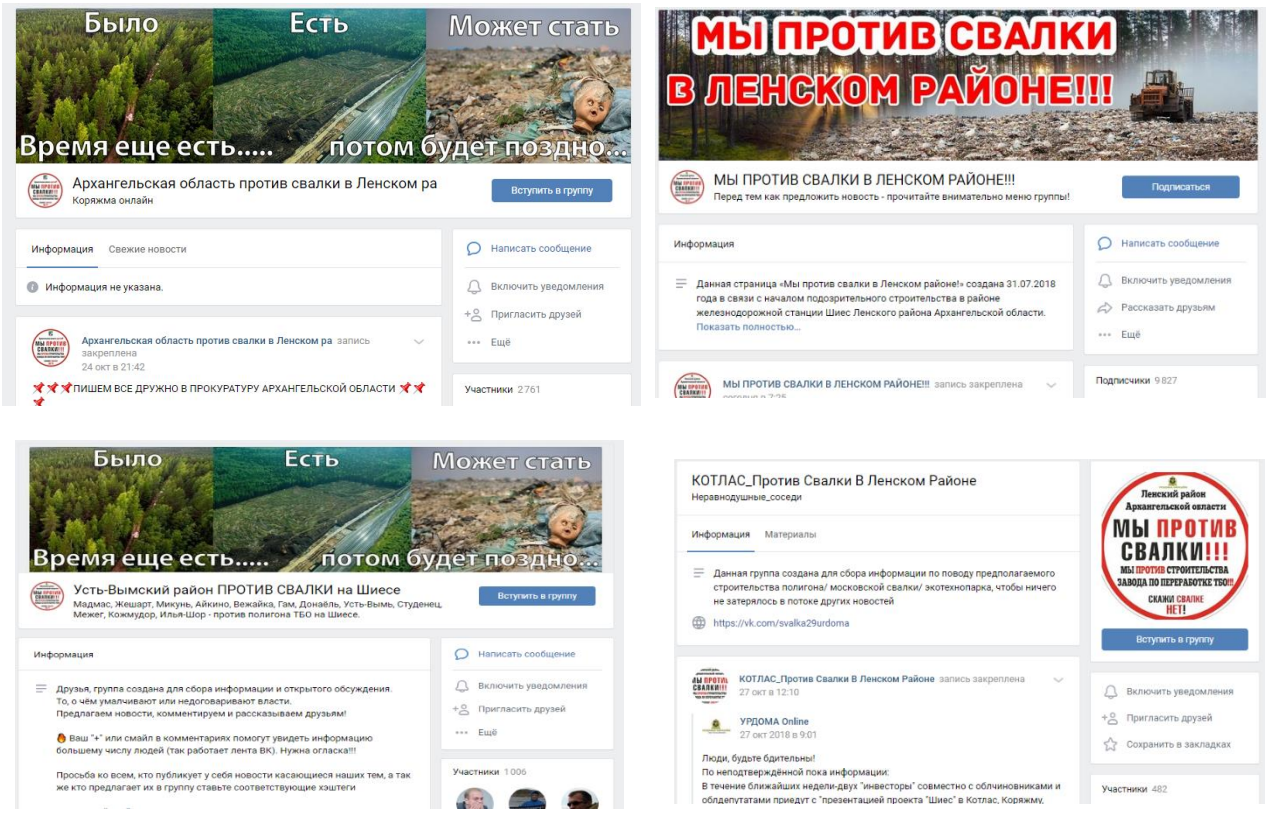

Рисунок 1

жителей.

[52] Бубнов А.Ю., Козлов С.Е. Политический активизм в социальных сетях (на примерах Москвы, Екатеринбурга и Шиеса) // Журнал политических исследований. - 2021. - Т. 5. - № 1. - С. 54-64.; Шаматонова Г.Л., Майоров В.О. Экологические протесты как форма проявления гражданской активности // Социальные и гуманитарные знания. - 2019. Т. 5. - № 3 (19). - С. 200-207.; Демчук А.Л. Политика регулирования экологических конфликтов: концептуальные основы и национальные модели: дис. д-р. полит. наук: 23.00.06. - Москва, 2020. - 565 с.

Точно такой же прием был использован оппозиционером Навальным А.А. во время выборов президента РФ в марте 2018 года, когда практически в каждом субъекте РФ была группа, посвященная деятельности данного оппозиционера. Использование этой технологии эффективно, так как она позволяет децентрализовать протест. В каждой группе есть свой администратор – организационный лидер, который занимается региональными вопросами. Территориальная сеть позволяет привлекать больше людей на локальном уровне, освобождает от этой функции центральное ядро протеста. Помимо Навального А.А.[53], таким методом пользовался Грудинин П.Н. – кандидат на должность президента РФ во время выборов в марте 2018 года[54].

Видеохостинги, в отличие от социальных сетей, обладают более скромной палитрой возможностей, однако ими не стоит пренебрегать[55]. На них публикуются фильмы, видеоматериалы, прямые трансляции различных событий. Существует возможность создания канала, который действует точно также, как и классический выпуск новостной телепередачи по телевизору. Большое количество людей узнают новости через подобные каналы. Помимо информирования ведущие онлайн-передач предоставляют аналитику новостей, которая позволяет сформировать у пользователей необходимую позицию. В качестве примера, можно вновь обратиться к оппозиционеру Навальному А.А. и его Youtube программе «Навальный Live» (организация «ФБК», владеющая каналом, признана в России экстремисткой). На канале существовало несколько рубрик со своими

---

[53] Полтерович В.М. Кризис институтов политической конкуренции, Интернет и коллаборативная демократия // Вопросы экономики. - 2021. - № 1. - С. 52-72

[54] Голосов В. Ю. Предвыборная кампания и результат кандидата в президенты Грудинина Павла Николаевича на президентских выборах во Владивостоке // Известия Восточного института. 2018. №3 (39). URL: https://cyberleninka.ru/article/n/predvybornaya-kampaniya-i-rezultat-kandidata-v-prezidenty-grudinina-pavla-nikolaevicha-na-prezidentskih-vyborah-vo-vladivostoke (дата обращения: 24.04.2022).

[55] Марин Е.Б. Представление о социальном протесте у молодежи российского Дальнего Востока // Вестник Института социологии. - 2021. - Т. 12. - № 1. - С. 62-92.; Пономарев Н.А., Балтодано У.А.С, Нешков С.В., Майлис А.А. Организация инфраструктуры протестных акций (на материалах Евромайдана) // Информационные войны. - 2018. - № 2 (46). - С. 51-56.; Рустамова Л.Р., Барабаш Б.А. Информационное воздействие в эпоху «постправды» и «фейк-ньюс» // Вопросы политологии. - 2018. - Т. 8. - № 5 (33). - С. 23-30.

ведущими. Наиболее популярной рубрикой была рубрика «Россия будущего», ролики которой набирали восемьсот-девятьсот тысяч просмотров. Вел ее сам оппозиционер. Такая технология помогает создать качественную политическую толпу, которая участвует в протесте не просто ради развлечения или под действием других неполитических факторов, а идет на протест осознано, преследуя вполне определенные политические цели.

В основе технологий политической мобилизации через мессенджеры лежит другая составляющая. В основном, эти площадки нужны для координации действий, быстрой связи, а в отдельных случаях используются в случае блокировки других ресурсов. Так было в Китае в 2014 год во время протестов в Гонконге[56]. Власть заблокировала не просто интернет, но и всю мобильную сеть в регионе. Тем не менее, люди нашли новый способ общения с помощью мессенджера Firechat[57], использующего для работы не Интернет, а локальную сеть, к которой можно подключаться с помощью Wi-Fi, либо Bluetooth. Сеть такого рода заблокировать сложнее. В некоторой степени именно этот фактор обусловил победу демонстрантов, добившихся отмены непопулярного законопроекта. Пользователям приходят сообщения, однако не создается эффекта массовости, за счет которого пропадает субъектность протеста[58]. В связи с этим снижается эффективность технологий. Однако ключевым преимуществом являются скорость и адресная доставка сообщений конкретным пользователям.

---

[56] Зверев А. Л., Федоров А. П. Социальные сети как инструмент политического манипулирования (на примере организации массовых протестов в Гонконге 2014 г.) // Вестник БГУ. - 2015. - №7. URL: https://cyberleninka.ru/article/n/sotsialnye-seti-kak-instrument-politicheskogo-manipulirovaniya-na-primere-organizatsii-massovyh-protestov-v-gonkonge-2014-g (дата обращения: 24.04.2022).

[57] Салицкий А.И., Виноградов А.В. Гонконгское противостояние: внутренняя динамика и внешние аспекты // Контуры глобальных трансформаций: политика, экономика, право. - 2021. - Т. 14. - № 1. - С. 135-150.

[58] Азаров А.А., Бродовская Е.В., Дмитриева О.В., Домбровская А.Ю., Фильченков А.А. Стратегии формирования установок протестного поведения в сети Интернет: опыт применения киберметрического анализа (на примере Евромайдана, ноябрь 2013). Часть I // Социология Интернет и новых технологий. 2014. - № 2. - С. 63 – 78. Гаврилов С.Д., Морозов С.И. Стратегии коммуникации в публичном политическом пространстве России: от интеграции до протеста // Право и политика. - 2021. - № 2. - С. 25-34.; Гасанова В.С. Социальные сети как инструмент управления протестными акциями // Информационные войны. - 2021. - № 1 (57). - С. 46-47.

Медиасоцсети или микроблоги (например, Twitter) используются, как помощники классических социальных сетей[59]. В них публикуются фото и видео материалы относительно какого-либо события, дополненные личным мнением пользователей. Ключевой особенностью данных площадок являются хэштеги – слова или фразы со знаком «#», которые позволяют найти все сообщения с запрашиваемым словом. Эти площадки используются для получения информации от очевидцев, участников политических акций. Так, например, во время событий на Украине в 2013-2014 годах особой популярностью пользовался хэштег #Euromaidan. Пользователи публиковали видео и фото с площадей, которые потом попадали на страницы популярных СМИ. С помощью хэштегов люди со всего мира могут оперативно посмотреть, что происходит в другом государстве и на основе этого выработать собственное мнение. Однако такой подход к анализу политических событий может оказаться неправильным. С помощью «ботов» - искусственных пользователей – технологи формируют картинку, зачастую не имеющую ничего реального. Подобную картину можно было наблюдать во время митингов в Белоруссии[60] (рис. 2).

Рисунок 2 - однотипные посты ботов в социальной сети «Twitter» по поводу митингов в Белоруссии

[59] Стукал Д.К., Беленков В.Е., Филиппов И.Б. Методы наук о данных в политических исследованиях: анализ протестной активности в социальных сетях // Политическая наука. - 2021. - № 1. - С. 46-75.; Сулейманова Ш.С. Роль средств массовой информации и новых медиа в межнациональных и межконфессиональных конфликтах // Вопросы национальных и федеративных отношений. - 2018. - Т. 8. - № 3 (42). - С. 178-190.; Сухов А.Н. Последствия деструктивных социальных конфликтов: историко-практический аспект // Вестник Московского университета МВД России. - 2021. - № 2. - С. 323-326.

[60] Бродовская Е.В., Давыдова М.А., Еремин Е.А. Пролонгированные политические протесты в России и в Республике Беларусь летом-осенью 2020 года: референтность российской аудитории социальных медиа // Гуманитарные науки. Вестник Финансового университета. - 2021. - Т. 11. - № 1. - С. 6-13.

Следующим критерием классификации интернет технологий политической мобилизации может быть субъектность. Можно выделить 2 варианта субъектности: открытая и скрытая. При открытой субъектности существует конкретная группа в социальных сетях или страница на видеохостингах, микроблогах, которая является субъектом протеста[61]. С помощью этой страницы координируют действия протестующих, популяризируют оппозиционных политических лидеров, объединяют пользователей и т.д. Задачей технологий протестной мобилизации при открытой субъектности является мобилизация граждан вокруг конкретной политической силы[62]. В случае скрытой субъектности преследуется другая задача – снижение уровня доверия к власти, ее институтам, фрустрация пользователей, политическая атака на представителя власти и т.д. В случае скрытой субъектности отсутствует единый источник контента – публикации появляются на популярных развлекательных страницах. К такому типу технологий можно отнести так называемые «вирусные видео». Они быстро распространяются по сети, вызывая у пользователей необходимые технологам чувства. Также примером технологий такого типа можно назвать рекламу в социальных сетях. Именно так, по мнению американских политологов, Россия вмешивалась в выборы президента США в 2016 года[63].

Третьим критерием классификации технологий протестной мобилизации является радиус воздействия. Технологии можно разделить на те, которые действуют на определенную локацию, территорию, сегмент интернета, и те, которые направленны на все государство, либо даже на весь мир. Отличать эти виды технологий друг от друга достаточно просто. Во-

---

[61] Ушкин С.Г. Вовлеченность пользователей социальных сетей в протестное движение // Власть. - 2014. - № 8. - С. 138 – 142

[62] Гаврилов С.Д. «Новые протесты» как состояние социально - политической реальности в отражении россиян // Прорывные научные исследования как двигатель науки. Сборник статей Международной научно-практической конференции. Уфа, 2021. С. 184-186.; Дмитриев С.С. Цифровая мобилизация: новые механизмы и возможности политического управления // Управленческое консультирование. - 2021. - № 2 (146). - С. 18-25

[63] Россия покупала рекламу в Facebook // ТСН URL: https://ru.tsn.ua/svit/rossiya-pokupala-reklamu-v-facebook-no-vliyanie-na-vybory-v-ssha-bylo-neznachitelnym-gendirektor-avast-1009110.html (дата обращения: 01.03.2022).

первых, необходимо обратить внимание на площадку. Если это международная социальная сеть, а не локальная (например, Facebook[64]), то очевидно, что целевой аудиторией контента являются не только граждане РФ, но и международное сообщество[65]. Во-вторых, следует обратить внимание на язык публикации: если пост опубликован не только на местном языке, но и на английском, то очевидны и цели такой публикации. Для примера предлагаем вновь обратиться к ситуации с вывозом мусора в Архангельскую область, на запроектированный полигон ТБО «Шиес», находящийся рядом с поселком городского типа Урдома. Вот так выглядит описание видеоролика, подготовленного активистами[66] (рис. 3).

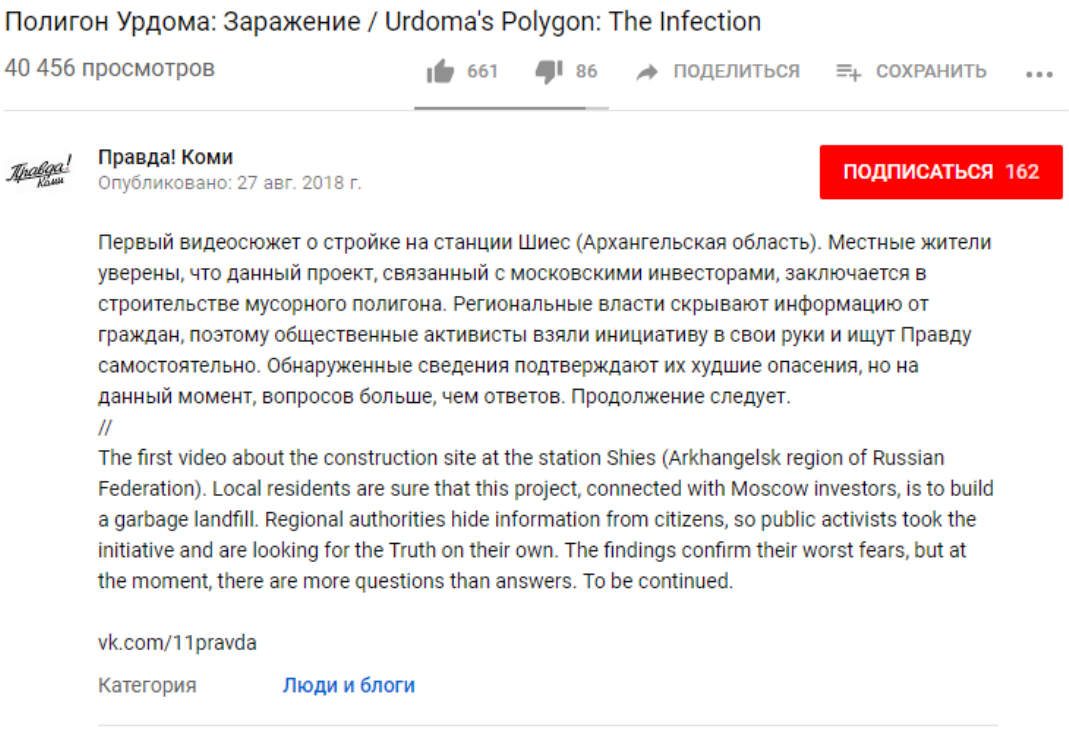

Рисунок 3

---

[64] Социальные сети «Instagram» и «Facebook», принадлежащие компании Meta Platforms, признаны экстремистскими организациями и запрещены на территории России согласно решению Тверского суда, г. Москва.

[65] Хабекирова З.С. Стратегия дискредитации и приемы ее реализации в политическом дискурсе демократической оппозиции // Вестник Адыгейского государственного университета. Серия 2: Филология и искусствоведение. - 2011. - № 2. - С. 138 – 144.; Челышева С.Д., Эльтикова Е.А. Социальные сети как инструмент политических манипуляций // Современные тенденции и технологии развития потенциала регионов. Сборник статей Национальной научно-практической конференции. Санкт-Петербург, 2021. - С. 40-43.

[66] Полигон Урдома: Заражение / Urdoma's Polygon: The Infection // Youtube URL: https://www.youtube.com/watch?v=POdsOHtV90o&t=262s (дата обращения: 01.03.2022).

Видно, что целью публикации были не только жители Республики Коми и Архангельской области, но и международное сообщество.

Также критерием классификации может быть время воздействия. Технологии могут быть направлены на краткосрочные результаты, или же быть частью долгосрочного плана. В частности, если контент способствует формированию критического восприятия пользователями органов власти, но при этом в его раскрутке отсутствует яркое событие, то есть нет достаточного информационного повода, то очевидно, были применены технологии, запущенные еще заранее и рассчитанные на перспективу. Они необходимы для того, чтобы вызвать постоянное чувство фрустрации и неудовлетворенности объектом мобилизации у пользователей. Целью технологий, рассчитанных на быстрый результат, является быстрая мобилизация пользователей. Она применяется не только тогда, когда случается какое-то событие, вызывающее общественный резонанс, но и на последних этапах реализации сценариев протестных политических акций. Именно такие технологии необходимы для того, чтобы вывести людей на улицу.

Еще одним критерием можно назвать акторов технологий политической мобилизации. Акторами технологий политической мобилизации являются авторы и организаторы протестных активностей в виртуальном пространстве. К ним относятся и «конечные заказчики», интересанты протестной активности, а именно политические силы или представители бизнеса, взаимодействующие с пользователями социальных сетей через администраторов групп, чатов и каналов в мессенджерах и социальных сетях. Существенное воздействие на пользователей оказывают и комментарии к опубликованным постам. Исследования показывают, что люди доверяют комментариям даже больше, чем самой информации в посте[67]. Это создает большие возможности для технологов политической

[67] How reading online comments affects us // Social media psychology URL: https://socialmediapsychology.eu/2016/10/05/onlineandsocialmediacomments/ (дата обращения: 01.03.2022)

мобилизации и для тех, кто оппонирует им. Так, например, в современных примерах информационных войн часто используются «боты» - фейковые аккаунты, созданные технологами с исключительно одной целью – оставлять комментарии в группах и сообществах в социальных сетях. Безусловно, вычислить такие аккаунты не представляет никакой сложности (стоит обратить внимание на время создания страницы, количество информации о пользователе, аватарку, группы, в которых состоит пользователь, чтобы сделать вывод – реальный это аккаунт или искусственный), но немногие люди всегда анализируют тех, кто оставляет комментарии.

Таким образом, выделены 5 критериев классификации интернет-технологий политической мобилизации. В ходе реализации сценариев политических акций, безусловно, используются сразу многие виды данных технологий. Однако классификация этих инструментов позволяет понять, с какой целью используется та или иная технология и в итоге определить, какой план поставили перед собой технологи протестов.

В качестве примера такого плана можно привести анализ технологической кампании по реализации сценария цветной революции.

Цветная революция - это технологии организации государственного переворота в условиях искусственно созданной политической нестабильности, в которых давление на власть оказывается в форме политического шантажа, а инструментом шантажа выступает молодежное протестное движение, организованное по специальной схеме[68]. «Цветные революции» реализуются, как и любой другой проект, с привлечением ресурсов. К таким ресурсам можно отнести финансовые, кадровые, административные. Доступ к финансам у технологов данной политической акции имеется через некоммерческие организации, фонды, международные организации. Кадры же проходят специальную подготовку, во время которой людей обучают поведению в толпе (учат быть лидерами толпы, управлять

[68] Манойло А.В., «Цветные революции и технологии демонтажа политических режимов» // NotaBene URL: e-notabene.ru/wi/article_12614.html (дата обращения: 02.02.2022)

ею), а также работе в СМИ и Интернете. Административные ресурсы заключаются в способности технологов и заказчиков найти выходы и договориться с лицами, принимающими решения на высоком политическом уровне внутри страны: видные политики, чиновники высшего звена, лица, замещающие политические должности и т.д. Данные элементы необходимы для создания организационной «архитектуры» проекта «цветной революции». Далее технологи начинают заниматься привлечением людей. С этой целью они начинают активно работать со СМИ и Интернетом, которых вместе принято называть средствами массовой коммуникации (СМК)[69].

Перед СМК ставится задача дестабилизировать обстановку в стране, заставить людей чувствовать некомпетентность правительства, его несостоятельность. При этом используются определенные инструменты:

1. Во-первых, это демонстрация более высоких жизненных стандартов в странах «Запада», что приводит к фрустрации населения и заставляет их усомниться в правильности действий власти.

2. Во-вторых, теле- или радиоэфир заполняется сюжетами противостояния малых групп, борющихся за свои права и авторитарных организаций, что дает населению пример, как действовать.

3. В-третьих, крупные новостные ленты формируют и распространяют информационные сообщения, которые создают альтернативную картину происходящего, в угоду контролирующих эти СМК сил.

Таковы основные инструменты воздействия СМК на население в предреволюционный период. Однако их деятельность не прекращается и во время революции. На этом этапе перед ними ставятся другие цели:

1) Активировать массовое сознание.

---

[69] Манойло А.В. «Фейковые новости» как угроза национальной безопасности и инструмент информационного управления // Вестник Московского университета. Серия 12: Политические науки. - 2019. - № 2. - С. 37-45.; Манойло А.В. Цепные реакции каскадного типа в современных технологиях вирусного распространения «фейковых новостей» // Вестник Московского государственного областного университета. - 2020. - № 3. - С. 75-107.; Манойло А.В., Попадюк А.Э. Зарубежные научные подходы к исследованию «фейковых новостей» в мировой политике // Россия и современный мир. - 2020. - № 2 (107). - С. 285-300.

2) Удерживать сторонников в этом состоянии «до победного конца».

3) Легитимировать революционные действия для внутренней и внешней аудитории.

4) Легитимировать новых лиц в качестве новой власти.

Таким образом, видим, что СМИ и интернет используются во время цветных революций с информационной и пропагандисткой функциями. Без них проведение искусственной революции невозможно.

Данные технологические подходы к организации цветных революций или иных протестных акций коррелируют с видами манипуляционных активностей, предложенных С.В. Володенковым:

- внедрение под видом «объективной информации» контента, необходимого субъекту политического управления и формирование у пользователей «собственного» мнения и отношения к различным политическим событиям.

- воздействие на эмоциональную сферу целевых аудиторий для повышения социальной напряженности и дестабилизации политической ситуации.

- перефокусировка общественного внимания на «выгодные» для субъекта политического управления темы.

- формирование альтернатив для создания в сознании целевых групп иллюзии выбора или действия.

- внедрение в общественное сознание различных социально-политических стереотипов и установок.

- подмена собственных целей объекта воздействия целями манипулятора.

Этапы организации конфликтной мобилизации в онлайн-пространстве предполагают применение лишь некоторых из этих манипулятивных методов. Так, воздействие на эмоциональную сферу достигается путем демонстрации «лучшей» жизни в других странах мира и утверждению, что их

модель государственного управления является единственно правильной для достижения высокого уровня жизни. Формирование альтернатив для создания в сознании пользователей иллюзии выбора действия происходит за счет демонстрации, что часть общества уже борется за ценности, позволяющие добиться перехода на тот путь развития, который придерживаются «лучшие» государства. Перефокусировка общественного внимания на выгодные для политического актора темы достигается за счет создания альтернативной структуры интерпретаций происходящих событий. Пользователи к постепенно утрачивают доверие к традиционным средствам массовой информации или их страницам в социальных сетях, и им предлагают альтернативный источник новостей, который в реальности использует целый набор манипулятивных методов формирования и демонстрации контента.

В то же время, этапы организации конфликтной мобилизации в интернете предполагают быстрое развитие конфликта в виртуальном пространстве и его выход в офлайн. Для этого многие из видов манипулятивного воздействия смешиваются друг с другом и одна тема публикуемого контента одновременно включает в себя несколько видов цифровой манипуляции.

Таким образом, был выделен алгоритм формирования протеста в онлайн-пространстве, учитывающий выявленные исследователями виды манипулятивных активностей.

1.5. Новые вызовы и угрозы национальной безопасности Российской Федерации в сфере интернет-технологий конфликтной мобилизации и управления протестом

Инструменты и интернет-технологии конфликтной мобилизации являются источником потенциальных угроз для национальной безопасности Российской Федерации. Под национальной безопасностью понимается состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны[70].

Также важно определить термин угроза национальной безопасности, так как рассматривать феномен интернет-технологий конфликтной мобилизации приходится в том числе и в разрезе данного термина. Под угрозой национальной безопасности понимается совокупность условий, факторов, создающих прямую или косвенную возможность причинения ущерба национальным интересам Российской Федерации.

В Стратегии национальной безопасности Российской Федерации обозначен ряд проблемных вопросов, в которых столкновение интересов с иностранными государствами является препятствием для развития мирового

[70] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации».

сообщества[71]. В числе прочих значится и проблема обеспечения международной информационной безопасности[72]. При этом для Российской Федерации одним из приоритетов, выраженных в национальных интересах государства, является развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия[73].

Стратегия национальной безопасности Российской Федерации также объясняет, какие именно угрозы включает в себя тема информационной безопасности. Это, в первую очередь, размещение материалов террористических и экстремистских организаций в сети Интернет, призывы к массовым беспорядкам, осуществление экстремистской деятельности, участие в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, совершение самоубийства, пропаганда криминального образа жизни, потребление наркотических средств и психотропных веществ. Объектом воздействия же перечисленных выше угроз является молодежь[74].

Следует раскрыть приведенные угрозы, представив их в конкретных примерах, послуживших причиной включения их в этот список. Так, угроза распространения террористических и экстремистских материалов объясняется эффектом запугивания граждан страны или пропагандой сомнительных идеалов на отдельных представителей населения. В качестве примера приведем видеоролик, созданный представителями так называемого «Исламского государства» (запрещенной в России террористической организации), созданный в формате видеообращения с угрозами в адрес

---

[71] Семченков А.С. Противодействие современным угрозам политической стабильности в системе обеспечения национальной безопасности России: дис. д-р. полит. наук: 23.00.02.. М., 2012. 304 с.; Сдельников В.А. Технологии формирования негативного имиджа России: дис. канд. полит. наук: 23.00.02. М., 2018. – 185 с.

[72] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»., С. 6

[73] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации».

[74] Фирсов А.В. Технологии поддержания политической стабильности в механизме обеспечения национальной безопасности: российский и зарубежный опыт: диссертация на соискание степени кандидата политических наук: 23.00.02. М., 2017. 166 с.

России и ее граждан и опубликованный на видеохостинге YouTube в августе 2016 года[75]. В этом видеоролике представители «Исламского государства» угрожали провести серию терактов в столице России и других крупных городах. Ролик активно обсуждался в социальных сетях, что оказывало планируемый террористами эффект на пользователей, посмотревших видео. Сама по себе возможность публикации подобного контента на самом популярном в мире видеохостинге вызывает опасения и требует вмешательства со стороны представителей законодательной власти Соединенных Штатов Америки, под юрисдикцию которых и включен YouTube.

Под призывами к массовым беспорядкам понимаются случаи пропаганды вооруженного или силового протеста с представителями силовых организаций Российской Федерации в том числе в социальных сетях. Российское законодательство обладает нормативными документами, разработанными для предотвращения и наказания за совершенное преступление, запрещающими призывы к массовыми беспорядкам, участие в них, а также призывы к насилию над гражданами. Данные нормативно-правовые акты представлены статьей 212 УК РФ. Всего по данной статье за актуальный период 2020 года пришлось тридцать четыре случая применения наказания, два из которых представлены в виде условного лишения свободы, а участники остальных кейсов получили уголовное наказание в виде лишения свободы.[76]

Проведение мероприятий в нарушении установленных законом правил является административным нарушением, регламентируемым статьями 19.3 ч.1 Кодекса об Административных правонарушениях Российской Федерации и 20.2 КоАП РФ. Опасность нарушения приведенных

[75] Уголовное судопроизводство. Данные о назначенном наказании по статьям УК // Судебная статистика РФ URL: stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17 (дата обращения: 20.02.2022).

[76] ИГ опубликовало видео с угрозами в адрес России // RBC URL: www.rbc.ru/politics/01/08/2016/579e6f5b9a7947cdb5cedc8a (дата обращения: 20.02.2022).

статей определяется следующими причинами, опубликованными на сайте-памятке от государственных органов Санкт-Петербурга[77]:

1. Ослабление способности к объективному восприятию реальности, т.к. называемый эффект «психологии толпы».

2. Уверенность отсутствия личной ответственности за происходящие на мероприятии.

3. Повышенный уровень агрессии, проявляющийся в связи с указанными выше факторами.

4. Опасность повторения действий других людей, участвующих в акции, выполнение призывов-команд, поступающих от организаторов и ведущих.

В результате участие в несанкционированных акциях происходят случаи излишне агрессивной реакции со стороны некоторых участников этих мероприятий, в последствие превращающиеся в уголовные дела.

Пропаганда совершения самоубийства также регламентируется российским законодательством в статье Уголовного Кодекса Российской Федерации № 110.1. «Склонение к совершению самоубийства или содействие совершению самоубийства». Серьезные наказание по данной статье тем не менее не останавливают отдельных граждан от организации системной работы по пропаганде совершения самоубийства, в том числе и среди несовершеннолетних граждан. Так, известным примером подобной работы является случай «игры» «Синий кит»[78], в рамках которой были созданы так называемые «группы смерти» в социальной сети Вконтакте: закрытые группы, вход в которые одобрялся только после проверки ее администратором, что пользователь действительно является несовершеннолетним гражданином. «Игра» шла по заранее спродюссированному сценарию, где участникам выдавались задания, связанные с нанесением физического вреда себе. Финальным заданием же

[77] Зовут поучаствовать в протестной акции? // Комитет по вопросам законности, правопорядка и безопасности URL: www.zakon.gov.spb.ru/advertisingsocial/mass-action.html (дата обращения: 20.02.2022).
[78] Синий кит (игра) // Wikipedia URL: ru.wikipedia.org/wiki/Синий_кит_(игра) (дата обращения: 20.02.2022).

являлось самоубийство. Несмотря на отсутствие проверенных данных о количестве случаев воздействия «игры» на детей и подростков, сама возможность организации подобных «игр» является недопустимой для сохранения тенденции развития Российской Федерации.

Пропаганда криминальной субкультуры ярко определяема на примере так называемого «движения АУЕ». В августе 2020 года данное движение было признано Верховным судом РФ экстремистским[79] и, как следствие, запрещено на территории Российской Федерации. В обосновании этого решения Генеральная прокуратору Российской Федерации обозначила, что «АУЕ является хорошо структурированной и управляемой организацией – молодежным движением экстремистской направленности. В рамках движения и в его интересах участниками АУЕ совершались экстремистские правонарушения, а также массовые беспорядки». После формирования такого решения Верховным судом депутаты Государственной Думы предложили укрепить текущее законодательство запретом на пропаганду криминальной субкультуры. Законопроект № 1009841-7 был внесен в Государственную Думу РФ 18.08.2020 года с пояснительной запиской, что подобные движения несут две угрозы для сохранения стабильного развития Российской Федерации, а именно: пропагандируют криминальные ценности и культивируют ненависть к представителям правоохранительных органов и судов. Запрет же подобных движения позволил защитить несовершеннолетних от негативного воздействия и вовлечения в совершение преступлений, укреплению состояния законности на территории исправительных учреждений и исправлению осужденных лиц и сформирует предпосылки для усиления эффективности правоохранительной системы Российской Федерации. Тем не менее, законопроект принят не был[80].

---

[79] Верховный суд признал экстремистским движение "АУЕ" // ТАСС URL: tass.ru/obschestvo/921776 (дата обращения: 20.02.2022).

[80] Законопроект # 1009841-7 О внесении изменений в Федеральный закон "Об основах системы профилактики правонарушений в Российской Федерации" и Федеральный закон "Об информации, информационных технологиях и о защите информации" в части реализации механизмов профилактики и противодействия распространению криминальных субкультур в Российской Федерации // Система

Пропаганда употребления наркотических средств и психотропных веществ также запрещена российским законодательством в статьях 230 УК РФ и 6.13 КоАП РФ. Особое внимание следует уделить п. «Д» ч. 2 ст. 230 УК РФ, предполагающей уголовное наказание для граждан, склоняющих пользователей сети интернет к употреблению наркотических веществ. Всего по части 2 статьи 230 УК РФ за период 2020 года было осуждено десять граждан, семь из которых получили реальные сроки, а трое понесли условное наказание.

Таким образом, стоит отметить, что те угрозы, которые приведены в Стратегии национальной безопасности Российской Федерации, действительно встречаются в жизни граждан страны и требуют от государства системной работы по их недопущению в будущем. Особенно актуальна данная проблематика становится при определении источником этих угроз иностранных государств, так как это само собой подразумевает системную работу этих стран по дестабилизации социально-политической ситуации в Российской Федерации.

Для обеспечения борьбы с данными угрозами Стратегия национальной безопасности предлагает следующие шаги. Их можно разделить на 3 группы:

1. Противодействие технологическим способом: повышение уровня защищенности информационной инфраструктуры и предотвращения деструктивного воздействия на нее, развитие технологий искусственного интеллекта и квантового вычисления.

2. Противодействие случаям с влиянием человеческого фактора: снижение до минимально возможного уровня количества утечек информации, снижение эффективности технической разведки силами иностранных государств.

обеспечения законодательной деятельности URL: sozd.duma.gov.ru/bill/1009841-7 (дата обращения: 20.02.2022).

3. Развитие социально-юридической инфраструктуры: обеспечение защиты прав и свобод человека при обработке персональных данных, установление международного правового режима обеспечения безопасности в сфере использования ИКТ, доведение до российской и международной общественности достоверной информации о внутренней и внешней политике РФ.

Широкий набор направлений деятельности государства для обеспечения безопасности от информационных угроз свидетельствует о понимании представителями государственных органов и лиц, замещающих государственные должности, глубины вопроса о серьезных последствиях в случае отсутствия контроля за этими угрозами.

Современные условия на международной политической арене, а именно, продолжающаяся гибридная война против России со стороны ряда стран, безусловно, будут иметь отражение в части определения угроз национальной безопасности Российской Федерации. С начала проведения специальной военной операции 24 февраля 2022 года американские и европейские интернет-площадки усилили свое давление на Россию: формируют негативный образ государства, запрещают использование своих возможностей для граждан РФ, призывают к публичному осуждению обычных жителей и военных Российской Федерации. Такие действия являются подготовительной фазой для онлайн-удара: попытки проведения протестных акций на территории Российской Федерации с применением виртуальных технологий конфликтной мобилизации. Подготовительный этап определяется задачей сформировать у пользователей интернета, независимо от их гражданской принадлежности, негативный образ нашей страны – легитимировать дальнейшие действия в онлайн-пространстве против России. В таких условиях особое значение приобретают исследования в области

анализа угроз и поиска методов противодействия виртуальным технологиям конфликтной мобилизации[81].

Интернет-технологии конфликтной мобилизации могут применяться в большинстве приведенных в Стратегии национальной безопасности угроз. Однако наиболее очевидными направлениями их применения являются угрозы призыва к массовыми беспорядкам, осуществлению экстремистской деятельности и участие в массовых мероприятиях, проводимых с нарушением закона. Как было указано выше, основным объектом таких угроз, согласно Стратегии национальной безопасности, является молодежь.

Помимо рисков информационно-когнитивного характера, немаловажное значение имеют и задачи, связанные с обеспечением цифрового суверенитета, основанного на обладании аппаратно-функциональной инфраструктурой – «hardware», то есть оборудованием, и «software» - программным обеспечением. Нынешние цифровые разработки в большинстве случаев созданы на языках программирования, созданных за рубежом и поддерживаются оборудованием также иностранного производства. В связи с этим важно отметить риски, которые несет в себе данная ситуация.

Для этого приведем несколько примеров раскрытия так называемых «backdoors» - «дыр» программного кода или языка программирования, благодаря которым у заинтересованных акторов получалось обходить все политики безопасности и неправомерным путем овладевать информацией. Так, например, Heartbleed (2014), Shellshock (2014), Spectre (2018), Meltdown (2018).

Heartbleed — это ошибка безопасности, которая затронула библиотеку OpenSSL, широко используемое программное обеспечение, используемое для защиты веб-сервисов. Она позволила злоумышленникам получить доступ к конфиденциальной информации: именам пользователей, паролям и ключам

[81] Денисенко П. В., Есиев Э. Т. Интернет-технологии как инструмент политической мобилизации в эпоху big data // Вопросы политологии. - 2021. - № 4

шифрования с серверов, использующих уязвимую версию OpenSSL. Heartbleed воспользовался уязвимостью в реализации расширения OpenSSL heartbeat, которое предназначено для поддержания соединений. Злоумышленники могут отправить вредоносный запрос на уязвимый сервер, обманом заставив его раскрыть больше данных, чем следует, включая ценную информацию, хранящуюся в его памяти[82].

Другой инцидент, произошедший также в 2014 году, получил название Shellshock или Bash Bug. Относится к уязвимости в интерпретаторе командной строки Bash (Bourne Again Shell), используемом в системах на базе Unix. Уязвимость позволяла злоумышленникам выполнять отправлять запрос манипулируя переменными среды. Когда Bash обрабатывал эти переменные, он непреднамеренно выполнял внедренный код, открывая несанкционированный доступ к системе. Shellshock существенно навредил интернет-безопасности таких устройств как маршрутизаторы и устройства Интернета вещей (IoT). Воспользовавшись уязвимостью, злоумышленники смогли получить несанкционированный доступ, выполнить вредоносные команды и скопировать конфиденциальные данные.

Нельзя не упомянуть и случай, получивший название Spectre — это класс уязвимостей безопасности, которые используют конструктивные недостатки современных компьютерных процессоров, в том числе процессоров Intel, AMD и ARM. Ошибка позволила злоумышленникам получить доступ к конфиденциальным данным, используя функцию оптимизации производительности процессоров. Уязвимость Spectre представляла серьезную угрозу безопасности вычислительных систем на самых разных устройствах, включая компьютеры, смартфоны и облачные серверы. Аналогичным образом действовал и «backdoor» Meltdown, управляя самими процессорами.

---

[82] Durumeric, Z., Adrian, D., Mirian, A., Kasten, J., Bailey, M., & Halderman, J. A. (2014). The Matter of Heartbleed. In Proceedings of the 2014 ACM SIGCOMM Conference (pp. 475-486). ACM.

Такой обзор наиболее ярких «дыр» в программном коде демонстрирует важнейшую проблему: невозможно быть уверенным, что языки программирования, программное обеспечение и технологическое оборудование, произведенное за рубежом, не должно использоваться для обеспечения критически важных направлений деятельности государства, в первую очередь в оборонной и финансовой сферах.

Таким образом, вызовы и угрозы национальной безопасности Российской Федерации в сфере интернет-технологий заключаются не только в информационно-когнитивном воздействии на интернет-сферу государства, но в том программной обеспечении и технологическом оборудовании, которое используется в критически важных сферах для государства.

Выводы к главе I

Сетевая конфликтная мобилизация неразрывно связана с феноменами политической коммуникации и мобилизации. Рассмотренные в работе походы к определению смысла политической коммуникации Г. Лассуэла, К. Шеннона и У. Уивера, М. Де Флера обладают общим признаком, позволяющим понять смысл данного феномена, а именно, то, что политическая коммуникация предполагает наличие коммуникатора (первоисточника информации), передатчика (субъекта, через который передается информация) и декодера (субъекта, принимающего информацию), оказывающими друг на друга манипулятивное воздействие в процессе передачи информации. Данный факт позволяет понять и суть феномена политической мобилизации как процесса манипулятивного воздействия источника информации или ее передатчика на декодера и конечного получателя с целью участия последнего в политическом процессе.

Развитие интернета и социальных сетей определило эволюцию и феномена политической мобилизации. В частности, появилась сетевая разновидность данного феномена – виртуальная или сетевая политическая мобилизация, - и далее сформировалась группа технологий, направленных на организацию политического противостояния. Приведенный в работе анализ эволюции подхода к феномену сетевой конфликтной мобилизации позволил определить, что она становится возможной при наличии следующих обязательных элементов: личного недовольства пользователей сети, участников такой мобилизации, личных возможностей для участия в

политическом процессе, доступа к виртуальной среде, а также наличия сформированной виртуальной идентичности у участников данного явления. Этот элементный каркас феномена сетевой конфликтной мобилизации также дополняется и другими факторами, позволяющими учесть ряд социальных и политических особенностей в каждом отдельном государстве. При этом указанные элементы являются неотъемлемой частью каждого из альтернативных подходов к выявлению набора необходимых условий для имплементации сценария сетевой конфликтной мобилизации.

Совокупность участников сетевой конфликтной мобилизации объединяется дефиницией виртуальной политической толпы[83], обладающей такими характеристиками, как передача информации в режиме реального времени, интерактивность, возможность анонимного участия, отсутствие организационного лидера, а также отсутствие рамок участия в политическом процессе.

Процесс создания виртуальной политической толпы и, соответственно, ее участия в политическом процессе, связан с применением интернет-технологий политической мобилизации[84]. Автор работы предложил классификацию этих технологий, где ключевыми компонентами выбраны 5 элементов: платформа, на которой применяются технологии (видеохостинги, социальные сети, мессенджеры, сайты и приложения), субъектность организатора мобилизации (открытая и скрытая), радиус воздействия технологий (локальные, государственные, межгосударственные), период воздействия (краткосрочные и перспективные), акторы распространения информации (централизованные и распределенные).

---

[83] Лайнбарджер П. Психологическая война. Теория и практика обработки массового сознания. М.: Центрполиграф, 2013. — 448 с.

[84] Марин Е.Б., Осмачко Н.В. Динамика протестных настроений студенческой молодежи в региональном контексте: на примере Приморского края // Социально-политические науки. - 2020. - Т. 10. - № 5. - С. 20-35.; Морозов И.Л. Уличный протест как технология антигосударственных действий радикальной оппозиции - опыт зарубежных стран и угроза для России // Общество: политика, экономика, право. - 2021. - № 3 (92). - С. 12-44; Негров Е.О. Роль и особенности молодежного политического онлайн-активизма в современной России // Вестник Российского университета дружбы народов. Серия: Политология. - 2021. - Т. 23. - № 1. - С. 18-30.; Нешков С.В. Массовые агитационно-пропагандистские материалы политических протестных акций 2017 г. в России // Вопросы национальных и федеративных отношений. - 2021. - Т. 11. - № 4(73). - С. 1181-1190.

Также в рамках первой главы выявлено, что интернет-технологии сетевой конфликтной мобилизации представляют угрозу для национальной безопасности Российской Федерации. Их использование напрямую связано с такими положениями в нормативно-правовых актах, определяющих действия России по обеспечению стабильности интернет-пространства, как: формирование безопасной среды оборота достоверной информации, развитие системы предупреждения угроз информационной безопасности, открытого доведения до российской и международной общественности информации о внутренней и внешней политике РФ и др.

В условиях гибридной войны, проводимой против России, особое внимание должно быть уделено изучению методов противодействия виртуальным технологиям конфликтной мобилизации. Онлайн-площадки уже используются для формирования негативного образа России, что является подготовительным этапом для дальнейших действий в виртуальном пространстве. После данного этапа, как показывает анализ подобных инцидентов, проводится попытка эскалации политических конфликтов внутри государства методами организации конфликтной мобилизации в интернет-пространстве. В связи с этим растут угрозы данного феномена.

Классификация интернет-технологий сетевой конфликтной мобилизации позволяет сформировать частные подходы к противодействию им, тем самым обеспечивая реализацию задач Российской Федерации в

Глава 2. Особенности использования технологий конфликтной мобилизации оппозиционными движениями в США и КНР

2.1 Формы и методы применения технологий конфликтной мобилизации и управления протестом в КНР

Интернет-технологии конфликтной мобилизации – универсальный инструмент для развития и эскалации политических конфликтов, используемый в различных государствах, независимо от их политических особенностей. Однако потенциал этого инструмента, как и методы противодействия ему, находятся в прямой зависимости от многих факторов, таких как уровень развития судебной системы, нормативно-правовая база в сфере регулирования действий пользователей в социальных сетях, политический режим и т.д.

Одной из ключевых задач данной работы является выявление особенностей противодействия интернет-технологиям конфликтной мобилизации в государствах с различными подходами к возможностям пользователей в социальных сетях. Для проведения такого сравнительного анализа были выбраны два государства, ключевым образом отличающиеся друг от друга по указанному принципу: Китайская Народная Республика и Соединенные Штаты Америки.

Объяснение выбора данных стран для сравнительного анализа лежит сразу в нескольких плоскостях. Во-первых, США и КНР используют противоположные методологии регулирования интернет сферы. В КНР создана система тотального контроля за деятельностью каждого пользователя интернета. Начиная от необходимости получения персонального идентификатора, привязанного к удостоверению личности, для входа в интернет, заканчивая контролем за комментариями людей в социальных сетях и системой рейтинга и блокировок в случае каких-либо антигосударственных записей. В США же подход противоположный: каждому пользователю разрешается использовать интернет без каких-либо ограничений, если, конечно, его действия не противоречат законодательству. Свобода комментирования, публикации в социальных сетях, минимум блокировок и барьеров для доступа в интернет.

Во-вторых, данных государства выбраны, как передовые в части технологического развития. У каждого государства есть свои языки программирования и самые большие производственные мощности по созданию аппаратно-функциональной инфраструктуры. Государства по праву считаются носителями своего цифрового суверенитета.

В связи с этим сравнение именно этих государств представляется автору перспективным для понимания альтернативных вариантов противодействия интернет-технологиям конфликтной мобилизации.

В качестве объекта анализа в КНР был выбран политический кризис 2019 года, произошедший в специальном административном районе КНР Гонконге. Конфликт между гражданским обществом и властью был вызван возможностью принятия законопроектов, корректирующих принципы взаимодействия исполнительной и судебной ветвей власти Гонконга и материкового Китая[85]. А именно, речь идет об изменении в двух законодательных актах: Законе о скрывающихся от правосудия

[85] Карпович О.Г., Карипов Б.Н., Литвинов В.О. Эволюция протестных настроений в Гонконге: основные уроки // Вестник Дипломатической академии МИД России. Россия и мир. - 2021. - № 2 (28). - С. 71-87.

правонарушителях и Указе о взаимной правовой помощи по уголовным делам. Принятие поправок позволило бы создать механизм индивидуальной передачи скрывающихся от правосудия лиц по распоряжению главы исполнительной власти в любую юрисдикцию, с которой Гонконг не имеет официального договора о выдаче, включая выдачу материковому Китаю. Законопроект был вынесен на обсуждение в феврале 2019 года, как реакция на инцидент с убийством жителей Гонконга на территории Тайваня.

Однако данная юридическая проблема не мобилизовала жителей Гонконга в поддержку законопроектов, воспринявших имплементацию поправок, как попытку снижения уровня независимости Гонконгской системы государственного управления от материкового Китая. На это были очевидные причины, ведь поправки не подразумевали возможность экстрадиции подозреваемых из некоторых территорий КНР[86], в связи с чем жители Гонконга восприняли эти действия, как попытку усиления контроля именно за их территорией. В связи с этим сразу после вынесения на обсуждение указанных поправок в общественном пространстве Гонконга начался конфликт между гражданским обществом и властью.

В результате конфликта законопроект был отвергнут, а глава Гонконга Кэрри Лам подала в отставку. Во время активной фазы конфликта были проведены многотысячные митинги, участники которых вступали в открытую насильственную конфронтацию.

В рамках данного противоборства были применены интернет-технологии конфликтной мобилизации, позволившие выполнить ряд задач для эскалации кризиса. Во-первых, главной задачей на начальных этапах стало информирование граждан о законопроектах и их негативная субъектизация. Во-вторых, интернет-технологии позволили подготовить активную фазу протеста: отметить основные точки сбора и донести план действий до участников. В-третьих, интернет использовался и как инструмент координации протестующих во время активной фазы кризиса.

[86] Martin Purbrick A report of the 2019 Hong Kong Protests, Asian Affairs. - 2019. - P. 465-487.

Данные задачи были решены с использованием социальных сетей, действующих на территории Гонконга. Среди них: YouTube, Telegram, WhatsApp, Signal, LIHKG, Weibo и WeChat и другие. Важно обратить внимание также на то, что на территории Гонконга действует отдельная законодательная система, отличная от той, что принята в материковом Китае, в связи с чем там работают те социальные сети, которые запрещены на «материке». К таким запрещенным социальным сетям относятся: YouTube, Telegram, WhatsApp, Instagram[87], Twitter, Facebook[88], все сервисы Google и т.д. Этот момент важен для анализа. Он подчеркивает, что публикация какой-либо информации в этих соцсетях не была ориентирована на центральное Китайское правительство и на граждан материковой части КНР. Публикации в данных соцсетях были направлены на жителей Гонконга и иностранных граждан.

Мессенджеры WhatsApp и Signal использовались гражданами уже на активной стадии кризиса: пользователи обменивались информацией о местах сбора протестующих и координировали протест[89]. Именно координация стала основной задачей соцсетей в рамках протестов. Связано это во многом с тем, что общество уже было готово к протестной активности в связи с митингами, начавшимися в 2014 году с так называемой «революции зонтиков». Инцидент с рассмотрением поправок в два нормативно-правовых акта спровоцировал быструю реакцию уже мобилизованного населения. Организаторам митингов было достаточно определить места сборов протестующих и план их действий. Отличие протестов 2019 года от той же «революции зонтиков» также заключалось в том, что их организаторы выбрали тактику децентрализованного протеста. Людей не собирали в одном

[87] Социальная сеть «Instagram», принадлежащая компании Meta Platforms, признана экстремисткой и запрещена на территории России согласно решению Тверского суда, г. Москва.
[88] Социальная сеть «Facebook», принадлежащая компании Meta Platforms, признана экстремисткой и запрещена на территории России согласно решению Тверского суда, г. Москва.
[89] Tin-yuet Ting From ‘be water’ to ‘be fire’: nascent smart mob and networked protests in Hong Kong, Social Movement Studies. – 2020. - P. 362-368.

месте, а создали несколько мест сбора[90]. Это значительно усложнило задачу правоохранительных органов. При этом это также повысило эффект от использования социальных сетей, ведь для координации многотысячных митингов, распределенных по всему Гонконгу, было необходимо постоянно управлять толпами, отправляя информацию о передвижениях полицейских сил.

Другим инструментом активного распространения информации об инцидентах политического кризиса был видеохостинг YouTube. Видеоролики, выполненные в формате новостей, подробно объясняли пользователям, как проходят митинги и интерпретировали те или иные заявления и действия властей таким образом, что провоцировало у зрителей формирование позитивного взгляда на необходимость продолжения протестных акций. Отдельно стоит отметить два канала: «Baton» и «Headliner». Эти два ресурса стали источником подогрева интереса к протестам в сети YouTube. Примечательно, что позднее оба канала были удалены по запросу Бюро экономического развития Гонконга, так как они способствовали разжиганию ненависти по отношению к представителям правоохранительных органов[91].

Особо стоит отметить социальную сеть LIHKG. Этот инструмент стал известен именно благодаря протестам в Гонконге. С его помощью жители обменивались информацией о ходе протестов, делились расписаниями и планами активностей, проводимых во время митингов, а также публиковали полезные для участников протеста руководства по тому, как готовить «коктейли Молотова», как оказывать первую медицинскую помощь, как вести себя с представителями полиции и т.д.[92] Интересной особенностью данной соцсети можно называть тот факт, что подключиться к ней могли только жители Гонконга. Для этого соцсеть LIHKG запрашивала адрес

[90] Tin-yuet Ting From ‘be water’ to ‘be fire’: nascent smart mob and networked protests in Hong Kong, Social Movement Studies. – 2020. - P. 362-368,
[91] Hongkongers rush to 'Save RTHK' from show purge. URL: news.rthk.hk/rthk/en/component/k2/1589017-20210503.htm (дата обращения: 20.02.2022)
[92] Purbrick, Martin. "A Report of the 2019 Hong Kong Protests". Asian Affairs. – 2019. - №50(4): - P. 463-475.

электронной почты, зарегистрированный Гонконгским провайдером. Это исключало возможность просмотра контента в соцсети жителями материкового Китая, в том числе представителями правоохранительных органов.

Отдельно стоит выделить мессенджеры, позволяющие жителям делиться текстовыми сообщениями, фото и видеофайлами без доступа к интернету. Это возможно благодаря использованию инструментов Bluetooth и Wi-Fi. Подключаясь к общему локальному пространству, пользователям становились доступны возможности мессенджеров даже при отключенном доступе в интернет. К мессенджерам, работающим на подобном принципе, относятся Airdrop для смартфонов производства компании Apple, а также FireChat и аналоги этих сервисов. Наиболее востребованы эти инструменты были у участников протестов. Однако пользоваться ими в рамках подготовки к митингам или для формирования информационного поля уже после них нерационально.

Наиболее важным ресурсом, повлиявшим на ход митингов, стал мессенджер Telegram. Именно с его помощью участники протестов получали информацию о ходе митингов, о передвижениях полиции, но еще более важная составляющая заключалась в использовании мессенджера для мобилизации населения на допротестной стадии. Использование Telegram для этих целей подтверждается статистическими данными о высоких темпах набора популярности этого мессенджера среди жителей Гонконга. В проведенном исследовании, посвященном роли Telegram в гонконгских протестах в 2019 году, авторов Александры Урман, Джастина Чун-тинг Хо и Стефана Катца приведены подобные данные.

Так, стоит обратить внимание на количество новых групп/каналов в мессенджере Telegram, образованных в период с конца марта 2019 года, когда было объявлено о рассмотрении законопроекта о поправках, и июлем 2020 года, когда был принят Закон о национальной безопасности.

На рис. 4 график, изображенный слева, показывает активность появления новых групп по датам. Видно, что две стадии активного роста количества новых групп в Telegram соответствуют пиковым значениям количества участников митингов. Именно на август 2019 года и на декабрь 2019 года приходится наибольшее количество митингующих (рис. 5), тогда как в августе 2019 года и в ноябре 2019 года (за неделю до крупнейшего декабрьского митинга в Гонконге) был зафиксирован наибольший всплеск

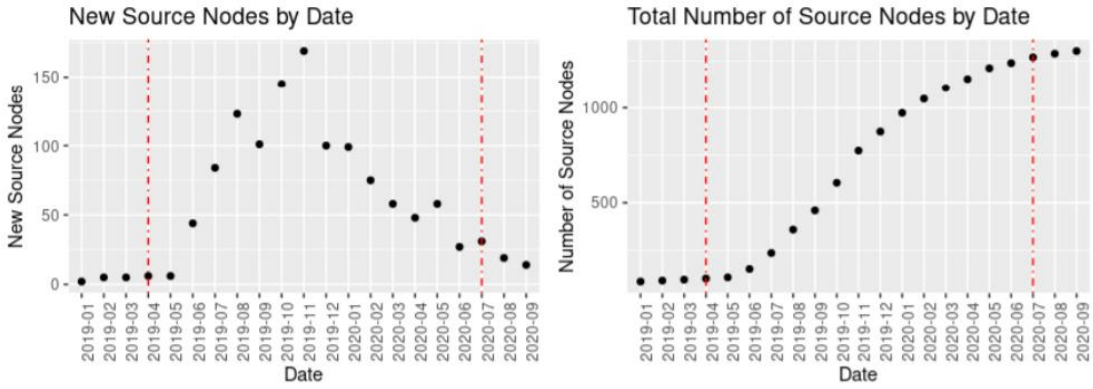

Рисунок 4

количества новых групп в социальных сетях[93]. Далее, активность появления каналов в Telegram снижалась, ровно, как и количество участников

Рисунок 5

[93] Hong Kong Police Review 2020 // Hong Kong Police URL: www.police.gov.hk/info/review/2020/en/hkpf_eng05.html (дата обращения: 23.04.2022).

демонстраций.

Интересен также и характер публикаций в группах и каналах в Telegram. Согласно данным уже указанного исследования были публикации, которые можно разделить на 6 категорий:

1. Анонсы протестов (announcement).
2. Действия полиции (recon).
3. Обсуждения хода и итогов протеста (discussion).
4. Новости об арестах участников акций (arrest news).
5. Новости (news).
6. Раскрытие информации о полицейских, жестоко обращавшихся с участниками митингов (curses).

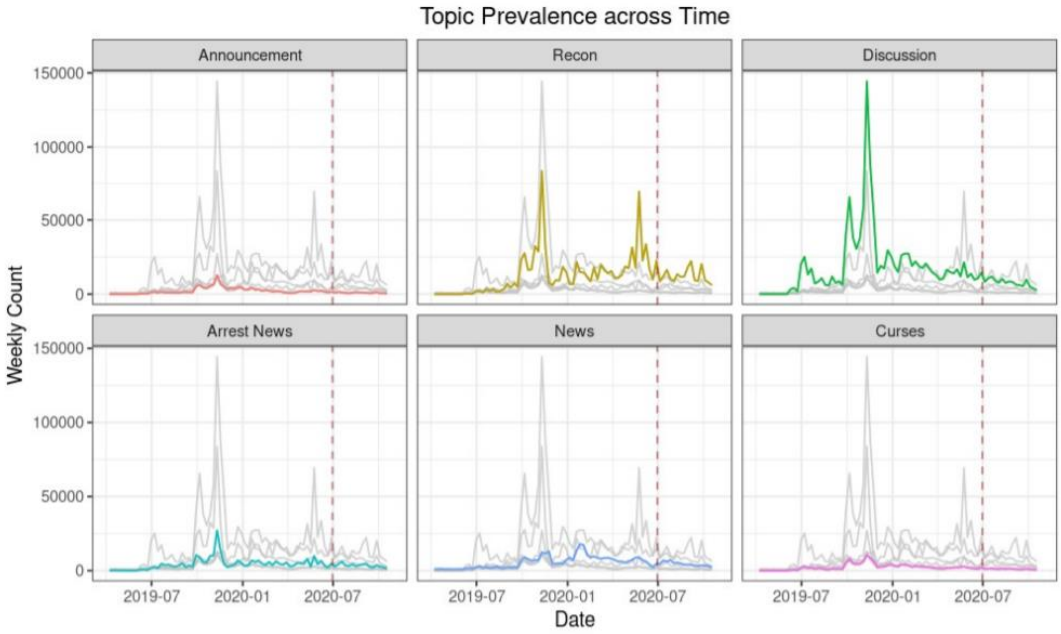

Рисунок 6

Согласно графику, на рис. 6, выявляется закономерность, что на начальных стадиях протестной активности наиболее активными были темы обсуждений и действий полиции. Первая категория может восприниматься, как тема, позволяющая сформировать единое негативное представление о действиях властей, о поправках в законы. Вторая же тема позволяла

координировать протестующих, уведомляя их о том, где и как расположены патрули правоохранительных органов.

Отдельно стоит проанализировать категорию раскрытия информации о полицейских. Так, были созданы отдельные группы и каналы в Telegram, публикующие персональные данные о полицейских, применяющих, по мнению авторов этих каналов, чрезмерное насилие по отношение к протестующим. Так, телеграм-канал Dadfindboy публиковал фотографии, адреса проживания, фотографии семей таких полицейских. Такая информация позволяла оказывать давление на представителей правоохранительных органов, вследствие чего в рядах сотрудников полиции появлялись опасения, затруднявшие применения ими силы во время столкновений с демонстрантами. Данный инструмент давления со стороны организаторов протестов и авторов Telegram-каналов оказался действенной силой, что подтверждается фактом его применения в иных случаях массовых протестов в других странах, например, Белоруссии.

Telegram стал ключевой социальной сетью, позволившей жителям Гонконга участвовать в постоянной протестной активности, длившейся на протяжении года, а ее организаторам эффективно управлять участниками, формируя точки сбора, сообщая о передвижениях полиции и т.д. Telegram, как и другие социальные сети и мессенджеры, использовался с ориентиром на целевую аудиторию публикуемой информации в качестве самих жителей Гонконга, а также представителей международного сообщества. Это подтверждается тем, что ряд каналов[94] публиковали информацию о протестах на английском языке, делая ее восприятие доступным для жителей других стран.

Кроме того, особенностью использования Telegram и других социальных сетей в рамках политического кризиса в Гонконге стало то, что

[94] Телеграм-канал @hkiswatching URL: t.me/hkiswatching (дата обращения: 23.04.2022).

протест был частично геймифицирован его организаторами[95]. А именно, участникам представилась возможность выбрать свою роль и действовать по ней, как по сюжету. Так, организаторы создали 5 ролей (рис. 7):

1. «Wo Lei Fei» («мирные помощники»), помощники «бойцов», которые должны были снабжать их необходимыми ресурсами, мониторить и сообщать о ситуации на улицах, а также участвовать в строительстве баррикад.

2. «Yung Mo» («доблестные бойцы»), в задачи которых входило активное противостояние полиции - участие в столкновениях.

3. «Kei Sau» («знаменосцы») – управленцы протестом, которые должны были анализировать поступающую от «мирных помощников» информацию, принимать решения на ее основе, а также следить за соблюдением порядка и правил «игры» в рядах протестующих.

4. «Yuen Kung» («нападающие на расстоянии») - в их задачи ставилась организация доступа к ресурсам за пределами территории активных действий. То есть, им нужно было следить за путями «отхода» протестующих, обеспечивать подвоз одежды, питания). Также участники этой роли должны были оказывать сопротивление полиции на расстоянии, например, используя рогатки или иное метательное оружие.

5. «Siu Fong Yuen» («пожарные») – должны были бороться с воспламенениями или со слезоточивым газом, применяемым силами правопорядка.

У каждой из ролей был свой визуальный символ, который использовался в схемах и картах «боевых» действий для обозначения позиций, на которых должны были располагаться участники.

Геймификация протеста – новый инструмент конфликтной мобилизации, примененный с помощью социальных сетей. Он начал использоваться в августе 2019 года спустя два месяца с начала активной

[95] DUMMIES GUIDE to confrontation and war strategies by frontline protesters in Hong Kong // Dimsum Daily URL: www.dimsumdaily.hk/exclusive-dummies-guide-to-confrontation-and-war-strategies-by-frontline-protesters-in-hong-kong/ (дата обращения: 20.02.2022).

стадии протеста и позволил сделать из политического события, сопряженного с чувством опасности у жителей, игру, вовлекающую новых участников протеста и погружающих их в условия компьютерной игры стратегии[96].

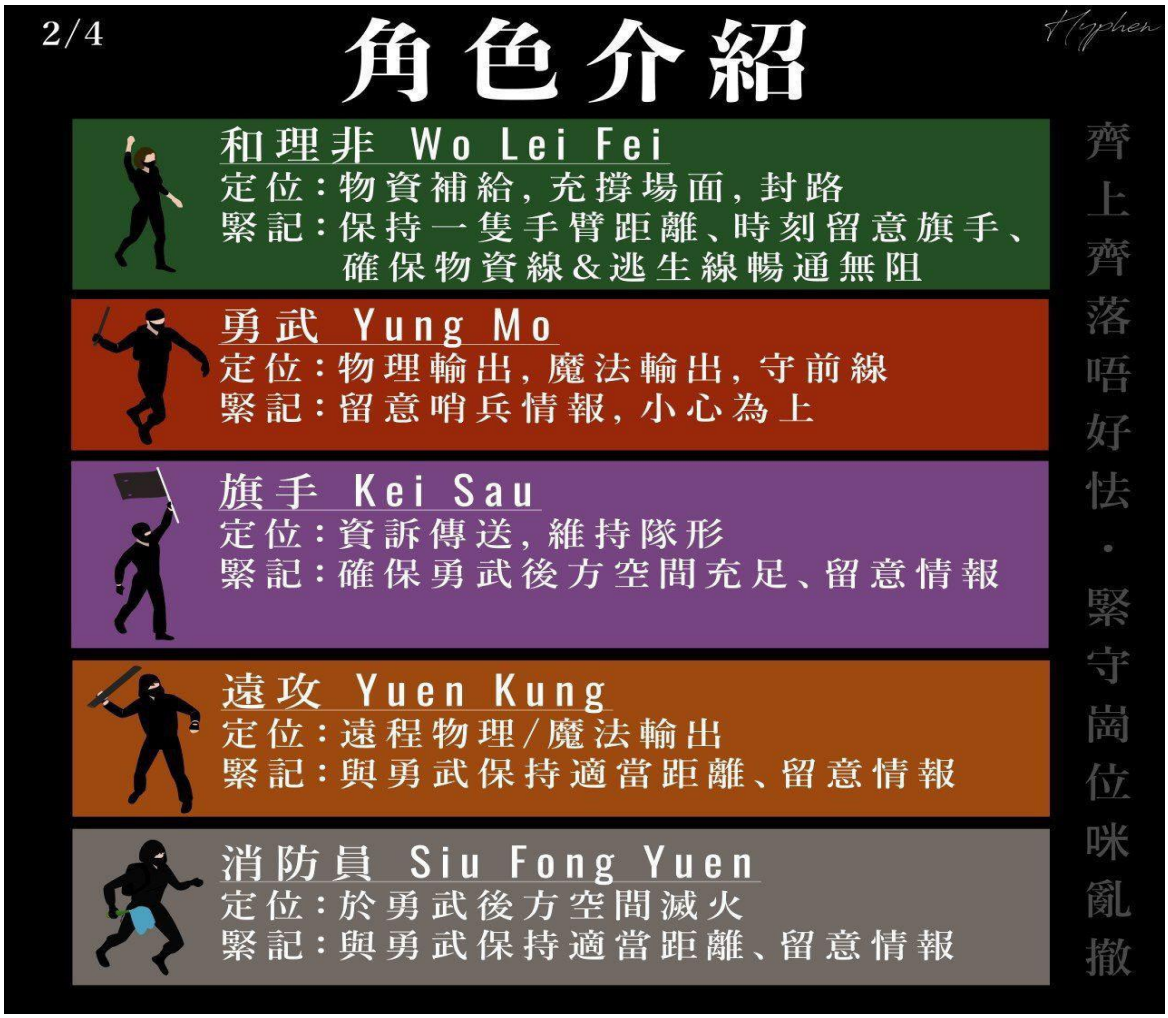

Рисунок 7

Истоки данной технологии происходят из феномена политического акционизма. Данное явление существовало в тех или иных формах еще с древних времен, однако в середине XX века превратилось в целостное направление политической активности населения. Так, в 60-х годах XX века в США прошли так называемые «кампусные протесты» - митинги, шествия и

[96] Есиев Э. Т. Геймификация протеста как технология сетевой конфликтной мобилизации // Информационные войны. - 2022. - № 2. - С. 2-5

столкновения с полицией, в которых основными участниками были студенты. Оставляя за скобками причины и тематику протестов, стоит подробнее остановиться на вопросе, как они проходили (рис. 8).

Кампусные протесты в 60-х годах были разнообразными по своей природе и методам действий. Вот общая картина того, как они проходили[97]:

Рисунок 8

1. Организация и мобилизация: Студенты, активисты и факультеты организовывали группы единомышленников, чтобы обсуждать общественно значимые проблемы и планировать проведение каких-либо акций. Они использовали печатные издания, листовки, а также межличностные контакты для мобилизации и привлечения большего числа участников.

2. Митинги и демонстрации: Студенты устраивали митинги, марши, забастовки и другие формы публичного протеста. Они выходили на улицы с плакатами, флагами и лозунгами, чтобы выразить свои требования и привлечь внимание общественности.

3. Захват зданий: зачастую студенты занимали здания университетов, чтобы привлечь внимание к своим требованиям. Это могло быть здание

[97] Gitlin, T. (2012). The Whole World Is Watching: Mass Media in the Making and Unmaking of the New Left. American Sociological Review. – 2012. - №77(1), - P. 69-95.

администрации, аудитория или другие объекты образовательной инфраструктуры.

4. Обсуждения и дебаты: кампусные протесты также включали обсуждения и дебаты, как внутри университетов, так и на публичных площадях. Студенты проводили собрания, публичные лекции и панельные дискуссии, чтобы обсудить проблемы и найти совместные решения.

Данный пример показывает, что еще в середине прошлого века элементы игрового процесса – в данном случае «игра в революцию» - были приняты на вооружение участниками и организаторами политических акций.

В России также были примеры политического активизма игровой формы. Например, известная акция «Монстрация», во время которой люди выходили на митинг с транспарантами с какой-то фразой юмористического содержания. «Монстрация» была пародией на митинг, а люди, участвующие в ней, чувствовали себя, как в игре[98].

Позднее, уже после инцидента с реализацией классического сценария компьютерной игры-стратегии во время реального протеста в Гонконге, в России прошел виртуальные митинг в приложении «Яндекс.Карты». Тогда граждане, недовольные ограничениями, связанными с мерами по защите от распространения пандемии коронавируса, устроили «митинг» в Ростове-на-Дону – писали сообщения в картах рядом с центральной площадью города.

Подобное развитие феномена геймификации протеста может говорить о перспективе этой технологии в части организации политических акций. Именно в связи с этим данная технология заслуживает подробного изучения и поисков вариантов нивелирование угроз, исходящих от нее.

Возвращаясь к изучению событий в Гонконге, необходимо отметить, что в рамках протестных активностей была осуществлена попытка использования и китайских социальных сетей, находящихся под юрисдикцией китайского правительства и имеющих собственную систему

[98] Матюсова А. И. История возникновения российских монстраций // Русская политология. - 2017. - №2 (3). - С. 87-93

противодействия каким-либо оппозиционным политическим проявлениям. К таким социальным сетям относятся WeChat и Weibo. Использовали эти соцсети в большинстве своем китайские студенты, отправившиеся на учебу в Гонконг[99]. Среди китайских граждан WeChat и Weibo являются наиболее популярными социальными сетями. Связано это с тем, что в них интегрированы многие функции, без которых жизнь современного человека в КНР представить сложно. Так, в WeChat есть возможность вызова такси, доставки продуктов, перевода денежных средств, оплаты коммунальных платежей, записи к врачу. Также к этой социальной сети подключены сервисы государственных услуг. Набор этих функций обеспечивает использование WeChat населением Китая. К первому кварталу 2021 году ежемесячная аудитория социальной сети достигла 1,2 млрд пользователей[100]. В рамках протестов в Гонконге информацию о них в китайских соцсетях в основном публиковали именно студенты, находившиеся на этой территории из-за учебы в местных университетах. Однако реального влияния на протест, его развитие подобные публикации не оказали в связи с тем, что инфраструктура для выявления и блокировки подобных сообщений в китайских социальных сетях развита на высоком уровне и не допускала вирусного распространения информации.

Анализируя протестную активность в Гонконге в 2019 году, стоит обратить внимание на четыре ключевых фактора, описанных выше. Во-первых, в процессе управления и координации участников демонстраций и митингов преимущественно использовались международные социальные сети. За исключением социальной сети LIHKG, которая стала популярной именно благодаря протестам, все остальные инструменты интернет-технологий конфликтной мобилизации являлись международными. Это является свидетельством того, что именно такие соцсети и мессенджеры

[99] The dark side of WeChat // Monmouth URL: www.monmouth.edu/magazine/wp-content/uploads/sites/7/2020/10/Monmouth-Magazine-Fall-2020.pdf. (дата обращения: 20.02.2022).

[100] China’s State-Run Companies Limit Use of Tencent’s Messaging App // WSJ URL: www.wsj.com/articles/chinas-state-run-firms-limit-use-of-tencents-messaging-app-11637837474 (дата обращения: 20.02.2022).

несут основную угрозу для обеспечения защиты населения от возможного вмешательства во внутренние дела государства со стороны организаторов протестных активностей с использованием интернет-технологий конфликтной мобилизации.

Во-вторых, в рамках политического кризиса 2019 года в Гонконге практически отсутствовала предварительная стадия конфликтной мобилизации населения. Такая стадия обязательно присутствует во время конфликтной мобилизации, связанной с запланированными на будущее политическими событиями, например, выборами[101], однако, как мы видим на примере Гонконга, она может отсутствовать при ситуативном политическом инциденте, таким, как, например, принятие того или иного закона. Этот ключевой вывод позволяет подчеркнуть важность социальных сетей в современном мире и их эффективность с точки зрения скорости в вопросах организации конфликтной мобилизации. Стоит, тем не менее, сделать уточнение, что подобная быстрая мобилизация возможна в ситуации наличия сразу двух важных условий. В первую очередь, само политическое событие, ставшее поводом для эскалации конфликта власти и общества, должно быть достаточно важным для этого общества. Вторым же условием является то, что конфликт уже должен существовать, пусть и находиться в латентной, пассивной, стадии. В Гонконге с 2014 года, с момента начала «революции зонтиков», продолжался конфликт между властью и обществом. А население, получившее политические дивиденды по результатам политического кризиса 2014 года, было готово к продолжению подобного противостояния в будущем. Эти условия и стали фундаментом для быстрой эскалации конфликта, а ее инструментом выступили социальные сети.

В-третьих, в рамках политического кризиса в Гонконге 2019 года была впервые применена технология запугивания представителей правоохранительных органов. Сделано это было с помощью публикации

[101] Ершов Н.А., Омерович А.Р., Попов С.И. Протестный потенциал как инструмент предвыборной кампании (Часть II: выборы в государственную думу 2021 года. Прогнозы) // Вопросы национальных и федеративных отношений. - 2021. - Т. 11. - № 3 (72). - С. 853-858.

персональных данных о них в социальных сетях. Полицейские, которые, по мнению авторов групп и каналов в мессенджерах и соцсетях, применили чрезмерную силу для противодействия демонстрантам, были раскрыты: их фотографии, телефоны, адреса проживания были опубликованы в открытом доступе, что, конечно же, сеяло в рядах правоохранительных органов неуверенность и страх от участия в противодействии активистам. Именно в связи с этим организаторам гонконгских протестов удалось поддерживать активную фазу конфликта на протяжении года. Далее такая технология использовалась и в других конфликтах: например, в протестных активностях в России, Белоруссии.

В-четвертых, стоит отметить фактор геймификации протеста в Гонконге. Спустя уже два месяца после начала активной стадии конфликта его организаторы создали игру, в которую погрузили участников демонстраций. Жители не просто выходили на улицы для защиты своих взглядов, а находились в игре, где у каждого участника были свои роли и, соответственно, функции. Затяжная протестная активность может принимать неожиданные и опасные для текущего политического режима формы. Геймификация протеста оказалась дополнительным фактором для привлечения новых участников, а также инструментом психологического давления, манипуляции на сознание граждан, принимающих участие в протесте.

Помимо конфликта в Гонконге анализировать протестную активность в Китайской Народной Республике можно и по ряду иных прецедентов. Однако именно конфликт в Гонконге в 2019 году наиболее ярко демонстрируют то, как организаторы протестных политических акций проводят конфликтную мобилизацию в онлайне.

Иным примером может стать анализ конфликта в том же Гонконге в 2014 году. Демонстрации по поводу изменения в избирательной системе региона вывели 28 сентября тысячи людей на улице, в результате чего произошли столкновения с полицией. Сами демонстрации растянулись более,

чем на 80 дней. А подготовительная фаза для организации протестов была реализована с применением виртуальных технологий конфликтной мобилизации. В социальных сетях, как и в случае с протестами 2019 года, был запущен хэштег Occupy Central (пер. «Займи центр города»). Сообщения с этими лозунгами заполонили социальные сети Facebook и Instagram 24 сентября и до 28 числа продолжали активно распространяться, после чего китайские власти заблокировали работу сотовых операторов, а вместе с ними и доступа в интернет.

Основными инструментами, примененными в этом конфликте, стали:

1. Технология распространения информации посредством создания вирусного контента, в т.ч. сообщений с однотипным хэштегом.

2. Управление конфликтом с помощью координации в интернете. В частности, была создана общая таблица в Google Sheets[102], на которой публиковалась информация о том, кому, что и где необходимо сделать для продолжения протестной активности.

3. Несмотря на блокировку интернета, граждане Гонконга нашли возможность получения доступа к всемирной паутине и продолжили использование международных социальных сетей. Информация о ходе протестов публиковалась в ряде групп в Facebook, Twitter и WhatsApp[103].

4. Формирование новых инструментов для координации действий и проведение конфликтной мобилизации в онлайн-пространстве. В частности, форум HKGolden, используемый ранее для обсуждения исключительно компьютерной техники, стал одной из главных площадок для коммуникации протестующих. Также именно во время «революции зонтиков» стал известен сервис FireChat, коммуникация в котором осуществляется посредством технологии Bluetooth, позволяющей обходиться без интернета и сотовой связи. Также популярность набрал сервис Code4HK – аналог сервиса

---

[102] Таблица Umbrella Revolution / URL: https://docs.google.com/spreadsheets/d/1psp1mPDWoT29KAcjuBrbywNumUvBEPNJG5tuUjJ8uaQ/pubhtml (дата обращения: 20.02.2022)

[103] LIVE: Verified updates // Facebook URL: https://www.facebook.com/hkverified (дата обращения: 20.02.2022).

YouTube, используемый протестующими для публикации видео, ведения прямых трансляций и т.д.

Данный прецедент конфликтной мобилизации в интернете также соотносится с опытом волнений в Гонконге в 2019 году. Но если в рамках конфликта 2014 года основной упор его организаторов делался на площадки коммуникации, то в 2019 году большее внимание было уделено уже контентному наполнению: типу информации, применению новых технологий, таких, как геймификация и т.д.

2.2. Формы и методы применения технологий конфликтной мобилизации и управления протестом в США

Для дальнейшего изучения феномена интернет-технологий конфликтной мобилизации необходимо рассмотреть пример использования таковых в государстве с другим политическим режимом и иным подходом к обеспечению политической безопасности информационного пространства. Наиболее подходящим для компаративного анализа представляется выбор Соединенных Штатов Америки. Государство активно выступает за свободу слова в интернете и выступает против блокировок тех или иных страниц в соцсетях во время протестов в других странах с одной стороны, а с другой - активно блокирует «ботов» или «троллей», оказывающих влияние, по мнению американских властей, на внутренний политический процесс. В качестве примера конфликта, в рамках которого были применены интернет-технологии конфликтной мобилизации в США можно привести кризис, приведший к попытке захвата здания американского Капитолия 6 января 2021 года. Тогда многотысячная толпа американцев, поддерживающих проигравшего на выборах, но еще не покинувшего пост президента США, Дональда Трампа, пришедшая на организованный им митинг у Белого дома в свою поддержку, отправилась к зданию Капитолия с целью его захвата. Последствия данного инцидента оказались масштабными: погибло 5 человек, более 65 человек арестовано, а самого Дональда Трампа заблокировали сразу в нескольких социальных сетях. Требования митингующих заключались в пересчете результатов выборов и объявлении победителем Дональда Трампа.

Социальные сети оказали существенное влияние на подготовку данной акции. Благодаря им удалось сформировать мобилизованную группу граждан, готовых применить насилие ради достижения политических интересов организаторов. Конфликтную мобилизацию проводили с помощью двух движений, поддерживающих Дональда Трампа: движение StopTheSteal и QAnon.

QAnon – теория заговора, популярная среди последователей Дональда Трампа, - о том, что реальная власть в США принадлежит некоей группе «сатанистов-педофилов», состоящей по большей части из представителей Демократической партии. Дональд Трамп являлся главным положительным героем данной теории. Его миссия заключалась в борьбе с этой группой путем арестов и чисток во органах власти США. Движение зародилось в 2016 году с момента победы Дональда Трампа на выборах президента и просуществовало до конца его полномочий. Пиком активности участников движения стала попытка захвата здания Капитолия 6 января 2021 года. Зародилось QAnon в развлекательных группах популярных социальных сетей: reddit и facebook[104], обрело там сторонников, готовых, как показало время, принять реальное участие в политическом конфликте с представителями власти. Конец же существования данного движения был связан с блокировкой их страниц в социальных сетях в связи с участием сторонников QAnon в атаке на Капитолий. Американские исследователи выделяют важную роль этого движения в организации беспорядков 6 января, а социальную сеть Facebook обвинили не только в бездействии по отношению к QAnon на этапах, предшествующих атаке на Капитолий, но в помощи в популяризации этого движения. Так, было проведено расследование «Carol`s Journey» (Путешествие Кэрол)[105], в рамках которого его автор зарегистрировал страницу на Facebook под именем Кэрол Смит,

[104] Социальные сети «Instagram» и «Facebook», принадлежащие компании Meta Platforms, признаны экстремистскими организациями и запрещены на территории России согласно решению Тверского суда, г. Москва

[105] ‘Carol’s Journey’: What Facebook knew about how it radicalized users // NBC News URL: www.nbcnews.com/tech/tech-news/facebook-knew-radicalized-users-rcna3581 (дата обращения: 20.02.2022).

подписался на аккаунты Республиканской партии США и Дональда Трампа и всего через несколько дней в предлагаемые списки групп и сообществ для подписок у него начала приходить рекомендация стать участником движения QAnon. Авторы этого исследования ставили вопрос о работе рекомендательных алгоритмов Facebook, которые на основании политических предпочтений сами помогали развить маргинальное движение, частью которого были сторонники Дональда Трампа. Особенно важно отметить, что к моменту проведения указанного исследования группы QAnon

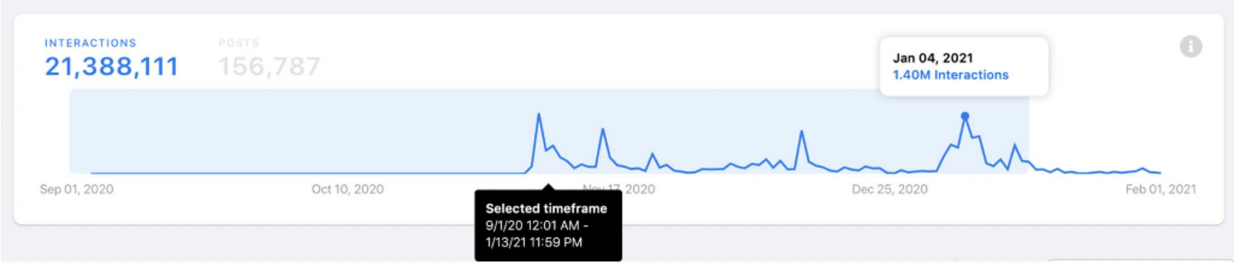

Рисунок 10

в Facebook должны были быть заблокированы, так как американское Федеральное Бюро Расследований (ФБР) еще в августе 2019 года признало само движение QAnon экстремистским[106]. Тем не менее, участниками групп QAnon становились тысячи и миллионы пользователей (рис. 9).

QAnon стало частью другого движения StopTheSteal («Остановите

Рисунок 9

воровство»), образованного после оглашения результатов выборов

[106] Local FBI field office warns of 'conspiracy theory-driven domestic extremists' // NBC News URL: www.nbcnews.com/tech/tech-news/local-fbi-field-office-warns-conspiracy-theory-driven-domestic-extremists-n1038441 (дата обращения: 20.02.2022).

президента США 2020 года. В движение Stop The Steal вошло не только QAnon, но и ряд другие правых организаций, многие их которых были экстремистскими. Согласно данным, опубликованным в открытых источниках, данное движение было упомянуто более 70 000 000 раз в социальных сетях. При этом 43,5 млн раз только за период декабря 2020 года, предшествовавший январскому инциденту. Особый интерес вызывает графики активности темы Stop The Steal в социальных сетях. Согласно ним, наибольшая активность публикаций на указанную тему совпадала с днями протестной активности (рис. 10). Виртуальное сообщество, появившееся 7 сентября, стремительно росло - во многом, благодаря риторике президента Дональда Трампа, публично нейтрально оценивающего различные радикальные движения, такие как QAnon, а также Proud Boys (антифашистское американское движение) и т.д. Сторонники правых радикальных взглядов в этой нейтральности замечали позитивное отношение со стороны президента. В связи с этим именно они активно развивали движение Stop The Steal. Помимо этого, Дональд Трамп открыто поддерживал агрессивные действия, направленные на своих оппонентов, представителей Демократической партии США, в социальных сетях. Так, например, 31 октября 2020 года американский президент выложил видео на своей странице в Twitter с комментарием «Я люблю Техас». На данном видео запечатлен автобус с рекламными слоганами конкурента Джозефа Байдена, остановленный насильно радикалами[107]. Подобные проявления симпатии к насильственным действиям стали основой конфликтной мобилизации населения в виртуальном пространстве. При этом целью такой мобилизации было привлечение своих сторонников к участию в выборах. Существенный всплеск активности упоминаний движения Stop The Steal пришелся на выборы 4 ноября 2020 года. Были созданы несколько групп в социальной

[107] Biden campaign says Trump supporters tried to force bus off highway // The Guardian URL: www.theguardian.com/us-news/2020/oct/31/biden-harris-bus-texas-trump-supporters-highway (дата обращения: 20.02.2022).

сети Facebook[108] с названием Stop The Steal, призывавших к выходу людей на акции протеста. Однако Facebook блокировал подобные сообщества. В связи с этим был создан отдельный сайт stopthesteal.us, где пользователи продолжили получать информацию. Протесты сторонников Трампа по итогам оглашения результатов выборов президента США стали следующим шагом в организации конфликтной мобилизации населения. Протесты продолжались в течение двух месяцев и в разных городах США. За три

Рисунок 11

недели до атаки на Капитолий, 19 декабря Дональд Трамп опубликовал первое сообщение с призывом участия в митинге (рис. 11).

[108] Социальные сети «Instagram» и «Facebook», принадлежащие компании Meta Platforms, признаны экстремистскими организациями и запрещены на территории России согласно решению Тверского суда, г. Москва

«Питер Наварро опубликовал тридцати шести страничный» доклад об ошибке во время выборов, достаточно существенной для того, чтобы отдать победу Трампу. Отличный доклад Питера. Статистически невозможно было проиграть выборы 2020 года. Большие протесты в Вашингтоне 6 января. Будьте там, будет дико!» - текст публикации президента США. К моменту публикации твита уже было сформировано понимание о том, что в протестах в поддержку Дональда Трампа, помимо его нерадикальных сторонников,

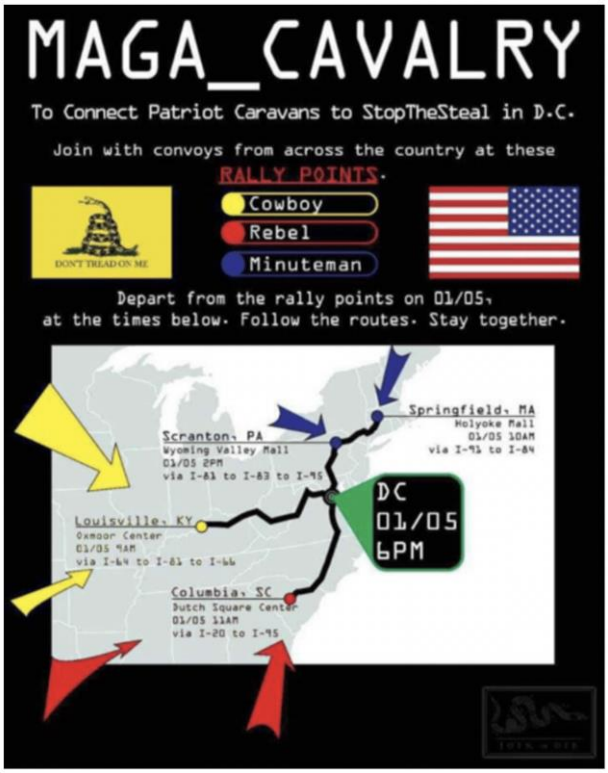

Рисунок 12

участвуют в том числе и представители радикальных правых групп и организаций. В связи с этим подобные сообщения с призывами «будет дико!» могли стать очевидным фактором эскалации конфликтной мобилизации.

Отдельно стоит отметить широкомасштабную мобилизацию радикальных групп к участию в митинге. В рамках мобилизации использовались также технологии по геймификации протеста. Пользователям предлагалось выбрать свою роль и в рамках нее принять участие в митинге (рис. 12).

Помимо наполнения популярных социальных сетей контентом о предстоящем мероприятии, был создан ряд дополнительных ресурсов, подконтрольных команде Дональда Трампа и лояльных ему организаций, на которых также шло распространение информации о митинге 6 января. К таким ресурсам относятся: america.win, wildprotest.com, marchtosaveamerica.com, TheDonald.win.

На этих ресурсах распространялась информация о расположении зданий в комплексе Капитолия, а также о тоннелях между ними и иных важных для захвата здания объектах (рис. 13).

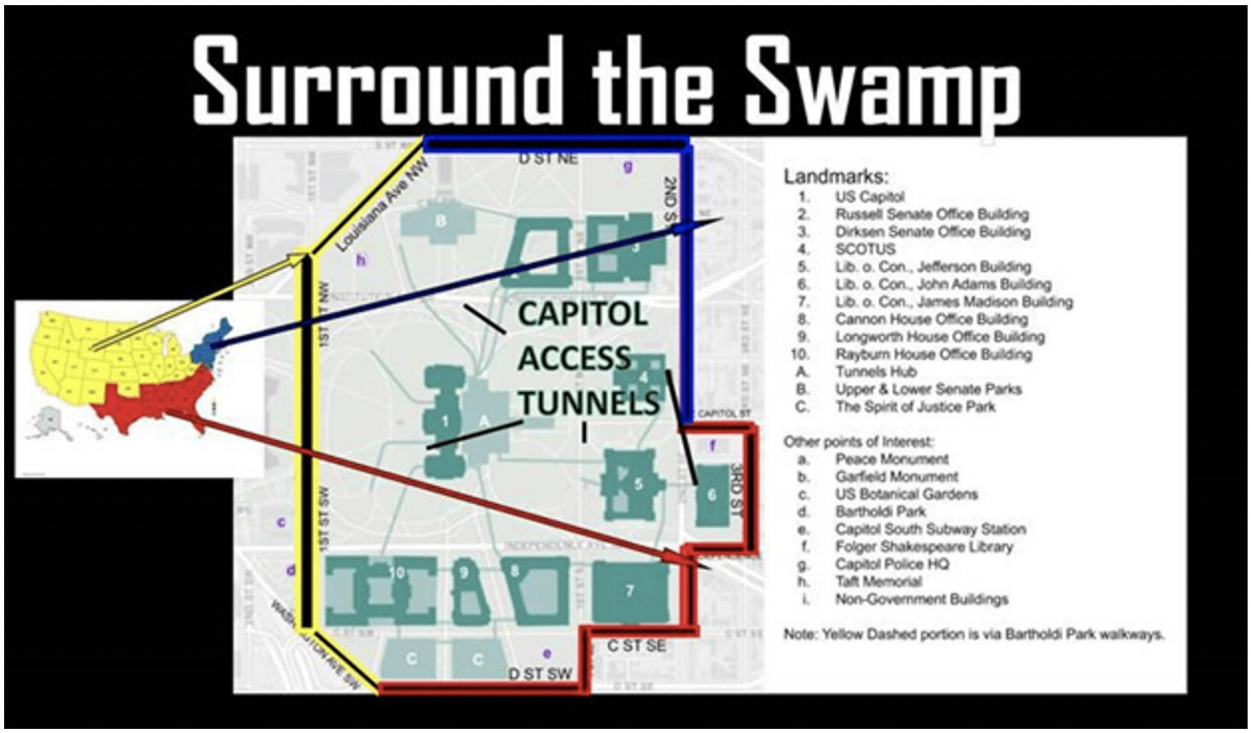

Рисунок 133

В результате подобной мобилизации к участию в митинге присоединились не только граждане, желающие защитить свои политические ценности, но и те, кто воспринял происходящее, как игру и участвовал в ней в образе игрока (рис. 14).

Таким образом, движение Stop The Steal, появившееся за месяц до дня голосования на выборах президента США, смогло объединить в своих рядах сторонников Дональда Трампа, представителей правых радикальных организаций, развернувших широкомасштабную мобилизацию в социальных

Рисунок 144

сетях и специально созданных сайтах. В результате развития этого движения политический митинг 6 января перерос в насильственную политическую акцию, направленную на захват здания американского Капитолия. Отличительными характеристиками кампании по конфликтной мобилизации в социальных сетях в данном случае стали:

1. Открытые призывы к насилию в социальных сетях.
2. Геймификация протеста.
3. Развитие инфраструктурной базы для контроля и управления протестом.

Выводы, полученные в результате анализа политической акции 6 января 2021 года в США, позволяют подчеркнуть важность контроля за публикациями в социальных сетях об участии в политических мероприятиях. Даже сама риторика и источники, призывающие к участию, могут определить тип участников протестной акции. «Громкие» призывы от действующего президента США Дональда Трампа по типу «приходите, это будет дико» спровоцировали восприятие протеста, как не просто политического события, а скорее исторического, имеющего определяющие последствия для жителей США. В связи с этим, многие из участников данного митинга воспринимали свое участие в нем, как роль в

драматическом кино или компьютерной игре, что подтверждается фотографиями, сделанными во время штурма здания Капитолия. Иными словами, характер мобилизации побудил процесс превращения политического события в игру. Несмотря на действия администраторов социальных сетей по недопущению эскалации насилия на этой акции, о которых пойдет речь в следующих частях работы, остановить такой политический протест оказалось невозможно. В том числе, в связи с появлением сразу нескольких ресурсов, получивших возможность

2.3. Стратегии реагирования центральных и региональных органов власти КНР и США на конфликтную мобилизацию

Сравнительный анализ случаев применения интернет-технологий конфликтной мобилизации в США и КНР актуален и потому, что стратегия противодействия данным технологиям в каждой из стран оказалась отличной друг от друга. Особенно это заметно по работе с международными социальными сетями, использовавшимися и в случае протестов в Гонконге в 2019 году, и в прецеденте конфликтной мобилизации в преддверии атаки на Капитолий в США 6 января 2021 года.

Политика социальных сетей в отношении событий в Америке в январе 2021 года состояла в попытке недопущения насильственных действий при сохранении возможности выражать свои взгляды на политические события. Так, социальная сеть Facebook[109] заблокировала самую крупную группу движения Stop The Steal в ноябре 2020 года, за 2 месяца до инцидента 6 января 2021 года[110]. При этом соцсеть отказалась от широкомасштабной «зачистки» информационного поля от упоминаний как о митинге, так и о самом движении Stop The Steal. Лишь после произошедшей атаки на Капитолий Facebook[111] решил удалить все сообщения, относящиеся к акции.

---

[109] Социальные сети «Instagram» и «Facebook», принадлежащие компании Meta Platforms, признаны экстремистскими организациями и запрещены на территории России согласно решению Тверского суда, г. Москва

[110] Facebook bans all 'stop the steal' content // NBC News URL: www.nbcnews.com/tech/tech-news/facebook-bans-all-stop-steal-content-n1253809 (дата обращения: 20.02.2022).

[111] Социальные сети «Instagram» и «Facebook», принадлежащие компании Meta Platforms, признаны экстремистскими организациями и запрещены на территории России согласно решению Тверского суда, г. Москва

Другая социальная сеть, Twitter, которой сорок пятый президент США Дональд Трамп пользовался наиболее активно, еще в мае 2020 года приняла меры против него: некоторые публикации действующего на тот момент президента стали помечаться, как распространяющие дезинформацию или требующие дополнительной верификации, проверки (рис. 15).

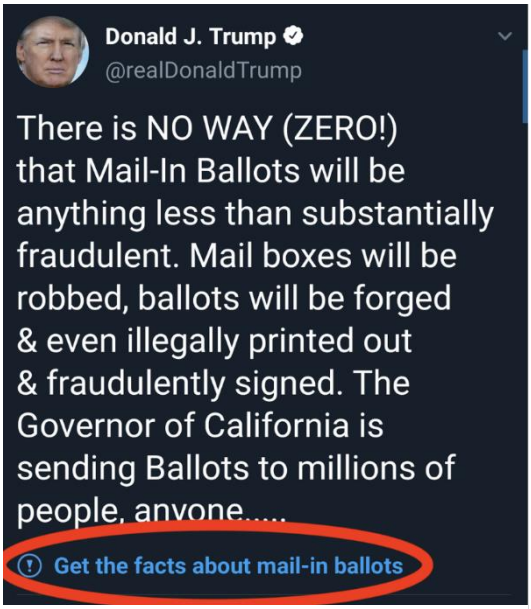

Рисунок 155

При этом ограничительные меры по недопущению распространения информации организаторами митинга 6 января социальная сеть приняла, как и Facebook, только после произошедшего: 11 января был заблокирован один из ключевых организаторов Али Александер, а 8 января был заблокирован сам Дональд Трамп[112].

Стоит отметить, что блокировка на тот момент действующего президента США была основана не на его активности по продвижению идеи участия в демонстрациях 6 января 2021 года, а на двух твиттах, сделанных 8 января 2021 г.:

1. «The 75,000,000 great American Patriots who voted for me, AMERICA FIRST, and MAKE AMERICA GREAT AGAIN, will have a GIANT VOICE long into the future. They will not be disrespected or treated unfairly in any way, shape or form!!!» (англ. Перевод: «75 тысяч патриотов Америки,

[112] Permanent suspension of @realDonaldTrump // Twitter URL: blog.twitter.com/en_us/topics/company/2020/suspension (дата обращения: 20.02.2022).

которые проголосовали за меня, за Америку, за то, чтобы сделать США вновь великими, получат гигантский голос в далеком будущем. Они не будут никем и никак запуганы в какой-либо форме»).

2. «To all of those who have asked, I will not be going to the Inauguration on January 20th.» (англ. Перевод: «Для всех, кто меня спрашивал, я не собираюсь присутствовать на Инаугурации 20 января»).

Социальная сеть Twitter в соответствующем заявлении аргументировала блокировку президента США следующими тезисами[113]:

1. Публикации Д. Трампа спровоцировали восприятие состоявшихся выборов, как нелегитимных.

2. Второй твитт, где Д. Трамп заявляет о том, что не будет присутствовать на Инаугурации, мог спровоцировать атаки во время церемонии, так как этим сообщением Д. Трамп давал понять, что он будет в безопасности в случае подобной атаки.

3. Использование выражения «Американские патриоты» интерпретируется, как поддержка участников беспорядков 6 января 2021 года.

4. Первый твитт, где Д. Трамп убеждает подписчиков в том, что голоса американских патриотов будут всегда услышаны и никто никогда не сможет их заглушить, формируют уверенность в том, что Д. Трамп продолжит поддерживать людей, не считающих выборы легитимными.

5. Действия Д. Трампа по эскалации насилия, в частности, его призывы к повторной попытке захвата Капитолия 17 января 2021 г.

Данные аргументы для блокировки аккаунта действующего президента США не представляется возможным называть объективными. Их интерпретация говорит о приверженности соцсети позиции исключительно позитивного восприятия итогов выборов. При этом известно о том, что Twitter, как и другие социальные сети, зачастую подвергают сомнению

[113] Permanent suspension of @realDonaldTrump // Twitter URL: blog.twitter.com/en_us/topics/company/2020/suspension (дата обращения: 20.02.2022).

результаты выборов в других государствах, в том числе и в Российской Федерации[114]. Безусловно, факт легитимности состоявшихся выборов и иных форм волеизъявления населения фиксируют центральные избирательные комиссии стран или аналоги таких органов. Единой позицией для социальных сетей мог бы стать общий подход по признанию выборов легитимными вслед за аналогичным решением подобных органов. Однако данное сравнение, безусловно, является свидетельством гибкой позиции Twitter по восприятию итогов выборов в разных государствах. Более того, в основе этого восприятия зачастую лежат личные взгляды владельцев или топ-менеджеров социальных сетей.

Тем не менее, американские власти обвиняют Twitter и другие социальные сети в том, что последние допустили мобилизацию радикальных представителей американского общества на своих ресурсах. Так, американским правительством был сформирован «Избранный комитет»[115], целью которого является расследование произошедшей 6 января 2021 года атаки на Капитолий. В функционал данного комитета входит в том числе снятие показания с прямых или косвенных участников события. В повестке, сформированной данным комитетом в адрес руководителя Twitter, в заключении имеется тезис о том, что эта социальная сеть препятствует расследованию дела, так как отказывается предоставить запрошенные комитетом документы по вопросам распространения дезинформации о выборах президента США, об использовании социальной сети лицами, совершающими акты домашнего насилия, экстремистами, иностранными агентами. Также Twitter обвиняют в том, что соцсеть не предоставила комитету документ, согласно которому было принято решение о блокировки

[114] Володенков С. В. Информационное вмешательство как феномен деятельности субъектов современной международной политики // Вестник ВолГУ. Серия 4, История. Регионоведение. Международные отношения. - 2020. - №3.
[115] ABOUT // U.S. House of Representatives URL: january6th.house.gov/about (дата обращения: 20.02.2022).

аккаунта Д. Трампа и иных лиц, участвующих в эскалации насилия, приведшего к атаке на Капитолий[116].

Таким образом, можно сделать вывод о том, что социальные сети, даже при их очевидно лояльной политике по отношению к правительству, не могут в полной мере обеспечить прозрачность как своих действий, так и деятельности пользователей на своих ресурсах. Этот тезис является ключевым в восприятии роли социальных сетей по сохранению стабильного политического состояния, а также недопущению актов искусственной эскалации конфликта с привлечением ресурсов этих интернет-площадок. Очевидно, что совокупность факторов, в числе которых отсутствие постоянного контроля за политическими акциями, личные интересы владельцев и топ-менеджеров социальных сетей, а также непрозрачные решения, принимаемые во время политического конфликта, не могут предоставить возможность правительствам различных государств делегировать функции мониторинга и контроля за виртуальной политической средой представителям социальных сетей.

Подтверждение тезиса об отсутствии единого подхода к обеспечению правопорядка со стороны социальных сетей можно найти на примере протестов в Гонконге. Китайское правительство, являющееся стороной конфликта, организовало работу в международных социальных сетях по продвижению собственной повестки. Напомним, что такие международное социальные сети, как Facebook и Twitter, доступны на территории Гонконга, в отличие от ситуации на материковой части Китая, где нет доступа к названным ресурсам. Китайское правительство использовало возможности рекламного кабинета Facebook и Twitter для популяризации своих антипротестных публикаций среди населения Гонконга[117]. Однако администрации социальных сетей заблокировали такую возможность.

---

[116] January 13, 2022 // U.S. House of Representatives URL: january6th.house.gov/sites/democrats.january6th.house.gov/files/2022-1-13.BGT%20Letter%20to%20Twitter%20-%20Cover%20Letter%20and%20Schedule_Redacted.pdf. (дата обращения: 22.02.2022)

[117] China Attacks Hong Kong Protesters With Fake Social Posts // Wired URL: www.wired.com/story/china-twitter-facebook-hong-kong-protests-disinformation (дата обращения: 20.02.2022).

Каждая из них выступила с заявлением, в котором подтвердила свой отказ от предоставления доступа к рекламному кабинету СМИ и иным акторам, имеющим отношение к китайскому правительству[118]. В то же время, Twitter и Facebook заблокировали более девятисот аккаунтов, связанных с китайским правительством, а Facebook обнаружил и заблокировал группы, распространяющие прокитайский контент (рис. 16).

Рисунок 166 - Перевод: «протестующие и боевики ИГ

В качестве аргументов для блокировки Facebook[119] представил ряд картинок (рис. 17), опубликованных в группах, которые администрация социальной сети посчитала неприемлемыми[120].

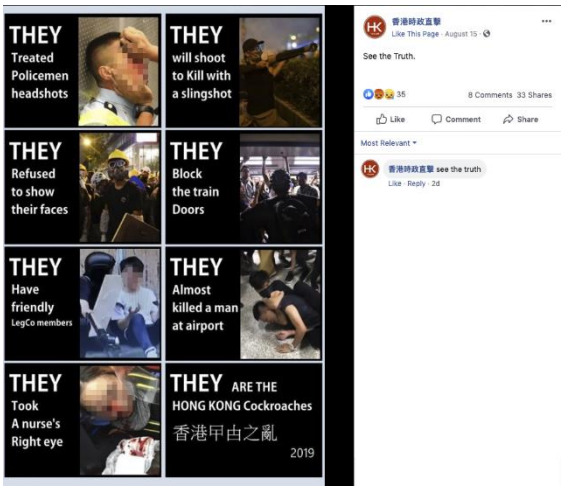

Рисунок 17 - Перечисление случаев насилия

---

[118] Facebook, Twitter accuse China of spreading Hong Kong disinformation // LA Times URL: www.latimes.com/business/story/2019-08-19/facebook-twitter-china-disinformation-hong-kong-protests (дата обращения: 20.02.2022).

[119] Социальные сети «Instagram» и «Facebook», принадлежащие компании Meta Platforms, признаны экстремистскими организациями и запрещены на территории России согласно решению Тверского суда, г. Москва.

[120] Removing Coordinated Inauthentic Behavior From China // Facebook URL: about.fb.com/news/2019/08/removing-cib-china/ (дата обращения: 20.02.2022).

[120] Information operations directed at Hong Kong // Twitter URL: blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong (дата обращения: 20.02.2022).

Социальная сеть Twitter же обосновала свои блокировки следующими примерами контента[121] (рис. 18):

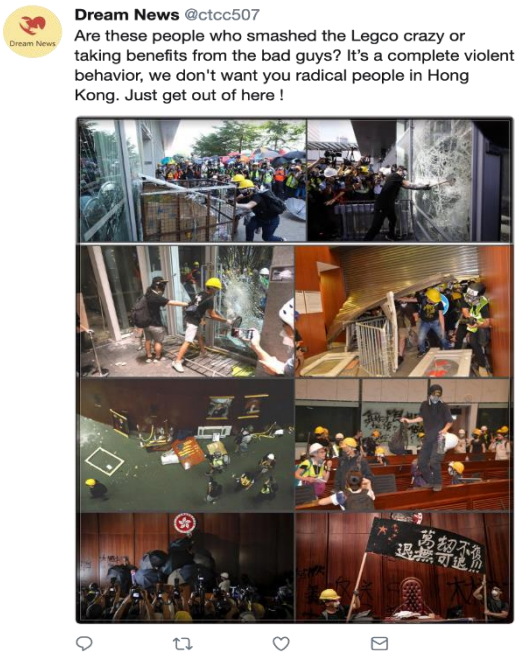

Рисунок 18

Перевод: «Неужели люди, которые уничтожили торговый центр реально получили от этого какое-то преимущество? Это в чистом виде акт насилия, мы не хотим видеть радикалов в Гонконге. Убирайтесь!»

Подобные публикации стали поводом для блокировок почти тысячи аккаунтов в Twitter.

Помимо Twitter и Facebook, китайское правительство также использовало и видеохостинг YouTube, в котором размещались видео в поддержку властей Гонконга[122].

Однако роль перечисленных социальных сетей в политическом кризисе 2019 года в Гонконге была значительно ниже, чем роль, например, мессенджера Telegram. Аудитория сервиса в городе за период конфликта увеличилась на сто десять тысяч пользователей, что при общем количестве населения в семь с половиной миллионов человек, является существенным

---

[121] Information operations directed at Hong Kong // Twitter URL: blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong (дата обращения: 20.02.2022).

[122] How China used Facebook, Twitter, and YouTube to spread disinformation about the Hong Kong protests // Vox URL: www.vox.com/recode/2019/8/20/20813660/china-facebook-twitter-hong-kong-protests-social-media (дата обращения: 20.02.2022).

значением. Попытки принять превентивные меры по недопущению эскалации конфликта в Telegram со стороны лояльных к руководству Гонконга пользователей не предпринимались. Это привело к тому, что данная социальная сеть превратилась в «главный виртуальный инструмент протеста». Тем не менее, нападки на представителей полиции не могли остаться незамеченными со стороны властей и по завершению острой фазы конфликта правосудие Гонконга открыло дело на администратора одной из страниц Siu Cheung-lung (Сюь Ченг Лунга). В результате он был приговорен к 4 годам лишения свободы по причине распространения персональных данных полицейских, распространении информации о способах подготовки бомб и иных видов вооружения[123].

Таким образом, можно сделать вывод о методологии представителей власти в Гонконге по противодействию интернет-технологиям конфликтной мобилизации, реализованной во время политического кризиса 2019 года. Одной из ключевых особенностей стало использование международных социальных сетей для формирования альтернативной повестки, способной представить ситуацию конфликта, отличную от про-протестной картинки. Успех данного инструмента нельзя называть существенным в связи с быстрой блокировкой страниц, распространяющих подобный контент, администраторами социальных сетей.

Следующей особенностью является отсутствие должного внимания к новым средствам онлайн-коммуникации, таким, как Telegram и LIHKG. Гонконгские власти не придавали значения данным инструментам в связи с их низкой популярностью, поэтому не смогли быстро выработать и реализовать сценарий противодействия интернет-технологиям политической мобилизации на этих площадках.

Также стоит отметить тот факт, что правительство Гонконга отказалось от метода блокировки всех социальных сетей для купирования

[123] Telegram user jailed for inciting riots // The Standard URL: www.thestandard.com.hk/section-news/section/4/236769/Telegram-user-jailed-for-inciting-riots (дата обращения: 20.02.2022).

виртуальной эскалации конфликта. На этапе уже сформированной протестной группы власти заблокировали доступ к Telegram и LINKG, однако данное решение не повлияло кардинальным образом на развитие ситуации. Более того, поняв безуспешность поздней блокировки далее правительств Гонконга восстановило доступ к социальной сети LINKG. Вероятно, это было сделано с учетом потенциального влияния первой особенности – распространения проправительственного контента. У данного решения были свои плюсы и минусы. К минусам стоит отнести предоставление возможности для протестующих продолжить эффективную координацию и планирование акций протеста. Очевидным преимуществом данного решения стоит обозначить лишение международных сил возможности оказывать дополнительное давление на представителей власти, используя аргументацию, связанную с ущемлением свободы слова.

Выводы к Главе II

В рамках данной главы были рассмотрены 2 примера политических кризисов, в рамках которых существенное влияние оказали интернет-технологии конфликтной мобилизации. В результате анализа данных прецедентов удалось сформулировать следующие выводы.

Во-первых, подтвержден тезис об эффективности социальных сетей на этапе эскалации политического конфликта. Так, в случае отсутствия каких-либо контрмер, социальные сети позволяют организовать силовое противостояние даже в государствах с высоким уровнем доверия к институтам власти и полиции

Во-вторых, в современных политических кризисах, где используются интернет-технологии конфликтной мобилизации, есть тенденция применения различных площадок на разных этапах. В большинстве случаев начальная стадия эскалации конфликта происходит в международных социальных сетях, таких, как Facebook, Twitter, Instagram[124], YouTube, WhatsApp[125]. Далее управление конфликтом переходит в локальные или неразвитые на территории конфликта социальные сети, сайты и иные инструменты. Причиной такого являются два фактора: политика администраций крупных социальных сетей, не позволяющих акторам конфликта развивать его на своих платформах, а также пристальное внимание к таким инструментам со стороны правоохранительных сил государства. В отличии от Facebook

[124] Социальные сети «Instagram» и «Facebook», принадлежащие компании Meta Platforms, признаны экстремисткими организациями и запрещены на территории России согласно решению Тверского суда, г. Москва.

[125] Ланге О.В. Современные манипулятивные технологии: вопросы теории и методологии: диссертация на соискание степени кандидата политических наук: 23.00.01. СПб., 2015. - 173 с.

локальные социальные сети находятся под меньшим контролем, что дает преимущество организаторам протестной активности в вопросах координации и планирования протеста.

В-третьих, был выявлен новый инструмент онлайн технологий конфликтной мобилизации – геймификация протеста. Он использовался как во время конфликта в Гонконге, где граждане, участвующие в акциях протеста, выбирали роли и действовали на улицах в зависимости от ролевых задач, так и во время атаки на Капитолий в США, где фактор геймификации помог привлечь к конфликту радикальных представителей американского общества, воспринявших акцию, как игру. Подобный инструмент позволяет реализовать следующие функции: в первую очередь, он способен привлечь новых участников конфликта, которым сама возможность «сыграть» в игру важнее, чем демонстрация своей политической позиции. Также, геймификация протеста позволяет продлить его активную фазу, превратив конфликт в затяжную стратегическую игру оппозиции против полиции.

В-четвертых, политический конфликт является фактором, влияющим на появление новых онлайн-платформ или развитии ранее непопулярных социальных сетей и мессенджеров. Современные подходы к противодействию интернет-технологиям конфликтной мобилизации привели к пониманию администраторами протестных групп и сообществ, что их ресурсы могут быть быстро заблокированы. В связи с этим они предпочитают использовать те платформы, которые еще не находятся под постоянным контролем со стороны правоохранительных и иных служб государства.

В-пятых, был сформулирован вывод о том, что крупные социальные сети, несмотря на развитие своих собственных ресурсов по недопущению эскалации конфликтов, не способны обеспечить прозрачность своих действий по сдерживанию или, наоборот, эскалации политических конфликтов. Так называемые «двойные стандарты» методов контроля за развитием политического кризиса на своих платформах не позволяют

делегировать администраторам социальных сетей вопросы по сохранению политической стабильности государств.

В-шестых, обращает на себя внимание вывод о снижении роли контрмер, применяемых в крупных социальных сетях (Facebook, Twitter, Instagram, WhatsApp)[126], как правило представителями властей в связи с противодействием со стороны этих социальных сетей. Так, в ряде стран, не являющихся частью современной западной, англо-саксонской и европейской политической культуры, социальные сети блокируют антипротестные сообщения в связи с рядом правил этих же социальных сетей, запрещающих политическое насилие, пропаганду и дезинформацию. Таким образом, развернутая кампания по недопущению распространения лишь одного оппозиционного варианта представления политической ситуации силами сторонников текущих властей ущемляется владельцами социальных сетей, тем самым потворствующих силам оппозиции вне зависимости от взглядов и предпочтений граждан государства[127].

Данные выводы являются основой для изучения феномена интернет-технологий конфликтной мобилизации с точки зрения анализа современных

[126] Социальные сети «Instagram» и «Facebook», принадлежащие компании Meta Platforms, признаны экстремисткими организациями и запрещены на территории России согласно решению Тверского суда, г. Москва.

[127] Пономарев Н.А., Нешков С.В. Видеоигра “People Power” как средство подготовки организаторов кампании ненасильственной борьбы // Вестник Московского университета. Серия 12: Политические науки. - 2018. - № 4, С. 99-111.

Глава 3. Особенности противодействия технологиям конфликтной мобилизации в интернет-пространстве

3.1 Подход Китайской Народной Республики к противодействию интернет-технологиям политической мобилизации

Прежде чем говорить о китайском подходе к противодействию технологиям политической мобилизации в Интернете, считаем необходимым привести некоторые статистические данные. Так, количество активных пользователей Интернета в Китае в 2020 году достигло показателя в девятьсот восемьдесят девять миллионов человек. Это 70,5% населения страны[128]. При этом доступ к мобильному Интернету есть у 98,3% от числа всех пользователей сети. Китайский сегмент Интернета растет и на примере использования различных приложений. Программами для осуществления банковских операций пользуются 71,9% всех пользователей Интернета. Популярный в Китае мессенджер WeChat собрал семьсот миллионов активных пользователей. Количество пользователей китайским языковым сегментом Интернета составило 19,4% от общего количества пользователей в мире. Это второй показатель в мире после английского языкового сегмента со значением в 25,3%. Данные факты говорят нам о значительной роли

[128] Число пользователей интернета в Китае приблизилось к 1 млрд человек // Коммерсантъ URL: www.kommersant.ru/doc/4672801 (дата обращения: 20.02.2022).

китайского сегмента Интернета, о его возможностях, о его объеме рынка и о сложности контроля за ним. Однако, несмотря на такие показатели, китайское правительство умело выстроило систему контроля за всем потоком информации в Интернете на территории Китая, а также установило свои правила пользования им для обычных граждан, компаний, СМИ и т.д.

Подход Китайской Народной Республики по обеспечению информационной безопасности – один из наиболее крайних вариантов решения существующей проблемы безопасности интернет-пространства. История интернета в Китае отлична от той, что есть в других странах мира. Интернет для правительства Китая всегда был инструментом развития и обучения, но не развлечения. Данная позиция определила сразу 2 фактора: во-первых, быстрое распространение доступа в сеть на территории Китая, включая небольшие деревни, а во-вторых, целостную политику властей в отношении интернета.

Китайский сегмент Интернета отличается централизацией. Это именно тот фактор, по которому можно прочертить разделительную линию мирового Интернета от китайского. В стране осуществляется контроль за сетью, определены правила пользования Интернетом физических и юридических лиц, созданы барьеры и фильтры для доступа во внешний сегмент Интернета. Контроль осуществляется сразу несколькими правительственными органами Китая. Среди них: Национальная администрация радио и телевидения, Министерство по делам культуры, Главное государственное управление КНР по делам прессы и издательств, Министерство промышленности и информации, Министерство общественной безопасности, Главное таможенное управление и др. Эти государственные органы осуществляют контроль за Интернетом в рамках своих компетенций.

Интернет в Китае иерархизирован и централизован. В основе иерархии лежит разделение Интернета на 3 сферы – локальную, государственную и межгосударственную. Локальная отвечает за состояние

информационной безопасности на уровне ограниченных территориальных образований, школьных и университетских сетей, муниципальных органов и т.д. Государственная действует в рамках территории Китая, цензурируя и блокируя ресурсы или пользователей. Что касается межгосударственного уровня доступа в Интернет, то стоит отметить, что он наиболее подвержен инструментам фильтрации информации. Вход во внешний Интернет осуществляется с помощью государственных серверов, позволяющих правительству контролировать весь поток информации, доступ к которому имеют граждане Китая. Также стоит отметить, что в настоящий момент в Китайской Народной Республике существуют 6 провайдеров, обеспечивающих доступ в Интернет на всей территории Китая: China Telecom, China Unicom, China Mobile, CSRNET, CERNET, CIETNET. Первые три – провайдеры общего пользования, наиболее популярным среди них является China Mobile. Последние три предоставляют доступ в определенные сегменты Интернета. Так, CSRNET необходим для научно-исследовательской работы, CERNET – для образования, а CIETNET предоставляет возможность выхода в коммерческий сегмент китайского Интернета. Такое разделение, с одной стороны, позволяет пользователям ориентироваться в Интернете, а с другой, обеспечивает государству легкий доступ к анализу действий пользователей.

Для демонстрации того, насколько ответственно китайское правительство относится к контролю за происходящем в китайском сегменте Интернета, приведем следующий пример. Так, в июле 2017 года многие пользователи заметили, что все сообщения, посты в различных социальных сетях, статьи на сайтах, зарегистрированных в КНР блокируются, если в них присутствует «эмодзи» (визуальная картинка, использующаяся в текстовом сообщении) свечи. Связано это с тем, что 13 июля скончался известный китайский диссидент, правозащитник Лю Сяобо (Liu Xiaobo). Многие пользователи в память о нем писали посты, используя «эмодзи» свечи. Чтобы не допустить «лишней» информации о правозащитнике и не

популяризировать его образ, китайское правительство решило удалить все посты, содержащие этот символ. Этот пример показывает нам мощь китайской машины контроля и готовность заблокировать любую информацию, если она является в какой-то степени опасной для правительства[129].

Таким образом, можно прийти к выводу, что Интернет в Китае полностью подконтролен властям, жестко иерархизирован и сегментирован. Такое состояние Интернета позволяет добиться максимальной информационной безопасности.

Для получения доступа в Интернет каждый гражданин должен пройти проверку в полиции, получить справку и передать ее провайдеру. После этого, ему назначается собственный индивидуальный номер, с помощью которого он сможет регистрироваться на разных ресурсах в Интернете.

Юридические лица получают доступ в интернет только после многомесячной проверки деятельности компании, а также при соблюдении некоторых правил, например, необходимо иметь крупный уставной капитал. Помимо этого, китайское правительство требует внесения взносов на покрытие расходов, связанных с контролем со стороны государства за самой компанией. Эти взносы эквивалентны расходам на наём ИТ-специалистов, которые будут заниматься мониторингом, развитие дата-центров и т.д. Поэтому сумма взносов зависит от размера трафика, на который ориентируется компания.

В КНР отсутствует возможность пользования Интернетом анонимно. При регистрации каждый пользователь указывает свои настоящие данные, индивидуальный номер и после проверки администраторами сайта и провайдером, получает возможность доступа на ресурс.

При нарушении правил пользования Интернетом – например, передаче запрещенных материалов или критике действий властей, человек

[129] Why China’s government is blocking the candle emoji // TechInAsia URL: https://www.techinasia.com/chinas-government-blocking-candle-emoji (дата обращения: 03.03.2019).

получает денежный штраф или лишается доступа в Интернет. В некоторых социальных сетях также внедрена функция контроля за пользователями. Так, например, сервис Sina Weibo при регистрации пользователя выдает ему 80 виртуальных баллов. В случае, если человек нарушает правила пользования социальной сетью, из этих баллов вычитается штраф. Если же человек исчерпал лимит баллов, то его страница удаляется из сети без возможности восстановления.

Следует также сказать, что в Китае отсутствуют известные нам социальные сети – Facebook, Twitter, Instagram, LinkedIn и др. Вместо них представлены местные аналоги. Сделано это с целью ликвидации угрозы информационной безопасности.

Отдельно стоит рассмотреть возможность создания информационного онлайн-ресурса в Китае. Для того, чтобы какое-либо СМИ получило возможность создания собственной интернет-странички, необходимо, чтобы минимум 51% акций этого СМИ принадлежал правительству Китая. Таким образом, в китайском сегменте Интернета не может появиться независимого средства массовой коммуникации.

Помимо этого, в китайской полиции создано специальное отделение киберполиции, которая занимается контролем форумов, социальных сетей и других ресурсов. Киберполицейские следят за комментариями, постами, контентом, блокируют пользователей и ресурсы. Китайское правительство способно заблокировать любой ресурс на своей территории благодаря полному контролю за Интернетом.

Такая политика китайских властей регулируется множеством нормативно-правовых актов. Одним из этих документов является Национальная стратегия безопасности в киберпространстве, принятая Национальным бюро информации по интернету 27 декабря 2016 года[130]. Помимо привычных тезисов о пользе и особенностях Интернета, которые

[130] Сайт Правительства Китая URL: http://www.cac.gov.cn/2016-12/27/c_1120195926.html (дата обращения: 20.02.2022).

можно встретить и в документах российских органов власти, в Стратегии содержится один важный тезис – Китай декларирует, что на китайский сегмент Интернета распространяется национальный суверенитет. Такая позиция разнится с той, которую придерживаются большинство государств на планете, аргументируя это тем, что Интернет создан, чтобы объединять людей, он стоит над государством, представляя собой общую площадку для коммуникации. Китайские власти считают по-другому. Их позиция заключается в том, что безопасность целого государства дороже, нежели возможности отдельного гражданина в киберпространстве. Это различие в подходах вызвало конфронтацию между западным странами и Китаем. Так, например, западное научное сообщество выступило против действий китайских властей, обвинив их в ущемлении прав человека, в частности, свободы слова. Более того, вышли научные статьи, обвиняющие американскую корпорацию Google в помощи китайскому правительству. Следует сказать, что компания ушла из Китая в 2010 году, не сумев договориться с правительством КНР по вопросу блокировки поисковых запросов. Однако, обвиняя Google в помощи КНР, многие отмечают[131], что компания наоборот старалась не становиться на сторону китайского правительства. Так, например, корпорация отказала в возможности гражданам Китая заводить аккаунты для использования электронной почты. Это объясняется тем, что Google хотел обезопасить себя от прессинга со стороны правительства КНР в вопросе доступа к письмам пользователей.

Возвращаясь к Национальной стратегии безопасности в киберпространстве, кажется необходимым перечислить те сферы, которые подвержены угрозам из Интернета. Среди них:

1) Политическая безопасность.
2) Экономическая безопасность.
3) Культурная безопасность.

[131] Kim, S. W., & Douai, A. Google vs. China's "Great Firewall": Ethical implications for free speech and sovereignty. Technology in Society. – 2012. - №34(2). – P. 174–181.

4) Социальное обеспечение.

5) Внешняя политика.

Среди основных угроз в тексте значатся кибертерроризм, международное влияние, «вредная информация», преступная деятельность и др. Особо следует отметить пункт «вредная информация», свидетельствующий о принципах управления страной китайским правительством.

Большая часть документа посвящена вопросу об организации международного контроля за киберпространством. Авторы стратегии предлагают следующие шаги в этом вопросе:

1) Уважение со стороны мирового сообщества к киберсуверенитету.

2) Мирное использование киберпространства.

3) Управление киберпространством в соответствии с законами государств.

4) Координация действий в вопросе безопасности и развития сети.

Данные четыре пункта, по мнению китайских властей, должны сделать киберпространство безопасным. Принимая этот тезис, нельзя обойти стороной отсутствие в этой части документа вопросов о свободе доступа к информации и свободе самовыражения граждан в киберпространстве. Приведенные китайской стороной шаги удовлетворяют интересам информационной политики Китая. Приняв их, другие страны мира лишь подтвердят право Китая на тотальный контроль за своими гражданами в Интернет-пространстве.

Также в документе значатся те задачи, которые Китай будет решать в Интернете:

1) Защита киберсуверенитета

2) Обеспечение национальной безопасности

3) Защита критически важной информационной инфраструктуры

4) Укрепление сетевой культуры граждан

5) Борьба с киберпреступлениями и кибертеррором

6) Улучшение системы управления Интернетом

7) Укрепление международного сотрудничества в киберпространстве

Однако регулирование китайского интернета не определяется исключительно Национальной стратегией безопасности в киберпространстве. Для управления виртуальным пространством правительство КНР приняло также и иные нормативно-правовые акты, среди которых: Закон о защите личной информации (2017), Закон о безопасности данных (2015), Закон о криптографии (2019), Антитеррористический акт (2015)[132].

Данные юридические документы позволяют правительству Китая регулировать деятельность в интернете по следующим вопросам:

1. Сбор и обработка персональных данных граждан;
2. Контроль за данными и их сохранение в единой государственной базе;
3. Доступ к частной переписке и всем данным пользователей, обеспечивающийся при запросе правоохранительных органов без санкции суда.

Как уже было сказано, китайский подход к кибербезопасности разнится с тем, к чему привыкло западное общество. Безусловно, основные претензии связанны с правами граждан. Необходимо обратить внимание и на другую проблему. Тотальный контроль за сегментом китайского Интернета не способен в полной мере защитить Китай от угроз технологий политической мобилизации. Здесь следует остановиться на примере протестов в Гонконге в 2014 году. Тогда жители Специального Административного района Гонконг «встретили в штыки» решение Пекина контролировать выборный процесс в местные органы власти. Кроме этого, жители района требовали предоставить им подлинное всеобщее избирательное право и желали ухода в отставку главы Гонконга. Активисты,

[132] О современной политике Китая в киберпространстве // D-russia URL: d-russia.ru/o-sovremennoj-politike-kitaja-v-kiberprostranstve.html (дата обращения: 20.02.2022).

среди которых основную массу составляли студенты, заняли несколько улиц города, захватили правительственные здания. С целью ликвидации протеста правительство Китая отправило военнослужащих на место политической акции, а также заблокировало Интернет и мобильную связь жителям Гонконга путем блокировки провайдеров и мобильных операторов. Прикованное к акции международное внимание не позволило китайским властям подавить протест насильственными методами, что позволило активистам занять улицы города на четыре месяца: с сентября по декабрь 2014 года. Учитывая возможности Китая в вопросе разрешения политических споров внутри государства, а также тот факт, что активисты были лишены связи, случай представляется уникальным. Однако уникален он не только самим фактом своего существования, но и тем, что активистам удалось обойти все блокировки китайского правительства и настроить коммуникацию на улицах Гонконга. Сделано это было с помощью мобильного мессенджера FireChat. Принцип его работы не предполагает возможности влияния со стороны государства. С помощью Bluetooth и Wi-Fi между пользователями образуется локальная сеть, через которую люди могут обмениваться информацией. В случае с Гонконгом, активисты использовали FireChat для координации своих действий. Именно эта технология позволила им задержаться на улицах города на такой длительный срок.

Данная технология - не единственное, против чего китайское правительство борется с трудом. В Китае некоторые граждане используют технологию VPN. Она позволяет пользователям заходить на запрещенные сайты, обходя блокировки. Однако с середины 2017 года китайское правительство борется с VPN. Так, например, полностью запретили использование технологии частными лицами. Юридические же лица должны получить специальную лицензию на пользование VPN. Все незарегистрированные сети, созданные с помощью данного инструмента, блокируются. Этим занимается киберполиция. Однако процесс создания таких сетей постоянный, поэтому пока блокируются одни каналы,

появляются другие. Стоит признать, что такой прессинг на технологию VPN позволяет достичь целей, которые ставит правительство Китайской Народной Республики. Количество пользователей, использующих такую технологию при общем количестве населения, невелико. Соответственно, доступ к запрещенным ресурсам у отдельных граждан не может стать причиной массовых акций протеста, так как граждане все равно остаются под контролем правительства. Существуют также и другие технологии, например, браузер Tor, объединяющий анонимных пользователей со всего мира. Однако эти инструменты в Китае заблокированы – власти сумели найти методы их блокировки и реализовали их.

Интерес представляет также политика КНР по развитию межгосударственного защищенного от политических провокаций интернет-пространства. Так, 8 сентября 2020 года Министром иностранных дел КНР Ваном И был предложен документ, предлагающий определить основные правила по деятельности государств и компаний в интернете[133]. Документ получил называние «Глобальная инициатива по безопасности данных». Инициатива носит декларативный характер и включает в себя следующие пункты:

1. Открытое поведение государств и компаний в Сети.

2. Противодействие использование Интернета для нанесения ущерба критической инфраструктуре государств.

3. Прекращение противозаконных действий, направленных на наблюдение и сбор данных о деятельности других государств.

4. Принцип уважение региональных законов и отказ от противодействия обязанности хранить данные компаний на территории иных государств.

[133] China’s Bid to Write the Global Rules on Data Security // The Diplomat URL: thediplomat.com/2020/09/chinas-bid-to-write-the-global-rules-on-data-security/ (дата обращения: 20.02.2022).

5. Уважение к суверенитету и личным данным граждан, запрет на распространение персональных данных в других государствах без разрешения самих граждан.

6. Предоставление возможности получения данных правоохранительными органами в компаниях и государствах по решению суда или путем международных консультаций.

7. Отсутствие в коде программного обеспечения «лазеек» для незаконного получения каких-либо данных.

Анализ документа предоставляет понимание, что правительство КНР уделяет особое внимание проблеме хранения и использования данных. При этом в документе не отражены пункты и какие-либо инициативы по обеспечению стабильности и открытости информационно-политического пространства в интернете. Связано это в первую очередь с тем, что по данному вопросу КНР ориентируется на собственный подход, критикуемый многими государствами западной политической культуры. В связи с этим вопрос открытости информационно-политического пространства в интернете не может быть в основе международных договоренностей Китая и других государств. Международная реакция на предложения Китая не была единой. Российская Федерация поддержала КНР в попытке организации диалога по недопущению развития противоправных действий, связанных с личными и государственными данными в интернете: «Стороны считают, что Глобальная инициатива по обеспечению безопасности данных, выдвинутая Китайской Стороной и в принципиальном плане поддержанная Российской Стороной, предоставляет основу для обсуждения и формирования Рабочей группой мер реагирования на угрозы безопасности данных и другие угрозы международной информационной безопасности»[134]. В то же время реакция Великобритании была противоположной – государство продолжило обвинять

[134] Совместное заявление Российской Федерации и Китайской Народной Республики о международных отношениях, вступающих в новую эпоху, и глобальном устойчивом развитии // Сайт Президента РФ URL: kremlin.ru/supplement/5770 (дата обращения: 20.02.2022).

Китай в организации кибератак и шпионажа за данными в интернете[135]. Следует, однако, отметить тот факт, что КНР осуществила попытку достижения международного консенсуса по поведению государств и компаний в интернете.

В заключении главы, посвященной Китайскому подходу противодействия технологиям политической мобилизации в Интернете, считаем важным продемонстрировать отношение к такой политике со стороны мирового сообщества. Эта часть является важной, так как не только провоцирует конфликты между государствами, защищающими свободу слова и Китаем в информационной среде, но и потому, что данные конфликты приводят к реальным кибератакам на информационную структуру Китая. Принимая данный фактор, необходимо обязательно учитывать его в случае выбора китайского варианта развития Интернета в России.

По данным Freedom House, проводившей исследование, посвященное свободе интернет-пространства, Китай занял позицию лидера несвободного интернета, набрав восемьдесят восемь баллов из ста и опередил Иран, Эфиопию и другие государства. Причинами такой оценки стали несколько факторов: закон о кибербезопасности, согласно которому всем международным интернет-компаниям, необходимо хранить данные о работе своих сервисов в Китае, используя китайские серверы, запрет на контент, порочащий, высмеивающий представителей власти и Си Цзиньпина в частности, блокировки VPN, а также доступ правительства к данным пользователей, возможность легкого доступа к их перепискам, видеозвонкам, электронным письмам и т.д.

В целом мировые лидеры в настоящий момент не высказываются публично против того пути, который выбрал Китай, предоставляя эту

---

[135] Embassy Spokesperson’s Comment on the Remarks by the UK Side about International Development Cooperation and Data Security // Chinese Embassy URL: www.chinese-embassy.org.uk/eng/PressandMedia/Spokepersons/202112/t20211202_10461007.html (дата обращения: 20.02.2022).

возможность для некоммерческих правозащитных организаций. Это объясняется авторитетом страны, а также наличием реальных последствий от обвинений в сторону КНР. Китайское правительство активно использует хакерские атаки с целью добиться своих целей на международной арене. К примеру, китайские хакеры взломали многие правительственные ресурсы Соединенных Штатов Америки с целью убедить американскую сторону пойти на уступки в переговорах о торговом соглашении.

К политике Китая в сети в мире отношение не единое. Многие страны предпочли пойти по стопам КНР в вопросе обеспечения информационной безопасности. Так, например, во Вьетнаме уже действует схожая система контроля за Интернетом, а в Индии правительство рассматривает возможность перехода на этот путь[136]. Заметна поддержка китайского варианта и в России, однако об этом будет сказано в следующих главах.

Итак, китайский подход к кибербезопасности – принимаемый многими странами вариант развития Интернета. Несмотря на то, что этот путь сопряжен с ущемлением прав граждан на свободу слова, защиту персональной информации и т.д., он способен обезопасить государство от внешнего воздействия через Интернет. Однако факт ограничения возможностей граждан в Интернете способен вылиться в серьезное недовольство правительством внутри страны, что приведет к проигранным выборам, увеличению количества протестных акций и т.д. Более того, такой путь заметно тормозит развитие бизнес структур, специализирующихся на сфере IT. В условиях ограниченных экономических возможностей и слабо развитого сегмента предпринимательства, такой вариант может лишь усугубить ситуацию и заметно затормозить развитие государства.

Продемонстрировав китайский вариант развития сети, перейдем к более демократичному подходу к защите от политического влияние через Интернет.

---

[136] India Proposes Chinese-Style Internet Censorship // The New York Times URL: https://www.nytimes.com/2019/02/14/technology/india-internet-censorship.html (дата обращения: 03.03.2019).

3.2 Методы противодействия интернет-технологиям политической мобилизации европейских государств, а также стран Северной Америки

Китайский вариант борьбы с интернет-технологиями политической мобилизации не единственный. Альтернативой ему является подход Соединенных Штатов Америки. США являются страной, в которой впервые появился Интернет, где он развивался стремительнее всего, где находятся штаб-квартиры и офисы крупнейших и наиболее влиятельных интернет-компаний. Это говорит нам о большом опыте Америки в этой сфере. Именно США начали использовать Интернет, как политический инструмент, а многие цветные революции были осуществлены с помощью всемирной паутины людьми, работающими в американских компаниях. Так, например, революция в Египте в 2011 году во многом была реализована с помощью социальных сетей Facebook и Twitter, а вел политическую кампанию, целью которой был государственный переворот, гражданин Египта, проживающий в Объединенных Арабских Эмиратах и возглавляющий один из департаментов компании Google в их арабском отделении. Доминирующая позиция США подкрепляется также и статистическими данными о развитии Интернета в стране. Америка занимает третью позицию по количеству пользователей Интернета с показателем в триста двенадцать миллионов человек. Это составляет 76,16% от всего населения страны. Данные говорят о том, что Интернет стал неотъемлемой частью жизни граждан в США и, соответственно, что политика, проводимая в сети, имеет большое значение для реального политического процесса в стране.

США – одно из самых влиятельных государств в мире на данный момент[137]. Долгое время после распада СССР Америка оставалась единственным глобальным игроком на международной политической арене, однако за последние несколько лет реальную конкуренцию ей навязали Китай и Россия. Такой геополитический статус не только позволяет Штатам влиять на политические процессы в странах третьего мира, но и защищает их от явного внешнеполитического влияния. Безусловно, это не означает, что против США не проводятся политические атаки в киберпространстве, но при этом исключается возможность реализации сценариев, например, цветных революций на территории США с использованием социальных сетей и других ресурсов в Интернете. Объясняется это, в первую очередь тем, что все крупнейшие интернет-компании оказывают помощь правительству США в защите национального и кибер-суверенитета. Однако, несмотря на такую помощь, полностью исключить влияние Интернета на политический процесс в США нельзя. Для подтверждения данного тезиса предлагается рассмотреть выборы президента США в 2016 году, на которых одержал победу кандидат от Республиканской партии Дональд Трамп. Его соперником от демократов была Хиллари Клинтон, старожил американской политики с большим опытом, связями в политических кругах. При изначально более высоких шансах Клинтон на победу, в итоге граждане США выбрали в качестве президента страны именно Трампа. В исследовании не будем вдаваться в подробности предвыборной гонки между кандидатами, однако уделим внимание аспекту международного интернет-влияния на нее.

Итак, использование интернет-технологий политической мобилизации можно наблюдать не только во время протестных акций, но и во время предвыборной кампании. Соединенные Штаты Америки на официальном уровне обвинили Россию в том, что наша страна посредством аккаунтов отдельных пользователей, или же с помощью рекламы в социальных сетях, а

[137] Ranked: World’s Most Influential Countries, 2021 // CEOMAGAZIN, 2021, URL: https://ceoworld.biz/2021/02/10/ranked-worlds-most-influential-countries-2021/ (дата обращения 17.07.2022)

также групп и сообществ помогла Д. Трампу одержать победу на выборах президента США в 2016 году. Об это заявил Директор Национальной разведки США. Далее начался судебный процесс, где сторону обвинения представлял бывший директор ФБР Роберт Мюллер. Несмотря на отсутствие конкретных результатов расследования, в качестве свидетелей был опрошен даже глава Facebook Марк Цукенберг, заверивший судей, прокурора и граждан США, что социальная сеть готова сотрудничать с правительством Штатов и будет бороться с проявлениями политического давления со стороны международных сил.

Ознакомившись с сутью обвинения, необходимо показать, как именно, по мнению американской стороны, осуществлялось это вмешательство. Одним из типичных примеров влияния пророссийских сил на американские выборы было признано распространение «фейк ньюз» - заведомо ложных новостей. Через социальную сеть Facebook с помощью Google Ads – сервиса, позволяющего размещать рекламу - публиковались и распространялись такие «фейковые» новости, не только порочащие честь и достоинство представителя Демократической партии США, но и обвиняющие саму партию в различных политических ошибках. После выборов по этой теме вышло множество статей в крупнейших американских изданиях. Например, The New York Times в ноябре 2016 года опубликовали статью «Inside a Fake News Sausage Factory: ‘This Is All About Income’»[138], в которой демонстрируются примеры таких новостей. Житель Грузии, а также популярный блогер в Канаде создавали новости, поддерживающие Д. Трампа и дискредитирующие его оппонента. Сами пользователи заверили журналистов, связавшихся с ними, что никакой политической составляющей в их действиях не было, лишь желание заработать деньги, которые они получали за количество переходов на их сайты. Тема оказалась популярной, а читателям понравились статьи, поэтому количество подписчиков страниц

[138] Inside a Fake News Sausage Factory: ‘This Is All About Income’ // The New York Times URL: https://www.nytimes.com/2016/11/25/world/europe/fake-news-donald-trump-hillary-clinton-georgia.html?module=inline (дата обращения: 03.03.2021).

быстро росло. И таких аккаунтов, таких новостей (рис. 19) во время президентской кампании было создано множество. При этом в статье утверждалось, что эти граждане имеют отношение к Российской Федерации.

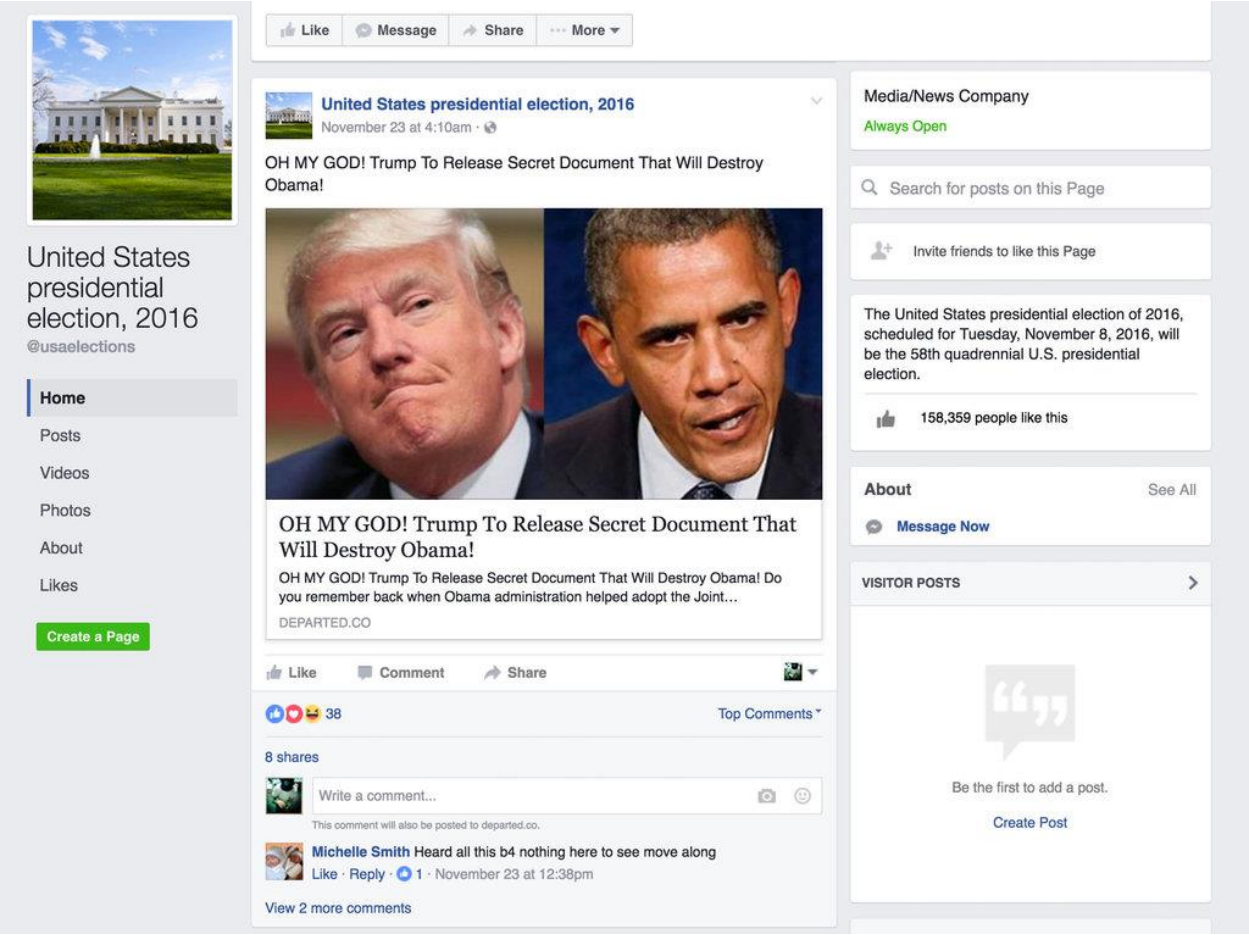

Рисунок 179

Сам же глава Facebook[139] Марк Цукенберг в июле 2018 года указал на то, как Россия вмешивалась в выборы в США. По словам главы корпорации, было создано множество искусственных аккаунтов, распространяющих «фейковые» новости. В российском сегменте Интернета искусственные аккаунты – т.н. боты. Популярность темы вмешательства в выборы в США достигла такой популярность, что многие люди решили отказаться от использования Facebook. Так, например, известный американский актер Джим Керри удалил свою страницу в связи с тем, что социальная сеть не

[139] Социальные сети «Instagram» и «Facebook», принадлежащие компании Meta Platforms, признаны экстремистскими организациями и запрещены на территории России согласно решению Тверского суда, г. Москва

может обеспечить защиту от информационных атак со стороны третьих стран[140].

Facebook извлек уроки из президентской кампании и принялся защищать суверенитет Америки в интернет-пространстве. Накануне выборов в Конгресс в 2018 году социальная сеть удалила более 100 «фейковых» аккаунтов, распространяющих недостоверные новости и стремящихся изменить расклад сил на политическом поле США[141].

Если посмотреть на эту ситуацию в целом, будучи независимыми исследователями, несмотря на то, что обвиняют в киберпреступлениях именно нашу страну, то заметим, что именно такая политика достаточно эффективна для защиты собственного политического пространства от влияния со стороны внешних сил. Стратегия США в этой сфере определяется следующими действиями[142]:

1) Государственная поддержка крупных интернет-компаний.

2) Популяризация «мифа» о вмешательстве иностранных государств в политический процесс

3) Удаление подозрительных аккаунтов в социальных сетях.

Для объяснения нашей позиции, считаем необходимым разобрать каждый отдельный пункт.

Государственная поддержка крупных интернет-компаний выполняет сразу две функции. Во-первых, она расширяет рамки существования компаний. Одно дело, когда социальная сеть существует лишь в рамках одного государства, как, например, в Китае. Тогда политические возможности этой социальной сети сконцентрированы лишь в рамках одного государства и не могут стать инструментом «мягкой силы» на международной политической арене. Во-вторых, поддержка таких компаний

---

[140] Джим Керри удалил свою страницу из Facebook из-за "российского вмешательства" // TSN URL: tsn.ua/ru/svit/dzhim-kerri-udalil-svoyu-stranicu-iz-facebook-iz-za-rossiyskogo-vmeshatelstva-1105557.html (дата обращения: 20.02.2022).

[141] Facebook удалил больше ста подозрительных аккаунтов накануне выборов в Конгресс США // Интерфакс URL: https://www.interfax.ru/world/636547 (дата обращения: 03.03.2021).

[142] Байков С.А. Стратегия коммуникации политической элиты и общества в России в условиях международной конфронтации // Вопросы политологии. - 2021. - Т. 11. - № 3 (67). - С. 719-727.

логичным образом укрепляет взаимоотношения между их менеджментом и государственными институтами, что в случае реальной опасности, как, например, вмешательство в выборы в США, позволит быстро найти общее решение по вопросам противодействия технологиям политической мобилизации. Главная проблема, с которой сталкиваются представители власти, если не превращают глав интернет-компаний в своих союзников, это то, что в самый необходимый момент, они отворачиваются от государства и позволяют действовать против него и его интересов на своих ресурсах. Допускать этого не стоит, если у представителей власти есть желание сохранить существующий государственный строй. Есть и альтернатива такому подходу – угрозы и требования, установленные на законодательном уровне. Однако в этом случае существуют недемократические инструменты, которые могут вызвать лишь неприятие и отторжение со стороны населения.

Второй пункт – популяризация «мифа» о вмешательстве иностранных сил в политический процесс – то, что позволит легитимировать действия властей в интернет-пространстве. Легитимация такой политики необходима, так как без нее власти могут спровоцировать собственное население на участие в протестных акциях. Реализуется такая популяризация с помощью известных СМИ, лидеров общественного мнения (например, действия Джима Керри помогли легитимировать введение дополнительных мер защиты от иностранного вмешательства в социальной сети Facebook), а также реальных политических процессов, как например, судебное разбирательство.

Удаление подозрительных аккаунтов в социальных сетях – третий пункт стратегии США по защите своей безопасности в сфере Интернета. Это скорее лишь частный случай такой политики, однако крайне демонстративный. Можно сказать, что такими удалениями Facebook нарушает права граждан на свободу слова, отстаивание собственных позиций. Но тот факт, что государство предприняло перед этим шагом два других, о которых было упомянуто, переворачивает ситуацию. Теперь общество видит в этих блокировках и удалениях не проявление деспотизма и

авторитарного управления своим ресурсом со стороны Марка Цукенберга, а защиту национальных интересов США. В результате американское правительство получило возможность управления своим сегментом Интернета не с помощью ограничительных мер, а с помощью информационной политики, демонстрации примеров внешнего воздействия. Это лишь укрепило легитимность государственных институтов США и их методов борьбы с информационным влиянием.

Вмешательство в выборы – не единственная угроза, которая стоит перед США. В сентябре 2018 года экз-президент США Дональд Трамп поставил свою подпись на Национальной стратегии США в киберпространстве. Документ состоит из нескольких глав, которые определяют следующие сферы деятельности США в киберпространстве:

1) Защита США путем контроля за сетями, системами и данными

2) Достижение процветания Америки с помощью перехода к цифровой экономике и развитием интернет-инноваций

3) Обеспечение мира и безопасности в интернет-пространстве совместно с союзниками США путем, если это потребуется, наказания тех акторов, которые используют инструменты киберпространства с негативными целями

4) Распространение влияния США в киберпространстве с целью защиты свободного, безопасного Интернета.

Для понимания того, как будут действовать США в своей внутренней и внешней политике по приведенным выше пунктам, необходимо подробно рассмотреть данную стратегию.

Среди методов защиты граждан Америки и самого государства от киберугроз, в документе содержаться следующие:

1) Защита федеральных сетей и информации.

2) Защита инфраструктуры.

3) Борьба с киберпреступностью и улучшение системы отчетности о таких происшествиях. В рамках этой задачи предлагается в том числе создать единую систему защиты от киберугроз совместно со странами-союзниками.

В рамках развития американской экономики и достижение экономического процветания в сфере IT, предлагается следующее:

1) Способствование развитию цифровой экономики

2) Развитие и защита американских инноваций

3) Развитие кадрового потенциала в сфере кибербезопасности

Стратегия США в киберпространстве недвусмысленно определяет свой подход по обеспечению мира в Интернете. Авторы документа предлагают действовать с позиции силы. В рамках главы, посвященной этому блоку вопросов, значатся следующие пункты:

1) Укрепление кибер стабильности через принятие норм ответственности государств за их поведение в киберпространстве.

2) Удерживание государств от неприемлемого поведения в киберпространстве. В рамках этого пункта предлагается объединить усилия разведок союзников США с целью выявления киберугроз, разработать список последствий за «неприемлемое» поведение отдельных государств, а также внедрение системы ответных кибератак на государства, использующие данные методы для достижения своих целей. В качестве главных угроз в этой части документа значатся Иран, Китай, Россия и Северная Корея.

Наиболее интересной частью документа является глава про распространение влияния США в киберпространстве. Среди ключевых пунктов здесь значатся:

1) Развитие открытого, многостороннего и защищенного Интернета. В рамках этого пункта предполагаются следующие шаги: защита свободы Интернета, совместная работа со странами, разделяющими подход США, создание модели мультиполярного управления в Интернете, развитие международной интернет-инфраструктуры, продвижение американских инноваций на международные рынки.

2) Разработка международной киберстратегии, регулирующей экономические и политические вопросы в киберпространстве.

Анализируя документ, кажется очевидным, что главной целью США является создание глобальной системы контроля за Интернетом, в которой главную роль будут играть именно Штаты. Такая система позволит не только защищать собственное государство от киберугроз со стороны других стран, но и позволит распространить американское влияние на киберпространства многих государственных образований. Это позволит США стать доминирующим игроком не только в реальном политическом мире, но и в виртуальном.

Стратегия США в киберпространстве может восприниматься, как элемент новой «холодной войны», где сторону противников Америки занимаются Россия, Китай, Северная Корея и Иран. Если рассматривать политику США с этих позиций, то заметно, что история со вмешательством России в президентские выборы – лишь повод для создания системы общей кибербезопасности. Окончательной же целью является организация проамериканского международного союза по контролю за интернет-пространством. Это в сущности будет означать не только контроль за безопасностью Интернета, но и появление больших возможностей по вмешательству в дела иностранных государств посредством технологий политической мобилизации населения.

Также в мое 2020 года, за несколько месяцев до публикации предложений Китая по обеспечению безопасности данных в киберпространстве, США выдвинули программу «Чистая сеть» (Clean Network), предлагающую регламентировать сферу обработки данных в интернете. Программа носит очевидно антикитайский характер. Ее ключевыми пунктами являются:

1. Запрет на возможность китайских операторов связи подключаться к телекоммуникационным сетям США.

2. Удаление «подозрительных» китайских приложений для телефонов из соответствующих магазинов.

3. Запрет на распространение на территории США китайских смартфонов с предустановленным пакетом приложений.

4. Запрет на обработку данных граждан США китайскими компаниями.

5. Защита интернет-кабелей, проложенных по дну Атлантического океана и обеспечивающих доступ в интернет.

6. Защита технологий 5G от потенциальных рисков со стороны китайских компаний.

Программу поддержал ряд международных компаний и государств, в том числе Албания, Австрия, Бразилия, Эквадор, Япония, Македония, Украина, ЕС и НАТО. Всего более 50 государств присоединились к программе.

Данный прецедент является демонстрацией формирования блоков в сфере работы в интернет-пространстве. Этот тезис приводит к следующему выводу: международный интернет может пойти по пути фрагментации, когда мир лишится общих универсальных правил деятельности в сети.

Интернет и технологии, связанные с ним, находятся в постоянном развитии. Это, безусловно, помогает развитию социально значимых сфер жизни граждан во всем мире. Одной из таких технологий становится 5G сети – пятое поколение мобильной связи, значительно расширяющее скоростные возможности передачи данных, а также их объем. Учитывая перспективы развития данной технологии и потенциальный эффект от них, правительства многих стран мира с опаской подходят к ней. В частности, Государственный департамент США инициировал анализ потенциальных последствий от использования технологии 5G у некоммерческой организации CSIS (Center for strategic and International Studies)[143]. В результате организация предложила

[143] Criteria for Security and Trust in Telecommunications Networks and Services // Amazonaws URL: csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200511_Lewis_5G_v3.pdf (дата обращения: 20.02.2022).

ряд рекомендаций для правительств и компаний, универсальных, по их мнению, для представителей разных стран мира. Рекомендации разделены на несколько категорий, в том числе и политическую, являющуюся наиболее интересной для данного исследования. В список политических рекомендаций по внедрению технологии 5G вошли следующие:

1. Поставщики заслуживают доверия, если их штаб-квартиры находятся в странах с демократически избранными правительствами, о чем свидетельствует наличие независимых оппозиционных партий, чистых выборов, а также присутствует разделение властей на судебную, исполнительную и законодательную.

2. Поставщики заслуживают доверия, если они зарегистрированы в государстве с развитой судебной системой.

3. Поставщики заслуживают доверия, если они зарегистрированы в странах, являющихся партнерами по безопасности с государством-покупателем технологии или оборудования.

4. Поставщики заслуживают доверия, если у государства, где они зарегистрированы, есть доказанная репутация по вопросу защиты персональных данных, а также по вопросу исполнения международных обязательств, таких, как соблюдение прав человека, защита свободы СМИ, отсутствие цензуры, произвольных задержаний и т.д.

5. Поставщики заслуживают доверия, если они выбраны не только в соответствии с фактором цены, но и с учетом факторов условий труда, соблюдения прав человека и экологических стандартов.

6. Поставщики не заслуживают доверия, если в государстве, где они зарегистрированы, есть законы, требующие сотрудничества с локальным правительством.

Данные ограничения или рекомендации, основанные не на экономических, а на политических установках, являются свидетельством того, что Соединенные Штаты Америки в вопросе управления информационно-технологическим полем, в том числе и интернетом,

ориентируются на идею формирования закрытого, лояльного правительству США, круга стран и поставщиков услуг, определяющих всю деятельность в Сети. Этот тезис может быть использован в качестве гипотезы о политике Соединенных Штатов Америки по созданию «лояльного» интернета, где каждый актор является сторонником правительства США и готов соблюдать законы именно этого государства, а не других стран, где данный актор также работает. Данный подход может быть назван империалистическим по отношению к идее свободного интернета с равным доступом в него всех людей в мире.

Итак, Соединенные Штаты Америки используют метод убеждения населения о необходимости контроля за киберпространством с целью формирования «лояльного» интернета. Для этого, они демонстративно ставят свою страну на позицию жертвы политической угрозы, осуществляемой посредством Интернета, проводят кампанию по убеждению населения в том, что необходимо укрепить безопасность национального суверенитета в социальных сетях и других ресурсах, а далее блокируют страницы групп, сообществ, отдельных пользователей, на которых есть какой-либо контент, показывающий Россию или другие страны в позитивном ключе, а правительство США в негативном. При розыгрыше такого сценария, у общества не возникает вопросов «почему заблокирован тот или иной ресурс?», жители наоборот поощряют действия правительства и администраций социальных сетей. В целом такой путь представляется достаточно умелым и политически перспективным. В отличие от китайского варианта, здесь у населения не появляется ощущение полного контроля со стороны властей, а значит действия правительства Штатов в киберпространстве не являются поводом для эскалации политического недовольства граждан. Россия может рассматривать данный подход в качестве одного из вариантов борьбы с технологиями политической мобилизации в Интернете.

3.3. Современные методы противодействия интернет-технологиям политической мобилизации в России

Российская Федерация считается одним из ключевых игроков на международной политической арене в части кибертехнологий. Недаром в Стратегии кибербезопасности США Россия значится, как один из главных соперников.

Общее количество пользователей Интернета в России в 2018 году составило 124 млн человек или 87% населения[144]. Сохраняется общая тенденция перехода пользователей на использование Интернета через мобильные устройства, а не компьютер. При этом, если статистика использования компьютерных устройств говорит, что наиболее популярным ресурсом является поисковик «Яндекс», то статистика мобильных устройств показывает, что большей популярностью пользуется социальная сеть «Вконтакте». Учитывая данную статистику, можем прийти к выводу, что социальные сети для россиян стали неотъемлемой частью жизни.

Этим активно пользуются политические активисты, использующие социальные сети для проведения своих акций. Типичным примером является оппозиционер Навальный А.А. Основатель Фонда борьбы с коррупцией (ФБК признана экстремистской организацией на территории Российской Федерации) в преддверии своих акций мобилизовывал граждан именно с помощью социальных сетей. Так как появление оппозиционного политика на

[144] Число пользователей интернета в России достигло 124 млн // ТАСС URL: https://tass.ru/obschestvo/12698757 (дата обращения: 20.02.2022).

федеральных телеканалах в России крайне затруднительно, то можно сказать, что большинство граждан, пришедших на митинги, организованные политиком – результат деятельности политтехнологов штаба Навального в социальных сетях. Для демонстрации конкретного примера такой мобилизации, предлагается разобрать подготовку к митингу 26 марта 2017 года, основной идеей которого был тезис противодействия коррупции в России.

За 2 недели до митинга ФБК выпустил фильм, посвященный бывшему председателю правительства РФ Медведеву Д.А., обвинив того в коррупционной деятельности. На тот момент группа ФБК в социальной сети «Вконтакте» (где и были сконцентрированы усилия по мобилизации граждан) насчитывала тридцать тысяч подписчиков. После размещения фильма на видеохостиге Youtube и демонстрации его в том числе в «Вконтакте», видеоролик собрал десять миллионов просмотров. Безусловно, это было бы невозможно, если бы он был опубликован исключительно на странице ФБК[145].

[145] Дубровский Г.Д. Протестные события 2019 г. в Москве: анализ политических технологий // Гуманитарное знание и искусственный интеллект: стратегии и инновации. Материалы международной конференции. Министерство науки и высшего образования Российской Федерации, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина. Екатеринбург, 2020. - С. 731-735.

Поэтому Навальный А.А. и его штаб прибегли к идее массового размещения фильма в наиболее крупных сообществах социальной сети

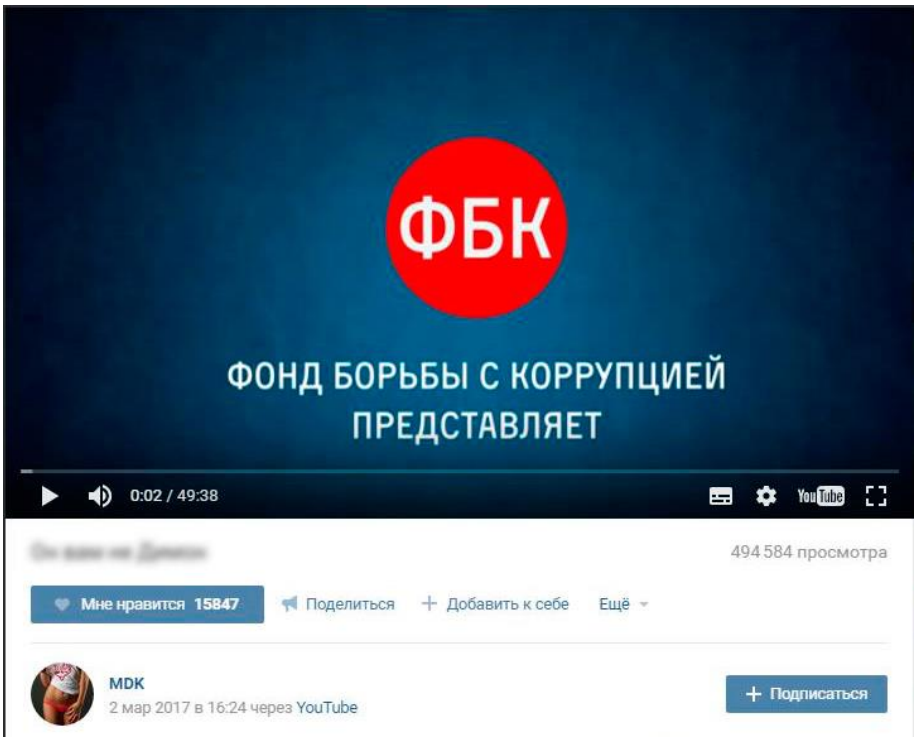

Рисунок 180

«Вконтакте». Среди таких сообществ и развлекательный ресурс «МДК», на тот момент насчитывающий семь миллионов человек (рис. 20).

Помимо «МДК», фильм был распространен и в других популярных группах. Кроме самого фильма, штаб А. Навального работал и с комментариями. В результате на митинги по всей стране 26 марта 2017 года пришло около девяноста тысяч человек.

Кроме этого, можно вспомнить пример кампании Навального А.А. во время предвыборной гонки за пост Президента РФ в 2018 году. Несмотря на то, что ЦИК РФ не допустил оппозиционера до выборов, не зарегистрировал его в качестве кандидата, штаб Навального А.А. все равно начал работу в этом направлении. Практически в каждом субъекте РФ были созданы группы в социальной сети «Вконтакте» с типичным названием «Штаб Навального» и указание города, например, «Штаб Навального в Иркутске», где публиковалась информация о ходе избирательно кампании, о планах Навального А.А., о нарушениях в ходе кампании, публиковались жалобы

граждан, координировались акции протеста и т.д. В среднем, численность каждой такой группы варьировалась от двух до пятнадцати-двадцати тысяч человек. С помощью этой сети Навальному А.А. удалось мобилизовать общество. В день, когда были запланированы акции в поддержку оппозиционера, 28 января 2018 года, в городах по всей России собралось от пяти тысяч человек (официальные данные МВД) до пятнадцати тысяч, а число задержанных составило около трехсот человек.

Другой пример эффективного использования интернет-технологий конфликтной мобилизации приведен в отдельном исследовании автора данной работы по проведению незаконных акций протеста в России в январе 2021 года с использованием технологий эскалации конфликта в социальной сети TikTok[146]. В указанном исследовании было продемонстрировано, как за ограниченный период времени в две недели удалось сформировать виртуальную политическую толпу, лояльную оппозиции.

Важно отметить, что интернет-технологии конфликтной мобилизации используются не только на территории России, но и в союзных для нашего государства странах. Так, они были применены в Белоруссии в период выборов президента в 2020 году. Подготовка к активной стадии конфликта началась за три месяца до дня выборов. В отдельном исследовании[147] автор данной работы определил несколько типов информационных сообщений, отличающихся друг от друга тематикой, и выявил последовательность использования этих сообщений в каждом из временных отрезков в предвыборный период. Основными тематиками стали: формирование негативного отношения к представителям власти и правопорядка, в частности, к президенту Республики Лукашенко А.Г., координация участников митингов, освещение протестных акций с попытками эскалации

[146] Есиев, Э.Т. Соответствие социальной сети TikTok установленным в Российской Федерации методам противодействия интернет-технологиям конфликтной мобилизации // Вопросы политологии. - 2021. - №12(76).
[147] Есиев, Э.Т. Интернет-технологии политической мобилизации в белорусских протестах на предвыборном этапе // Вестник Московского областного университета. – 2021. - №2.

конфликта через демонстрацию насилия, а также тематика позитивного восприятия протестов в государствах с западной политической культурой. Интернет-кампания была разделена на четыре этапа, в каждом из которых выполнялись свои функции. Первые два этапа (общий период которых с 01.05.2020 г. по 30.06.2020 г.) были посвящены формированию виртуальной политической толпы, третий этап (с 01.07.2020 г. по 31.07.2020 г.) был нацелен на превращение виртуальной политической толпы в реальную, способную выйти на улицы и оказать сопротивление органам правопорядка. Четвёртый же этап был посвящен эскалации конфликта власти и общества с увеличением количества протестующих и усилением качества протестов, переходом его в насильственное противостояние.

Таким образом, становится очевидным, что в России так же, как и во многих других государствах используются интернет-технологии политической мобилизации. Более того, проблема их использования носит не внутренний, а внешний характер с учетом влияния не только на Российскую Федерацию, но и на союзные государства. Безусловно, нашему государству также требуется взять на вооружение методы противодействия таким технологиям. Для анализа действий РФ в этом направлении предлагается проанализировать два документа: Доктрину информационной безопасности РФ от 02.12.2016 года, а также Стратегию национальной безопасности РФ от 02.07.2021 года.

Анализируя Стратегию национальной безопасности РФ 2021 года в контексте данной работы, выше уже были приведены основные проблемные позиции, определенные в качестве угроз национальной безопасности. В данной главе приведем и проанализируем методологию противодействия интернет-технологиям конфликтной мобилизации, принятой Стратегией.

Так, основными задачами для сохранения информационной безопасности в Стратегии указаны и формирование безопасной информационной среды, и развитие систем прогнозирования, и недопущение использования инфраструктуры экстремистскими организациями, и, конечно,

предотвращение деструктивного информационно-технического воздействия на российские информационные ресурсы.

Данные задачи действительно являются приоритетными для обеспечения информационной безопасности РФ. Они определяют большинство сфер потенциальных угроз в направлении противодействия интернет-технологиям конфликтной мобилизации: сохранность критической инфраструктуры, защита от пропаганды иностранных государств, развитие внутренних инструментов, обеспечивающих открытый диалог власти с обществом в интернете.

В поддержку Стратегии национальной безопасности, в Доктрине информационной безопасности, принятой 02.07.2016 года четко описаны те тенденции, угрозы, которые существуют в этой сфере, а также конкретные действия по сдерживанию этих угроз. В данной главе предлагаем уделить внимание методам противодействия технологиям информационного влияния, указанным в Доктрине.

В пункте 21 Доктрины информационной безопасности значатся действия по обеспечению военной безопасности от информационных угроз. Наиболее значимым для нас тезисом является следующий: «нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества». Важно отметить, что использовано слово «нейтрализация», а не блокировка, что говорит о стремлении к объективизации информации, а не попытке «зачистить» российский сегмент интернета от «нелояльных» по отношению к власти сообщениям.

В п. 23 Доктрины информационной безопасности РФ перечислены цели противодействия технологиям конфликтной мобилизации в сфере государственной и общественной безопасности. К ним относится: противодействие пропаганде экстремизма, противодействие деятельности, наносящей ущерб национальной безопасности России, профилактика правонарушений в онлайн-сфере, защита критической инфраструктуры и

нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей.

Среди методов достижения безопасности в информационной сфере важно обратить внимание на п. 34 Доктрины, в котором сказано, что необходимо сохранять баланс «между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности». Данный тезис является ключевой идеей российского подхода к противодействию технологиям политической мобилизации в Интернете. Именно он декларирует позицию России, показывая, что наши государственные деятели не намерены идти по китайскому сценарию создания собственной зоны Интернета, защищенной многоуровневой системой фильтров и блокировок.

Оценивая применимость данной доктрины к реальной политике российских властей, можно прийти к выводу, что зачастую те тезисы, которые изложены в ней оказываются проигнорированы политическими деятелями, управленцами и чиновниками.

Перечисленные документы покрывают широкую часть проблемного поля развития интернета и обнаружения угроз для сохранения стабильности политического пространства за счет сдерживания интернет-технологий конфликтной мобилизации. Однако современная ситуация оказывается шире и несет больше угроз, чем те, которые указаны в доктринальных документах.

Так, например, оба документа не учитывают проблематику империалистического подхода Соединенных штатов Америки по управлению интернет-пространством. Помимо этого, в Российской Федерации до сих пор не сформировано собственного подхода к созданию защищенного международного интернет-пространства по типу того, который существует в Китайской Народной Республике или Соединенных штатах Америки. При этом проблематика незащищенного международного пространства для России как никогда актуальна, учитывая реальные попытки дестабилизации

политической ситуации посредством интернета в союзных государствах, например, Белоруссии.

Также в документах не обозначены пути и способы решения проблемы с доверием граждан к действиям власти в интернете. Принцип «жертвы хакерских атак», используемый в США для консолидации общественного мнения по отношению к государственному контролю за социальными сетями, не нашел аналога в России. Многие инициативы государства воспринимаются гражданами негативно, что в определенном смысле блокирует потенциальный набор решений, необходимых для обеспечения виртуальной политической стабильности.

С другой стороны, в России существуют перспективные технологии борьбы с политической мобилизацией в Интернете, которые позволяют обходиться в этом вопросе без блокировок и запретов. Например, ООО «Медиалогия» разработала сервис «Инцидент-менеджмент»[148], который призван обеспечить постоянное присутствие властей РФ в Интернете и отработку негативного контента. Суть работы сервиса сводится к следующему алгоритму: система проводит мониторинг пяти социальных сетей на предмет выявления негативных комментариев, касающихся муниципальной, региональной или федеральной политики. Далее, при появлении большого количества комментариев на одну тему, создается единый запрос, который обрабатывается администраторами ООО «Медиалогия». После обработки этот запрос передается в компетентный государственный орган, где чиновники должны подготовить комментарий с ответом на недовольство граждан в течение одного дня. После этого, ответ регистрируется системой «Инцидент-менеджмент» и автоматически публикуется в социальных сетях к каждому из комментариев, относящихся к этому блоку вопросов. Данная система кажется нам перспективной исходя сразу из двух позиций: во-первых, она способна быстро выявлять проблемы,

[148] Как Кремль будет реагировать на жалобы в соцсетях // РБК URL: https://www.rbc.ru/politics/23/07/2018/5b50d1579a7947c62c195e8b (дата обращения: 03.03.2021).

вызывающие общественный резонанс, что позволит государственным органам РФ реагировать на них и не допускать эскалации конфликтных ситуаций; во-вторых, технология ООО «Медиалогия» способна транслировать позицию государства и объективно демонстрировать шаги государственных органов в вопросах разрешения подобных ситуаций в социальных сетях, где ключевой проблемой как раз и является отсутствие коммуникации с российскими властями. На наш взгляд, система «Инцидент-менеджмент» способна положительно влиять на противодействие интернет-технологиям политической мобилизации, отрабатывая каждый комментарий, пост политически активных граждан, что явным образом усложнит задачу заказчикам протестов.

Также в России создана АНО «ДИАЛОГ», в задачи которой входит организация диалога между властью и обществом в интернете. Помимо этого, стоит отметить открытость представителей власти, многие из которых ведут собственные страницы в социальных сетях.

Общие усилия многих организаций, находящихся в системе государственных органов РФ или являющихся негосударственными организациями, позволили сделать онлайн-пространство более сбалансированным и снизить уровень негатива к представителям власти[149]. Однако текущий статус «КВО» не должен быть фактором, усыпляющим бдительность государственных органов в вопросе защиты от использования интернет-технологий конфликтной мобилизации.

Подводя итог описанию российского подхода в части обеспечения противодействия технологиям конфликтной мобилизации в Интернете, необходимо сказать, что Российская Федерация значительно развила нормативно-правовую базу, определяющую стратегию нашего государства по борьбе с указанным явлением. Однако были обнаружены пробелы,

[149] Матюсова А. И., Есиев Э.Т. Использование губернаторами российских регионов инструментов онлайн-коммуникаций в период режима самоизоляции // Русская политология. - 2020. - №4 (17).

необходимые для исправления путем активных действий по большей части на международной арене.

Среди этих проблем:

1. Отсутствие актуальных решений в документах, представляющих собой нормативно-правовую базу, по противодействию тенденции управления интернет-пространством компаниями и правительством Соединенных штатов Америки.

2. Отсутствие актуальных решений в области формирования позитивного имиджа представителей власти Российской Федерации в интернет-пространстве.

Данные проблемные зоны являются угрозой по сохранению национальной безопасности Российской Федерации. С другой стороны, именно их можно назвать наиболее перспективными точками роста для развития бренда Российской Федерации в интернет-пространстве, а также по формированию новых подходов к обеспечению национальной безопасности в интернете.

3.4. Практические рекомендации по противодействию интернет-технологиям политической мобилизации в Российской Федерации

Подводя итог предыдущей главе, было установлено, что эволюция подхода Российской Федерации в области обеспечения безопасности интернет-пространства обеспечила выработку целостного подхода к принципам, которых придерживается наше государство для сохранения этой безопасности. При этом очевидна необходимость дальнейшего развития нормативно-правовой и практической базы данного направления.

Существующий порядок организации интернет-пространства в будущем может претерпеть существенные изменения. Так, актуален в настоящее время вопрос о его фрагментации. Деятельность многих стран западной политической культуры, а также уже выстроенный закрытый интернет в Китае – подтверждение данного тезиса. Возможен сценарий, при котором и социальные сети будут выбирать, в какой стране функционировать, ориентируясь на показатель лояльности местных властей по отношению к западной политической культуре. Фрагментация, в свою очередь, может стать причиной открытого противоборства в виртуальной среде между «блоками» государств. Текущая политика таких социальных сетей, как Twitter и Facebook по мониторингу и блокировке аккаунтов пользователей, транслирующих на своих страницах подход российских политических сил по различным вопросам, - яркий пример такой виртуальной борьбы.

Продолжающаяся гибридная война против России, включающая использование интернета для формирования негативного образа нашего

государства, будет усиливаться: будут проводиться попытки дестабилизации политической ситуации путем организации онлайн-протестов.

Российская Федерация, как и большинство других государств, находится в ситуации неопределенности в вопросах обеспечения национальной безопасности в интернет-пространстве. Очевидна существующая проблема регламентации поведения в социальных сетях пользователей и организаций всех государств мира. Однако решение данной проблемы еще не найдено.

Российская Федерация выступила с открытой поддержкой инициативы Китайской Народной Республики «Глобальная инициатива по обеспечению безопасности данных». Однако этот документ касается исключительно вопроса о безопасности данных и исключает какие-либо шаги к обеспечению равного и безопасного доступа к социальным сетям и не использованию их в качестве инструмента для продвижения политических интересов одного государства в ущерб политическим интересам другого. Именно в данном направлении Российской Федерации следует искать варианты решения и инициировать их принятие международным сообществом.

Среди вариантов подобных решений предлагается рассмотреть возможность создания международного контрольного органа с делегированием ему функции обеспечения свободы от политически ангажированного контента. Подобный международный орган должен иметь возможность формировать обязательные для исполнения социальными сетями решения. Для этого этот международный орган должен быть признан и администрациями этих социальных сетей. Опыт диалога на подобные темы у Российской Федерации есть. Так, в следствие такой коммуникации удалось договориться с мессенджером Telegram об условиях сотрудничества, после чего Роскомнадзор снял с него[150] санкции, а премьер-министр Российской

[150] О мессенджере Телеграм // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций URL: rkn.gov.ru/news/rsoc/news73050.html (дата обращения: 20.02.2022).

Федерации Михаил Мишустин даже провел встречу с вице-президентом компании Ильей Перекопским[151]. Подобный подход актуален и для организации диалога с представителями других социальных сетей и формированием единого поля сотрудничества.

Уже по итогам подобного диалога возможно создание международного контролирующего органа, реализующего функции по обеспечению чистого от политически ангажированных запретов и кампаний интернет-пространства. При этом, учитывая действия Соединенных Штатов Америки и иных государств западной политической культуры по формированию альянсов и союзов стран, совместно работающих в интернете, предполагается их противодействие созданию такой международной организации и вхождению в нее различных государств. В связи с этим, актуальным решением данного вопроса является поэтапное создание подобной организации, где первым этапом может выступить формирование диалога о создании этого органа на площадках уже существующих международных организаций: ШОС, СНГ, ОДКБ и т.д.

Вторым тезисом-предложением для обеспечения стабильного развития и безопасности Российской Федерации в интернет-пространстве является формирование нормативно-правовой базы для развития отношений власти и общества в интернете. В Российской Федерации ведется активная работа в этом направлении. Так, например, у семидесяти шести из восьмидесяти пяти глав российских регионов есть страницы в социальных сетях[152]. Более того, динамические показатели[153] открытости диалога представителей власти и общества в интернете свидетельствуют о большом внимании к этой проблеме со стороны государства. Однако сохраняется проблема доверия общества к власти в интернете, в том числе в связи с тем,

---

[151] Telegram в гостях у Мишустина // The Bell URL: thebell.io/telegram-v-gostyah-u-mishustina-vstrecha-s-putinym-na-2-mlrd-i-wirecard-s-novichkom (дата обращения: 20.02.2022).

[152] Сторис успеха: рейтинг глав регионов в Instagram // ЦПК URL: cpkr.ru/issledovaniya/tsifrovye-portrety-glav-rossiyskikh-regionov/storis-uspekha-reyting-glav-regionov-v-instagram/ (дата обращения: 20.02.2022).

[153] Открытость государства в России – 2021 // URL: ach.gov.ru/upload/pdf/Otkrytost-2021.pdf (дата обращения: 20.02.2022).

что у граждан нет ориентиров в виде нормативно-правовых актов, регламентирующих деятельность представителей власти в Сети. Таким образом, общение с властью в социальных сетях граждане воспринимают, как «рекламу» первых, а не как способ ведения открытого диалога. Стоит отметить, что соответствующие инициативы уже имеются. В частности, депутаты Государственной Думы ФС РФ вносили на рассмотрение законопроект, который обязал государственные органы открыть свои страницы в социальных сетях. Это, безусловно, один из необходимых законов, но ограничиваться им не стоит. Среди перспективных сфер регулирования деятельности государственных органов в интернете стоит выделить следующие:

1. Диалог между властью и обществом. Так, зачастую граждане жалуются на те или иные недостатки в работе государственных органов в социальных сетях этих органов. Перспективным решением могло бы стать признание подобных комментариев официальным обращением к государственному органу. В этом случае его представители были бы обязаны отвечать на это обращение и в ряде случаев принимать решения в связи с ним. Такой диалог в Сети сделал бы страницы государственных органов популярнее, а доверие к представителям власти могло бы увеличиться.

2. Регламентация процесса информирования о деятельности государственного органа. Так, недостаточно просто завести страницы в социальных сетях и не вести информирования о своей деятельности в них. Открытый диалог помог бы сформировать стабильную повестку в интернет-пространстве.

3. Формирование отдельных государственных страниц в социальных сетях, способных объяснить и донести до широких слоев населения позицию государства по различным политическим вопросам и действиям, которыми занимается государство. Именно такой контент мог бы стать основным источником «альтернативного», не оппозиционного взгляда в интернете во время политических конфликтов в обществе.

Данные шаги будут способствовать увеличению «веса» государства в интернете и его открытости. Это, в свою очередь, позволит повысить уровень доверия к государству в интернет-пространстве и создаст источник диалога с обществом для власти во время политических кризисов и конфликтов.

Третьим шагом по обеспечению политической безопасности в интернет-пространстве является развитие собственной IT-инфраструктуры, способной обеспечить бесперебойную работу серверов и иного оборудования, необходимого для постоянного доступа в интернет граждан, а также для работы крупных промышленных, военных и иных организаций. Российская Федерация делает шаги и в этом направлении[154], однако стоит принять тот факт, что на данным момент эта сфера неразвита. Необходимо увеличивать количество инвестиций в сфере создания IT-инфраструктуры, привлекать к этому вопросу молодежь, формируя соответствующие научные и прикладные программы подготовки в университетах и т.д.

Совокупность данных шагов позволит государству укрепить свой авторитет в социальных сетях, а также повысить роль государства в российском сегменте интернета. Также такой подход привлечет внимание международных социальных сетей к практике России, как к перспективному примеру поведения государства в интернете. Это, в свою очередь, поможет в организации диалога между РФ и международными социальными сетями, который необходим для обеспечения свободного от политически ангажированного контента интернет-пространства.

[154] Яндекс, «ЛАНИТ», Gigabyte и ВТБ построят под Рязанью завод по производству серверов // Яндекс URL: yandex.ru/company/press_releases/2021/2021-10-06 (дата обращения: 20.02.2022).

Выводы к Главе III

Рассмотренные в данной главе варианты подходов США, КНР и России к обеспечению безопасности в интернет-пространстве могут говорить об отсутствии единого понимания перспектив его развития. Отличные друг от друга подходы США и КНР являются двумя «полюсами» возможных практик по поведению государства в социальных сетях. Подходы отличны друг от друга, как в вопросе организации внутригосударственного интернета, так и в вопросе коллективной безопасности в Сети.

Отдельно стоит отметить тот факт, что государства преследуют схожие цели в информационном пространстве и формально похожие механизмы достижения этих целей. Так, общими для подходов являются цели контроля за обработкой персональных данных граждан в интернете, контроль за данными и их хранение на территории государств, соблюдение киберсуверенитета. Общим же методом для достижения целей можно назвать формирование межнациональных институтов или же договоренностей для диалога и защите своих интересов на межгосударственном уровне. Под цифровым или киберсуверенитетом понимается «верховенство и независимость государственной власти при формировании и реализации информационной политики в национальном сегменте и глобальном информационном пространстве»[155]. Еще одним вариантом интерпретации этого феномена является определение профессора Пекинского университета

[155] Кучерявый М. М. Государственная политика информационного суверенитета России в условиях современного глобального мира // Управленческое консультирование. - 2014. - 9 (69). - С. 12.

Вэньсяна Гонга: цифровой суверенитет – верховная власть государства при принятии решений и поддержании информационного порядка в стране[156].

Еще одно определение цифрового суверенитета предложено Володенковым С.В.: «Под цифровым суверенитетом мы понимаем эмерджентное свойство государства как сложной системы, которое возникает в результате адекватного и релевантного параметрам технологического развития человеческой цивилизации соединения цифровой технологической инфраструктуры государства с цифровыми компетенциями и навыками общественных, политических, экономических и управленческих институтов и самих граждан»[157]. Авторское определение цифрового суверенитета – возможность самостоятельного и независимого от влияния иных государств или транснациональных компаний обеспечения технического исполнения правовых норм в цифровом пространстве.

В остальном данные подходы отличаются. В части противодействия интернет-технологиям сетевой конфликтной мобилизации сформированы следующие подходы в рамках предложенной автором работы классификации.

Что касается платформы, на которой реализуются указанные технологии, США сторонник диалога с крупными социальными сетями. При этом сами социальные сети лояльны к американским властям, что выражается в поддержке соцсетями позиции властей во время политических конфликтов. Подход КНР же предполагает полную блокировку и отсутствие диалога с такими социальными сетями. Разные подходы предполагают и разное использование крупных социальных сетей организаторами сетевой конфликтной мобилизации. Так, в США оппозиционные силы не получают поддержки от Facebook, Twitter, YouTube, их сообщения отмечаются, как сомнительные. Оппозиция в КНР напротив, свободна в использовании этих

---

[156] Gong, Wenxiang. Information Sovereignty Reviewed // Peking University. Intercultural Communication studies XIV: 1, 2005.

[157] Володенков С.В., Воронов А.С., Леонтьева Л.С., Сухарева М Цифровой суверенитет современного государства в условиях технологических трансформаций: содержание и особенности // Полилог/Polylogos. - 2021. - Т.5. - №1

площадок, а жители получают к ним доступ при подключении инструментов обхода блокировок.

По критерию субъектности организационного лидера конфликтной мобилизации подходы также отличны. Если в США субъектность зачастую бывает открытой, а государство борется с лидерами протеста правовыми формами или такими же технологиями, то в КНР субъектность в основном скрытая в связи с рисками арестов и реальных тюремных сроков.

По критерию радиуса воздействия технологий у КНР и США разные возможности в части использования фактора межгосударственных контртехнологий сетевой конфликтной мобилизации. Тот факт, что международные социальные сети намного более лояльны к администрации США, чем к правительству КНР, не позволяет Китаю эффективно разворачивать кампании по противодействию виртуальному протесту на этих площадках. В связи с этим организаторы протестов в Китае зачастую прибегают к использованию Facebook и Twitter для поддержки своих активностей. В США же сетевая мобилизация проходит, как правило, на локальном уровне: отдельных сайтах, блогах, группах в мессенджере.

По критерию периода воздействия технологий Китаю, как правило, приходится бороться с технологиями быстрого периода действия – краткосрочными. Это связано с тем, что сформированная в КНР бюрократическая система борьбы с сетевой конфликтной мобилизацией позволяет оперативно купировать и устранять потенциальные источники опасности. В связи с этим использование долгосрочных, перспективных технологий становится для организаторов протестов нерациональным. Это в свою очередь ведет к появлению новых форм и технологий сетевой конфликтной мобилизации, с которыми китайское правительство еще не было знакомо. В США же подобной проблемы не наблюдается и там могут быть одинаково эффективны как краткосрочные, так и долгосрочные технологии.

По критерию акторов распространения информации в США чаще используются технологии с централизованным источником информации, в то время, как в КНР приоритетным вариантом является распределенная передача контента: в рамках виртуального протестного движения образуется множество групп в мессенджерах и социальных сетях, их авторы и участники анонимны. Это связано с высокими рисками задержания активистов китайской системой по недопущению призывов к митингам в интернете.

Таким образом, можем сделать вывод, что в Китае предпочтительнее для борьбы с интернет-технологиями сетевой конфликтной мобилизации подход закрытого, защищенного интернет-пространства с элементами глубокого мониторинга, выявления технологий и их оперативной ликвидации внутри киберпространства КНР. Это приводит к быстрому образованию новых технологий, а также ограничивает Китай в вопросах использования межгосударственных контртехнологий сетевой конфликтной мобилизации.

США же, принимая во внимание факт их лояльных взаимоотношений с администрациями крупнейших социальных сетей, предпочитают разделять и делегировать работу по противодействию интернет-технологиям конфликтной мобилизации администрациям социальных сетей. Это делает их использование различными политическими акторами вероятнее, но при этом менее эффективными за счет отсутствия поддержки со стороны социальных сетей.

Стоит также обозначить проблему международного противодействия в киберпространстве, конфронтации между Китаем и США и использовании социальных сетей в этой борьбе. Данное противостояние не позволяет скорректировать стратегию КНР в отношении международных социальных сетей и делает подход КНР неизменным в обозримой перспективе.

Подход Российской Федерации к противодействию интернет-технологиям сетевой конфликтной мобилизации имеет общие черты, как с подходом Китая, так и США. Современные отношения власти РФ с

администрациями международных социальных сетей заметно деградировали, что приведет в будущем к еще большему давлению с их стороны. При этом российский сегмент интернета в настоящий момент не изолирован по типу китайского. Совокупность данных факторов приведет с росту случаев использования технологий сетевой конфликтной мобилизации. Во многом российский подход к противодействию интернет-технологиям конфликтной мобилизации в настоящий момент претерпевает изменения, связанные с актуальной внешнеполитической ситуацией, наступившей после февраля 2022 года.

В части использования крупных социальных сетей Россия до февраля 2022 года зачастую пользовалась их возможностями: позитивный образ властей формировался на страницах Instagram и Facebook. Во время протестных акций данные социальные сети также использовались и для формирования позитивного отношения к повестке властей. Сейчас ситуация изменилась, а социальные сети компании Meta признаны на территории нашего государства экстремистскими. Государство ограничило доступ к ним и прекратило формировать свой позитивный образ на страницах запрещенных соцсетей. При этом сохраняются возможности для доступа пользователей к ним посредством технических инструментов, например, VPN. В связи с этим, можно спрогнозировать успешное использование крупных социальных сетей технологами будущих социально-политических конфликтов, с учетом отсутствия контрмер со стороны властей.

По критерию субъектности организационного лидера конфликтной мобилизации в России использовался подход открытой субъектности. Существовали политические акторы, представляющие несистемную оппозицию и консолидирующие вокруг себя протестные настроения общества. В настоящий момент таких акторов нет, что делает затруднительным для технологов протестов использование открытой субъектности для мобилизации населения.

Радиус воздействия виртуальных технологий конфликтной мобилизации также в России также был многовекторным: социально-экологические конфликты в большей части были ориентированы на локальную и внутригосударственную аудиторию, в то время, как социально-политические – на внутригосударственную и межгосударственную. Учитывая консолидацию администраций российских социальных сетей: Вконтакте, Одноклассники и т.д., а также блокировку доступа к крупным международным социальным сетям, и, тем самым, снижение возможностей для локальной и внутригосударственной мобилизации, следует ожидать развитие технологий, ориентированных на международные социальные сети.

Критерий периода воздействия технологий также претерпел в российском сегменте интернета изменения. Если ранее организации, близкие к оппозиционным политикам, как и сами эти политики, могли постепенно развивать протестную повестку, как это было сделано в Египте в 2011 году, Белоруссии в 2020, то сейчас их действия значительно ограничены, что не дает возможности получить достаточное количества времени для использования технологий долгосрочного периода воздействия.

Что касается критерия акторов распространения информации о протестной активности в сети, то в сегменте интернета Российской Федерации доминировала до февраля 2022 года тенденция использования оппозицией технологий централизованного источника информации о протесте. Организации, близкие к оппозиционным политикам, создали вертикальную крупную структуру групп и сообществ в социальных сетях уровня «регионы-центр», которая позволяла им эффективно доносить информацию о готовящихся протестных мероприятиях до своей целевой аудитории, запускать рекламу в социальных сетях с призывами принять участие в подобных акциях. В настоящий момент, учитывая отсутствие подобных несистемных оппозиционных сил найти источник централизованного распространения информации о готовящихся в будущем акциях протестов невозможно, что ведет нас к предположению об

использовании в протестах на территории Российской Федерации технологий распределенной передачи информации о политической акции.

Таким образом, была выявлена тенденция изменения методов использования интернет-технологий конфликтной мобилизации в Российской Федерации на основе анализа этих технологий по предложенным автором работы критериям. В связи с таким изменением, необходимо также предложить и рекомендации по нивелированию будущих угроз использования виртуальных технологий конфликтной мобилизации в России.

Во-первых, необходимо развивать в российских социальных сетях, а также в неангажированных международных позитивный образ властей Российской Федерации. Так, например, следует выстроить работу PR-служб глав российских регионов, министерств и иных органов исполнительной и законодательной власти так же эффективно, как это было сделано и в Instagram.

Во-вторых, необходимо продолжать работу над формированием позитивного образа России в зарубежных запрещенных на территории РФ площадках путем использования технологий распределенной передачи информации. Не выполняя данную рекомендацию Российская Федерация рискует столкнуться с тем, что в этих соцсетях будет существовать только антироссийская повестка, что приведет к дополнительной мобилизации пользователей при использовании данных площадок технологами протеста.

В-третьих, следует усилить работу по мониторингу и обнаружению новых виртуальных технологий конфликтной мобилизации. Учитывая, что технологии долгосрочного периода воздействия, как было определено выше, не будут популярны среди организаторов протестов в обозримом будущем, внимание следует уделять современным технологиям краткосрочного периода действия. Они, как правило, интенсивно развиваются, что требует их постоянного выявления и соответствующего мониторинга в протестах за рубежом.

В-четвертых, следует способствовать развитию российских социальных сетей и поощрять их выход на зарубежные рынки. Такая стратегия позволит добиться расширения потенциальной возможности формирования пророссийской позитивной повестки в международном интернет-пространстве. В свою очередь, укрепление роли России в вопросе международного политического киберпространства приведет к началу равного, паритетного диалога с другими государствами и откроет возможность для создания международного курирующего органа по обеспечению контроля за применением интернет-технологий конфликтной мобилизации.

Заключение

В результате проведенного исследования, оценивающего роль виртуальных технологий конфликтной мобилизации в противодействии политическому протесту, удалось сформулировать следующие выводы.

Во-первых, выявлена эволюция развития научного подхода к феномену сетевой конфликтной мобилизации. Определено, что это явление, берущее свое начало из классических теорий коммуникации. Субъекты этих теорий: источник информации, ее передатчик и получатель, нашли свое отражение в современных подходах к анализу данного феномена. Эволюция феномена конфликтной мобилизации в интернете произошла быстро и напрямую связана с появлением социальных сетей. Популярность площадок, где каждый человек является источником информации, побудила технологов протестов начать использование социальных сетей для организации политического противостояния. Активное применение подобные технологии получили во время революций «Арабской весны». В течение десятилетия с этого момента интернет-технологии конфликтной мобилизации появлялись, развивались, эволюционировали и устаревали. Их количество привело к необходимости выявления специфики использования каждой из таких технологий с целью ее анализа и поиска противодействия.

Во-вторых, для определения специфики каждой из имеющихся технологий автором работы была сформулирована классификация интернет-технологий конфликтной мобилизации. Такие технологии были распределены по следующим критериям:

1. Платформа, на которой применяются технологии (видеохостинги, мессенджеры, сайты, приложения);

2. Субъектность организационного лидера протеста (открытая или скрытая);

3. Радиус воздействия технологий (локальные, государственные, межгосударственные);

4. Период воздействия технологий (краткосрочные и перспективные);

5. Акторы распространения информации (централизованные и распределенные).

В-третьих, с помощью приведенной классификации были проанализированы случаи применения виртуальных технологий конфликтной мобилизации в США на примере социального протеста 6 января 2021 года, известного, как «Штурм Капитолия», а также в КНР на примере долгосрочного противостояния в Гонконге в 2019 году.

В результате определено, что в США используются следующие интернет-технологии конфликтной мобилизации:

1. По платформе: социальные сети и сайты локального уровня.

2. По субъектности организационного лидера протеста: открытая.

3. По радиусу воздействия технологий: локальный уровень.

4. По периоду воздействия технологий: перспективные и краткосрочные.

5. По акторам распространения информации: централизованные.

В основе подхода Соединенных Штатов Америки по противодействию интернет-технологиям конфликтной мобилизации лежит тезис о взаимосвязи администрации США с администрациями социальных сетей, а также юридическая зависимость последних от государства. Это позволяет американским властям делегировать функции контроля за крупными международными социальными сетями им самим, что, в свою очередь, блокирует возможность публикации антигосударственного контента. При этом США поощряют политическое использование международных социальных сетей за рубежом, рассматривая данные платформы, как инструменты мягкой силы.

Подход технологов протестов в Китайской народной Республики в рамках предложенной классификации можно определить следующим образом:

1. Платформа: международные социальные сети, видеохостинги, сайты, локальные платформы.

2. Субъектность организационного лидера конфликтной мобилизации: скрытая.

3. Радиус воздействия технологий: международный, локальный.

4. Период воздействия технологий: краткосрочные.

5. Акторы распространения информации: распределенная передача информации.

Подход КНР к противодействию технологиям сетевой конфликтной мобилизации заключается в государственном контроле за внутренним сегментом интернета. Такой контроль не позволяет технологам работать через лидеров протеста, формируя вокруг них протестную мобилизацию, а также не оставляет возможности использования внутригосударственных социальных сетей. В то же время использование краткосрочных технологий приводит к появлению новых локальных платформ, созданных специально для консолидации и координирования участников политической акции. Государственный контроль за китайским сегментом интернета не позволяет технологам использовать перспективные, долгосрочные технологии конфликтной мобилизации, что ведет к существенному перевесу внимания со стороны технологов протестов к краткосрочным, тем самым побуждая их развитие.

В Российской Федерации произошла корректировка подхода организаторов протестов в части выбора ими интернет-технологий конфликтной мобилизации. Преобладающий набор технологий, используемых в российском сегменте интернета до февраля 2022 года, выглядел следующим образом. По платформе: крупные международные и российские социальные сети. По субъектности: открытая субъектность

организационного лидера конфликтной мобилизации. По радиусу воздействия технологий: локальные, внутригосударственные, международные. По критерию периода воздействия технологий: долгосрочные, краткосрочные. По критерию акторов распространения информации: централизованный источник информации.

После февраля 2022 года набор технологий по выделенным критериям существенно изменился. Теперь по критерию платформ, учитывая мобилизацию российских социальных сетей вокруг государственной повестки, для организаторов протеста сохранилась возможность использования исключительно международных крупных социальных сетей. В связи с уходом из публичной повестки лидеров несистемной оппозиции нет предпосылок для использования технологий открытой субъектности. По радиусу воздействия технологий, учитывая, что этот критерий связан с используемыми платформами, сформулирован вывод, что локальный и внутригосударственный радиус воздействия станет менее доступным для технологов протестов, их инструменты будут ориентированы на международный уровень. По критерию периода воздействия технологий, учитывая лояльность российских социальных сетей государству, для организаторов протестов становится затруднительным использовать долгосрочные технологии, поэтому предпочтение будет отдаваться быстрым, краткосрочным инструментам. Наконец, по критерию акторов распространения информации по той же причине, которая определена в критерии субъектности, следует ожидать использования технологий распределенной передачи информации.

В-четвертых, изменение подхода организаторов протестов к использованию интернет-технологий конфликтной мобилизации повлияло на выработку актуальных рекомендаций для государства по противодействию таким технологиям. В рамках настоящей работы автор пришел к следующим из них:

1. Развитие позитивного образа власти и государства в российском сегменте интернета: российских социальных сетях и неангажированных международных. Наиболее эффективным методом достижения данной цели будет использование распределенных и централизованных технологий интернет-коммуникации, ориентация на локальный и внутригосударственный уровень, использование комбинации долгосрочных и краткосрочных технологий.

2. Формирование позитивного образа власти и государства в зарубежных, в настоящее время запрещенных, социальных сетях, путем применения технологий распределенной передачи информации. Учитывая частые случаи с блокировкой позитивного по отношению к россиянам и России контента в международных социальных сетях, для реализации этой задачи необходимо использовать технологии скрытой субъектности, распределенные по методу передачи информации, краткосрочные по скорости распространения информации.

3. Поиск и выявление новых технологий, новых технических решений, которые могут быть применены в рамках будущих протестных активностей, учитывая риски использования организаторами таких политических акций быстрых, краткосрочных технологий. Одной из новых технологий конфликтной мобилизации, выявленной в рамках изучения социально-политического конфликта в Гонконге в 2019 году, стала технология геймификации протеста, формирующая у участников политической акции представление ролевой игры и их активного участия в ней. Данные технологии могут проверяться и тестироваться в рамках эндогенных сценариев сетевой конфликтной мобилизации.

4. Стимулирование развития российских социальных сетей, мессенджеров и иных платформ и поощрение их выхода на международный уровень для укрепления возможностей Российской Федерации формировать через них позитивную международную повестку.

Таким образом, в настоящей работе удалось выявить эволюцию научного подхода к определению феномена сетевой конфликтной мобилизации, предложить классификацию интернет-технологий, используемых в рамках данного феномена, проанализировать подходы США, КНР и России к противодействию этим технологиям. Также благодаря анализу конкретных примеров применения сетевой конфликтной мобилизации, удалось определить и подходы организаторов протестов в каждой из этих стран. В конечном итоге выполненное исследование привело к предложению автором работы практических рекомендаций для органов государственной власти, руководителей пресс-служб высших должностных лиц регионов России, государственных и некоммерческих организаций, занимающихся продвижением позитивного образа России за рубежом, а также для специалистов, работающих в организациях, оказывающих противодействие феномену сетевой конфликтной мобилизации.

Библиография

Нормативно-правовые акты

1. Указ Президента Российской Федерации "«Доктрина информационной безопасности Российской Федерации» " от 5.12.2016 № 646 // Российская газета. – 2016.
2. Закон Российской Федерации "О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности" от 6.07.2016 г № №374-ФЗ " // Российская газета. – 2016.
3. Закон Российской Федерации "О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности" от 6.07.2016 г № №375-ФЗ " // Российская газета. – 2016.
4. Указ Президента Российской Федерации "О Стратегии национальной безопасности Российской Федерации" от 02.07.2021 № 400 // Российская газета. – 2021.
5. Указ Президента Российской Федерации "О Стратегии национальной безопасности Российской Федерации" от 31.12.2015 № 683 // Российская газета. – 2015.

6. Указ Президента Российской Федерации "О Стратегии национальной безопасности Российской Федерации" от 12.05.2009 № 537 // Российская газета. – 2009.

7. The White House «National cyber strategy of the United States of America» from 09.2018 whitehouse.gov. 2018.;

8. Законопроект # 1009841-7 "О внесении изменений в Федеральный закон "Об основах системы профилактики правонарушений в Российской Федерации" и Федеральный закон "Об информации, информационных технологиях и о защите информации" в части реализации механизмов профилактики и противодействия распространению криминальных субкультур в Российской Федерации // СОЗД URL: sozd.duma.gov.ru/bill/1009841-7 (дата обращения: 20.02.2022).

Монографии

9. Аронсон Э., Пратканис Э. Р. Эпоха пропаганды: Механизмы убеждения, повседневное использование и злоупотребление - СПб.: Прайм–Еврознак, 2003. – 384 с.

10. Дзялошинский И. М. Коммуникационные процессы в обществе: институты и субъекты. М., 2012. – 592 с.

11. Дзялошинский, И. М. Экология коммуникаций. – Саратов: Ай Пи Эр Медиа, 2019. – 443 с.

12. Егорова-Гантман Е. В. В тумане войны. Наступательные военные коммуникативные технологии. Самара, М.: «Никколо М», 2010. – 432 с.

13. Кастельс М. Информационная эпоха: экономика, общество, культура. Пер. с англ. под науч. ред. О. И. Шкаратана. М.: ГУ ВШЭ, 2000. – 608 с.

14. Кастельс, М. Власть коммуникации: учеб. пособие / «Высшая школа экономики». – 2016. – 564 с.

15. Кастельс М. Галактика Интернет: Размышления об Интернете, бизнесе и обществе. Екатеринбург, 2004. Екатеринбург: У-Фактория, 2004. – 328 с.

16. Лебон Г. Психология народов и масс. Пер. с фр.; М.: Книжный клуб, 2008. – 135 с.

17. Лайнбарджер П. Психологическая война. Теория и практика обработки массового сознания. М: Центрполиграф, 2014. – 528 с.

18. Манойло А.В. Государственная информационная политика в особых условиях. М., 2003. – 388 с.

19. Мельвиль А.Ю. [и др.] Политология: учеб. / Московский государственный институт международных отношений (Университет) МИД России, ТК Велби, Проспект, 2008. – 624 с.

20. Наим М. Конец власти. От залов заседаний до полей сражений, от церкви до государства: почему управлять сегодня нужно иначе. Corpus, 2016. – 512 с.

21. Почепцов Г.Г. Информационно-политические технологии. М., 2003. – 381 с.

22. Сундиев И.Ю., Смирнов А.А. Теория и технологии социальной деструкции (на примере «цветных революций»). М., Институт экономических стратегий, 2016. – 433 с.

23. Танина М.А., Юрасов И.А., Юдина В.А., Зябликова О.А., Юрасова О.Н. Цифровой протест в провинциальных городах России: структура, дискурс, модели. Пенза, 2021. – 164 с.

24. Шульц Э.Э. Технологии управления радикальными массовыми формами социального протеста в политической борьбе. М., 2018. – 248 с.

25. Etzioni A. The Active Society. A Theory of Societal and Political Processes. L., 1968.

26. Castells, Manuel (2012). Networks of outrage and hope – social movements in the Internet age // Chichester, UK: Wiley, 298 p.

27. Rheingold H. Smart Mobs: The Next Social Revolution // Cambridge, Mass.: Perseus Publ., 2009.

28. Mathis D., Grace H. Chronicling Civil Resistance. Washington, DC, 2021.

29. Pinckney J. How to Win Well Civil Resistance Breakthroughs and the Path to Democracy. Washington, DC, 2021

Научные статьи в печатных изданиях

30. Азаров А.А., Бродовская Е.В., Дмитриева О.В., Домбровская А.Ю., Фильченков А.А. Стратегии формирования установок протестного поведения в сети Интернет: опыт применения киберметрического анализа (на примере Евромайдана, ноябрь 2013). Часть I // Социология Интернет и новых технологий. – 2014. – № 2. – С. 63 – 78.

31. Байков С.А. Стратегия коммуникации политической элиты и общества в России в условиях международной конфронтации // Вопросы политологии. – 2021. – Т. 11. – № 3 (67). – С. 719 – 727.

32. Бродовская Е.В., Давыдова М.А., Еремин Е.А. Пролонгированные политические протесты в России и в Республике Беларусь летом-осенью 2020 года: референтность российской аудитории социальных медиа // Гуманитарные науки. Вестник Финансового университета. – 2021. – Т. 11. – № 1. – С. 6 – 13.

33. Бубнов А.Ю., Козлов С.Е. Политический активизм в социальных сетях (на примерах Москвы, Екатеринбурга и Шиеса) // Журнал политических исследований. – 2021. – Т. 5. – № 1. – С. 54–64.

34. Бугаец Д.В., Анисимов В.П. Доктрина информационной безопасности РФ - основа противодействия угрозам безопасности России в информационной сфере // Россия в XXI веке: новые тенденции развития. Материалы Международной научно-практической студенческой конференции. – 2017.

35. Володенков С. В. Политическая коммуникация и современное политическое управление // Вестник Московского университета. Серия 12. Политические науки. – 2011. – №6.

36. Володенков С. В. Интернет-коммуникации в глобальном пространстве современного политического управления // Проспект Москва, 2018. – С 271.

37. Володенков С. В. Интернет-технологии как современный инструмент виртуализации массовой политической реальности // Вестник Московского университета. Серия 12. Политические науки. – 2017. – №2

38. Володенков С. В. Особенности интернет-коммуникации в современном политическом процессе // Вестник Московского университета. Серия 12. Политические науки. – 2014. – №2.

39. Володенков С. В. Медиатизация и виртуализация современного пространства публичной политики // Коммуникология. – 2016. – №4.

40. Володенков С.В. Роль информационно-коммуникационных технологий в современной политике // Антиномии. – 2018. – №2.

41. Гаврилов С.Д. «Новые протесты» как состояние социально - политической реальности в отражении россиян // Прорывные научные исследования как двигатель науки. Сборник статей Международной научно-практической конференции. Уфа, 2021. – С. 184–186.

42. Гаврилов С.Д., Морозов С.И. Стратегии коммуникации в публичном политическом пространстве России: от интеграции до протеста // Право и политика. – 2021. – № 2. – С. 25–34.

43. Гасанова В.С. Социальные сети как инструмент управления протестными акциями // Информационные войны. – 2021. – № 1 (57). – С. 46–47.

44. Гончаров Д.В. Политическая мобилизация // Полис. Политические исследования. – 1995. – №6. – С. 129.

45. Громова А. В. Роль СМИ в осуществлении «Цветных революций» // Вестник РУДН. Серия: Литературоведение, журналистика. – 2008. – №2.

46. Денисенко П. В., Есиев Э. Т. Интернет-технологии как инструмент политической мобилизации в эпоху big data // Вопросы политологии. — 2021. — № 4.

47. Докука С. В. Практики использования онлайновых социальных сетей // Социологические исследования. – 2014. – № 1. – С. 137–145.

48. Дмитриев С.С. Цифровая мобилизация: новые механизмы и возможности политического управления // Управленческое консультирование. – 2021. – № 2 (146). – С. 18–25.

49. Дубровский Г.Д. Протестные события 2019 г. в Москве: анализ политических технологий // Гуманитарное знание и искусственный интеллект: стратегии и инновации. Материалы международной конференции. Министерство науки и высшего образования Российской Федерации, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина. Екатеринбург, 2020. – С. 731–735.

50. Ершов Н.А., Омерович А.Р., Попов С.И. Протестный потенциал как инструмент предвыборной кампании (Часть II: выборы в государственную думу 2021 года. Прогнозы) // Вопросы национальных и федеративных отношений. – 2021. – Т. 11. – № 3 (72). – С. 853–858.

51. Есиев Э.Т., 2021. «Соответствие социальной сети TikTok установленным в Российской Федерации методам противодействия интернет–технологиям конфликтной мобилизации» Вопросы политологии. – 2021. – 12(76). – С. 3526–2535.

52. Есиев Э. Т. Интернет-технологии политической мобилизации в белорусских протестах на предвыборном этапе // Вестник Московского государственного областного университета (электронный журнал). – 2021. – № 2. – С. 23–37.

53. Есиев Э. Т. Геймификация протеста как технология сетевой конфликтной мобилизации // Информационные войны. – 2022. – № 2. – С. 2– 5.

54. Ибрагимова Г.Р. Стратегия КНР в области управления интернетом и обеспечения информационной безопасности // Индекс безопасности. – 2013. – Т. 19. – № 1 (104), – С. 169–184.

55. Карпович О.Г., Карипов Б.Н., Литвинов В.О. Эволюция протестных настроений в Гонконге: основные уроки // Вестник Дипломатической академии МИД России. Россия и мир. – 2021. – № 2 (28). – С. 71–87.

56. Кёхлер Г. Новые социальные медиа: шанс или препятствие для диалога? – Полис. Политические исследования. – 2013. – № 4. – С. 75–87

57. Кузнецов И. И. РУНЕТ как часть российского электорального пространства // Общественные науки и современность. – 2003. – № 1. – С. 115–128.

58. Кремень Т.В. Политическая мобилизация: объекты и субъекты // Историческая и социально-образовательная мысль. – 2013. – №5. – С. 146–149.

59. Манойло А. В. Информационный фактор цветных революций и современных технологий демонтажа политических режимов // Вестник МГИМО. – 2014. – №6 (39).

60. Манойло А.В. «Фейковые новости» как угроза национальной безопасности и инструмент информационного управления // Вестник Московского университета. Серия 12: Политические науки. – 2019. – № 2. – С. 37–45.

61. Манойло А.В. Цепные реакции каскадного типа в современных технологиях вирусного распространения «фейковых новостей» // Вестник Московского государственного областного университета. – 2020. – № 3. – С. 75–107.

62. Манойло А.В., Попадюк А.Э. Зарубежные научные подходы к исследованию «фейковых новостей» в мировой политике // Россия и современный мир. – 2020. – № 2 (107). – С. 285–300.

63. Манойло А.В. — Цветные революции и технологии демонтажа политических режимов // Мировая политика. – 2015. – № 1. – С. 1 – 19

64. Марин Е.Б. Представление о социальном протесте у молодежи российского Дальнего Востока // Вестник Института социологии. – 2021. – Т. 12. – № 1. – С. 62–92.

65. Марин Е.Б., Осмачко Н.В. Динамика протестных настроений студенческой молодежи в региональном контексте: на примере Приморского края // Социально–политические науки. – 2020. – Т. 10. – № 5. – С. 20–35.

66. Морозов И.Л. Уличный протест как технология антигосударственных действий радикальной оппозиции - опыт зарубежных стран и угроза для России // Общество: политика, экономика, право. – 2021. – № 3 (92). – С. 12–16.

67. Нагорняк К.И. Активность оппозиционных Telegram-каналов и поведенческий фактор пользователей Google как метод исследования протестов в Белоруссии 2020 года // Вестник Российского университета дружбы народов. Серия: Политология. – 2021. – Т. 23. – № 1. – С. 60–77.

68. Негров Е.О. Роль и особенности молодежного политического онлайн–активизма в современной России // Вестник Российского университета дружбы народов. Серия: Политология. – 2021. – Т. 23. – № 1. – С. 18–30.

69. Нешков С.В. Массовые агитационно–пропагандистские материалы политических протестных акций 2017 г. в России // Вопросы национальных и федеративных отношений. – 2021. – Т. 11. – № 4(73). – С. 1181–1190.

70. Панцерев, К.А. "Твиттерные революции" в странах Северной Африки – обратная сторона развития информационного общества // Азия и Африка сегодня. – 2016. – №4 (705).

71. Полтерович В.М. Кризис институтов политической конкуренции, Интернет и коллаборативная демократия // Вопросы экономики. – 2021. – № 1. – С. 52–72.

72. Пономарев Н.А., Нешков С.В. Видеоигра «People Power» как средство подготовки организаторов кампании ненасильственной борьбы // Вестник Московского университета. Серия 12: Политические науки. – 2018. – № 4, – С. 99–111.

73. Пономарев Н.А., Балтодано У.А.С, Нешков С.В., Майлис А.А. Организация инфраструктуры протестных акций (на материалах Евромайдана) // Информационные войны. – 2018. – № 2 (46). – С. 51–56.

74. Рустамова Л.Р., Барабаш Б.А. Информационное воздействие в эпоху «постправды» и «фейк–ньюс» // Вопросы политологии. – 2018. – Т. 8. – № 5 (33). – С. 23–30.

75. Рыдченко К.Д. Интересы и угрозы безопасности России в информационно-психологической сфере // Пробелы в российском законодательстве. – 2009. – №4.

76. Салицкий А.И., Виноградов А.В. Гонконгское противостояние: внутренняя динамика и внешние аспекты // Контуры глобальных трансформаций: политика, экономика, право. – 2021. – Т. 14. – № 1. – С. 135–150.

77. Самсонова Т.Н., Гурылина М.В. Основные тенденции политической мобилизации и политического участия граждан в современном российском обществе // Известия Тульского государственного университета. Гуманитарные науки. – 2016. – № 4.; – С. 41–46.

78. Стукал Д.К., Беленков В.Е., Филиппов И.Б. Методы наук о данных в политических исследованиях: анализ протестной активности в социальных сетях // Политическая наука. – 2021. – № 1. – С. 46–75.

79. Сулейманова Ш.С. Роль средств массовой информации и новых медиа в межнациональных и межконфессиональных конфликтах // Вопросы национальных и федеративных отношений. – 2018. – Т. 8. – № 3 (42). – С. 178–190.

80. Сухов А.Н. Последствия деструктивных социальных конфликтов: историко-практический аспект // Вестник Московского университета МВД России. – 2021. – № 2. – С. 323–326.

81. Сивоволов Д.Л. Новые угрозы национальному суверенитету России в сфере информационной безопасности // РАНХиГС М.: Социум и власть, 2015. – № 6. – С. 82–88.

82. Танцура М. С., Садовникова А. А. Исследование сетевой активности как инструмента политической мобилизации молодёжи (на примере антикоррупционных митингов 26 марта 2017 г.) // Известия Восточного института. – 2019. – №1 (41).

83. Тастенов А. Устименко А.В.; Априянц К.В. «Твиттер–революции»: микроблоги как инструмент выражения протестных настроений гражданского общества // Вестник ВГУ. Серия: Филология. – 2014. – № 1.

84. Ушкин С.Г. Теоретико–методологические подходы к изучению сетевой протестной активности: от «умной толпы» к «слактивизму» // Мониторинг общественного мнения: экономические и социальные перемены. – 2015. – № 3. – С. 3–11.

85. Ушкин С.Г. Вовлеченность пользователей социальных сетей в протестное движение // Власть. – 2014. – № 8. – С. 138 – 142.

86. Филатова О.Г. Интернет–технологии политической мобилизации в современной России // Политическая экспертиза: ПОЛИТЭКС. – 2014. – Т. 10. – №4.

87. Фукуяма Ф. Доверие: социальные добродетели и путь к процветанию // ООО «Издательство АСТ»: ЗАО НПП «Ермак», 2004. – С. 730.

88. Хабекирова З.С. Стратегия дискредитации и приемы ее реализации в политическом дискурсе демократической оппозиции // Вестник Адыгейского государственного университета. Серия 2: Филология и искусствоведение. – 2011. – № 2. – С. 138 – 144.

89. Челышева С.Д., Эльтикова Е.А. Социальные сети как инструмент политических манипуляций // Современные тенденции и технологии развития потенциала регионов. Сборник статей Национальной научно-практической конференции. Санкт-Петербург, 2021. – С. 40–43.

90. Шаматонова Г.Л., Майоров В.О. Экологические протесты как форма проявления гражданской активности // Социальные и гуманитарные знания. – 2019. – Т. 5. – № 3 (19). – С. 200–207.

91. Шентякова А.В., Гришин Н.В. Мобилизация политического протеста молодежи и российские видеоблогеры: результаты когнитивного картирования // Galactica Media: Journal of Media Studies. – 2021. – Т. 3. – № 2. – С. 88–109.

92. Якунин В. И., Акаев А. А., Кочетков А. П. и др. Вызовы времени: Устойчивость государства в условиях современной трансформации // Вестник Московского университета. Серия 12: Политические науки. – 2021. – № 4.

93. Якунин, В. И., Кузнецов, И. И., Вилисов, М. В. Устойчивость государственных систем на постсоветском пространстве: контуры теоретической модели // Контуры глобальных трансформаций: политика, экономика, право 13, 4. – 2020, – С. 6–33.

94. Якунин, В. И. Идеологические клише и мифы как инструмент внешней политики США // Российский журнал правовых исследований. – 2018. – 1(14). – С. 9–19.

95. Breuer, A., Landman, T., & Farquhar, D. Social Media and Protest Mobilization: Evidence from the Tunisian Revolution // SSRN Electronic Journal, 2012.

96. Deibert R.J. Parchment, Printing and Hypermedia: Communications in World Order Transformation // N.Y.: Columbia University Press, 1997.

97. Jost, J. T., Barberá, P., Bonneau, R., Langer, M., Metzger, M., Nagler, J. Tucker, J. A. How Social Media Facilitates Political Protest: Information, Motivation, and Social Networks // Political Psychology. 2018. № 39, С. 85–118.

98. Kahn, R., Kellner D. Oppositional Politics and the Internet: A Critical // Reconstructive Approach. Cultural Politics. 2005. № 1. С. 75–100.

99. Kim, S. W., & Douai, A. (2012). Google vs. China's «Great Firewall»: Ethical implications for free speech and sovereignty // Technology in Society, 34(2), 174–181.

100. Lasswell H.D. The structure and function of communication in society // The communication of Ideas / Ed. By l. Bryson. N.Y., 1948.

101. Lemos, Carlos & Coelho, Helder & Lopes, Rui Jorge. Agent-Based modeling of protests and violent confrontation: a micro-situational, multi-player, contextual rule-based approach // Proceedings of the 5th World Congress on Social Simulation, São Paulo, Brazil, November 4-7. 2014, p. 136-160.

102. Purbrick M. (2019) A REPORT OF THE 2019 HONG KONG PROTESTS // Asian Affairs, 50:4, 465–487,

103. Melvin L. De Fleur, Theories of Mass Communications // New York, Mckay, 1970.

104. Morozov E. The Net Delusion: The Dark Side of Internet Freedom. // NY: PublicAffairs, 2012.

105. Polat R. K. The Internet and Political Participation: Exploring the Explanatory Links // European Journal of Communication. 2005. № 20(4), 435–459.

106. Sung Wook Kim, Aziz Douai Google vs. China's "Great Firewall": Ethical implications for free speech and sovereignty // Technology in Society. 2012. № 34, Issue 2.

107. Shannon, Claude and Warren Weaver, The Mathematical Theory of Communication // Urbana, IL: The University of Chicago Press, 1949

108. Tin-yuet Ting From 'be water' to 'be fire': nascent smart mob and networked protests in Hong Kong // Social Movement Studies, 2020. 19:3, 362–368.

Научные статьи в электронных изданиях

109. Бауман З. Способны ли Facebook и Twitter помочь распространению демократии и прав человека? // Русский журнал. 2013 URL: http://russ.ru/Mirovaya-povestka/Sposobny-li-Facebook-i-Twitter-pomoch-rasprostraneniyu-demokratii-i-prav-cheloveka. (дата обращения 12.03.2021).

110. Володенков С. В. Информационное вмешательство как феномен деятельности субъектов современной международной политики // Вестник ВолГУ. Серия 4, История. Регионоведение. Международные отношения. 2020. №3. URL: https://cyberleninka.ru/article/n/informatsionnoe-vmeshatelstvo-kak-fenomen-deyatelnosti-subektov-sovremennoy-mezhdunarodnoy-politiki (дата обращения: 06.02.2022).

Диссертации и авторефераты

111. Володенков С.В. Технологии интернет-коммуникации в системе Современного политического управления: дис. д-р. полит. наук: 23.00.02. – Москва, 2015. – 441 с.

112. Демчук А.Л. Политика регулирования экологических конфликтов: концептуальные основы и национальные модели: дис. д-р. полит. наук: 23.00.06. М., 2020. – 565 с.

113. Докука С.В. Коммуникация в социальных онлайн-сетях как фактор протестной мобилизации в России: дис. канд. социол. наук: 22.00.04. – Москва, 2014. – 150 с.

114. Кинаш Ю.С. Роль СМИ и «новых медиа» в современных политических конфликтах (на примере «Арабской весны» и Ливии): дис. канд. полит. наук: 23.00.06. Москва, 2017. – 169 с.

115. Ланге О.В. Современные манипулятивные технологии: вопросы теории и методологии: диссертация на соискание степени кандидата политических наук: 23.00.01. СПб., 2015. – 173 с.

116. Семченков А.С. Противодействие современным угрозам политической стабильности в системе обеспечения национальной безопасности России: дис. д-р. полит. наук: 23.00.02. М., 2012. – 304 с.

117. Сдельников В.А. Технологии формирования негативного имиджа России: дис. канд. полит. наук: 23.00.02. М., 2018. – 185 с.

118. Смирнов Д.Н. Манипулятивные технологии и их применение в условиях смены политического режима: опыт оранжевой революции на Украине: дис. канд. полит. наук: 23.00.02. Нижний Новгород, 2009. – 352 с.

119. Фирсов А.В. Технологии поддержания политической стабильности в механизме обеспечения национальной безопасности: российский и зарубежный опыт: диссертация на соискание степени кандидата политических наук: 23.00.02. М., 2017. 166 с.

Источники из сети Интернет

120. Десять фактов, доказывающих, что Facebook — инструмент западных спецслужб // Федеральное агентство новостей URL: https://riafan.ru/1223939-desyat-faktov-dokazyvayushikh-chto-facebook-instrument-zapadnykh-specsluzhb (дата обращения: 20.02.2022).

121. Закон о национальной безопасности КНР 2015 года в контексте региональной безопасности: возможности или угрозы // Российский совет по международным делам // РСМД URL: http://russiancouncil.ru/blogs/evgeny-gamerman/?id_4=2051 (дата обращения: 28.02.2021).

122. Аудитория интернета в России выросла на 4% // РИФ/2018 URL: https://2018.rif.ru/news/auditoriya-interneta-v-rossii-virosla-na-4 (дата обращения: 03.03.2021).

123. В Китае число интернет-пользователей превысило 800 миллионов человек // РИА Новости URL: https://ria.ru/20180822/1526980024.html (дата обращения: 03.03.2021).

124. Верховный суд признал экстремистским движение "АУЕ". // ТАСС URL: tass.ru/obschestvo/9217761 (дата обращения: 20.02.2022).

125. "Евромайдан" в цифрах // РИА Новости. Украина URL: https://rian.com.ua/infografika/20141121/359801817.html (дата обращения: 01.03.2021).

126. Как Кремль будет реагировать на жалобы в соцсетях // РБК URL: https://www.rbc.ru/politics/23/07/2018/5b50d1579a7947c62c195e8b (дата обращения: 03.03.2021).

127. Компания Facebook удалила фальшивые аккаунты из РФ и Украины, в которых критиковалась украинская власть. https://gordonua.com/news/worldnews/kompaniya-facebook-nakanune-vyborov-v-radu-udalila-falshivye-akkaunty-iz-rf-i-ukrainy-v-kotoryh-kritikovalas-ukrainskaya-vlast-1143248.html (дата обращения: 03.03.2021).

128. Китайский интернет и софт: о наболевшем // Habr URL: https://habr.com/ru/post/370659/ (дата обращения: 03.03.2021).

129. Китай предложил обеспечить глобальную безопасность данных // Коммерсант URL: www.kommersant.ru/doc/4483436 (дата обращения: 20.02.2022).

130. О современной политике Китая в киберпространстве. // DRussia URL: -russia.ru/o-sovremennoj-politike-kitaja-v-kiberprostranstve.html (дата обращения 20.02.2022).

131. Открытость государства в России – 2021 // Счетная палата РФ URL: ach.gov.ru/upload/pdf/Otkrytost-2021.pdf (дата обращения: 20.02.2022).

132. Пожар в Кемерове: откуда пошли разговоры о том, что власти скрывают 300 погибших // Medialeaks URL: https://medialeaks.ru/2703bva-zhertvy-v-kemerovo/ (дата обращения: 03.03.2021).

133. Полигон Урдома: Заражение / Urdoma's Polygon: The Infection // Youtube URL: https://www.youtube.com/watch?v=POdsOHtV90o&t=262s (дата обращения: 01.03.2021).

134. Роскомнадзор начал против Facebook и Twitter административное производство // РИА Новости URL: https://ria.ru/20190121/1549648300.html (дата обращения: 03.03.2021).

135. Роскомнадзор против Twitter и Facebook. Краткая история противостояния // RTVI https://rtvi.com/stories/roskomnadzor-protiv-twitter-i-facebook/ (дата обращения: 03.03.2021).

136. Россия покупала рекламу в Facebook // ТСН URL: https://ru.tsn.ua/svit/rossiya-pokupala-reklamu-v-facebook-no-vliyanie-na-vybory-v-ssha-bylo-neznachitelnym-gendirektor-avast-1009110.html (дата обращения: 01.01.2021).

137. СМИ: ТВ и интернет / ФОМ URL: https://fom.ru/SMI-i-internet/14258 (дата обращения: 01.01.2021).

138. Синий кит (игра) // Википедия URL: ru.wikipedia.org/wiki/Синий_кит_(игра) (дата обращения: 20.02.2022)

139. Совместное заявление Российской Федерации и Китайской Народной Республики о международных отношениях, вступающих в новую эпоху, и

глобальном устойчивом развитии. // Сайт президента России URL: kremlin.ru/supplement/5770 (дата обращения: 20.02.2022).

140. Сторис успеха: рейтинг глав регионов в Instagram // ЦПКР URL: cpkr.ru/issledovaniya/tsifrovye-portrety-glav-rossiyskikh-regionov/storis-uspekha-reyting-glav-regionov-v-instagram/ (дата обращения: 20.02.2022).

141. ТОП-10 штрафов и взысканий, наложенных на Интернет-компании // URL: https://fznc.world/wp-content/uploads/2019/04/TOP-10-shtrafov.pdf (дата обращения: 20.02.2022).

142. ТОП-11 случаев цензуры в социальных сетях // URL: https://fznc.world/%D0%B1%D0%B5%D0%B7-%D1%80%D1%83%D0%B1%D1%80%D0%B8%D0%BA%D0%B8/top-11-sluchaev-tsenzury-v-sotsialnyh-setyah/ (дата обращения: 20.02.2022).

143. ИГ опубликовало видео с угрозами в адрес России // РБК URL: www.rbc.ru/politics/01/08/2016/579e6f5b9a7947cdb5cedc8a (дата обращения: 20.02.2022)

144. Facebook заблокировал 58 аккаунтов за возможную связь с Ираном // МК URL: https://www.mk.ru/social/2019/05/29/facebook-zablokiroval-58-akkauntov-za-vozmozhnuyu-svyaz-s-iranom.html (дата обращения: 20.02.2022).

145. Уголовное судопроизводство. Данные о назначенном наказании по статьям УК. // URL: stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17 (дата обращения 20.02.2022).

146. ABOUT // January 6th URL: january6th.house.gov/about (дата обращения: 20.02.2022).

147. ‘Carol’s Journey’: What Facebook knew about how it radicalized users. // NBC News URL: www.nbcnews.com/tech/tech-news/facebook-knew-radicalized-users-rcna3581 (дата обращения: 20.02.2022).

148. Criteria for Security and Trust in Telecommunications Networks and Services // CSIS Working Group on Trust and Security in 5G Networks URL: csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200511_Lewis_5G_v3.pdf (дата обращения: 20.02.2022).

149. China’s State-Run Companies Limit Use of Tencent’s Messaging App // Wall Street Journal URL: www.wsj.com/articles/chinas-state-run-firms-limit-use-of-tencents-messaging-app-11637837474 (Дата обращения 20.02.2022).

150. China Attacks Hong Kong Protesters With Fake Social Posts. // Wired URL: www.wired.com/story/china-twitter-facebook-hong-kong-protests-disinformation/ (дата обращения: 20.02.2022).

151. Local FBI field office warns of 'conspiracy theory-driven domestic extremists' // NBC News URL: www.nbcnews.com/tech/tech-news/local-fbi-field-office-warns-conspiracy-theory-driven-domestic-extremists-n1038441 (дата обращения: 20.02.2022).

152. DUMMIES GUIDE to confrontation and war strategies by frontline protesters in Hong Kong. // Dimsum Baily URL: www.dimsumdaily.hk/exclusive-dummies-guide-to-confrontation-and-war-strategies-by-frontline-protesters-in-hong-kong/ (дата обращения 20.02.2022).

153. Embassy Spokesperson’s Comment on the Remarks by the UK Side about International Development Cooperation and Data Security. // Chinese Embassy in United Kingdom URL: www.chinese-embassy.org.uk/eng/PressandMedia/Spokepersons/202112/t20211202_10461007.htm (Дата обращения: 20.02.2022).

154. The dark side of WeChat. // Monmouth URL: www.monmouth.edu/magazine/wp-content/uploads/sites/7/2020/10/Monmouth-Magazine-Fall-2020.pdf (дата обращения: 20.02.2022).

155. Telegram user jailed for inciting riots // The Standard URL: www.thestandard.com.hk/section-news/section/4/236769/Telegram-user-jailed-for-inciting-riots (дата обращения: 20.02.2022).

156. Facebook удалил больше ста подозрительных аккаунтов накануне выборов в Конгресс США // Интерфакс URL: https://www.interfax.ru/world/636547 (дата обращения: 03.03.2021).

157. Facebook bans all 'stop the steal' content // NBC News URL: www.nbcnews.com/tech/tech-news/facebook-bans-all-stop-steal-content-n1253809 (дата обращения: 20.02.2022).

158. Facebook, Twitter accuse China of spreading Hong Kong disinformation. // LA Times URL: www.latimes.com/business/story/2019-08-19/facebook-twitter-china-disinformation-hong-kong-protests (дата обращения: 20.02.2022).

159. How reading online comments affects us // Social media psychology URL: https://socialmediapsychology.eu/2016/10/05/onlineandsocialmediacomments/ (дата обращения: 01.03.2021).

160. Hong Kong protests: Twitter and Facebook crack down on "deceptive" accounts linked to China // CBS News URL: https://www.cbsnews.com/news/hong-kong-protests-twitter-facebook-crack-down-on-deceptive-accounts-linked-to-china/ (дата обращения: 20.02.2022).

161. In May, I predicted that backdoors in WhatsApp would keep getting discovered, and one serious security issue would follow another, as it did in the past // Telegram URL: https://t.me/durov/109 (дата обращения: 03.03.2021).

162. India Proposes Chinese-Style Internet Censorship // The New York Times URL: https://www.nytimes.com/2019/02/14/technology/india-internet-censorship.html (дата обращения: 03.03.2021).

163. Inside a Fake News Sausage Factory: ‘This Is All About Income’ // The New York Times URL: https://www.nytimes.com/2016/11/25/world/europe/fake-news-donald-trump-hillary-clinton-georgia.html?module=inline (дата обращения: 03.03.2021).

164. Information operations directed at Hong Kong // Twitter URL: blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong (дата обращения: 20.02.2022).

165. Hongkongers rush to 'Save RTHK' from show purge. // RTHK URL: news.rthk.hk/rthk/en/component/k2/1589017-20210503.htm (дата обращения: 20.02.2022).

166. Hong Kong Police Review 2020. // Police of Hong Kong URL: www.police.gov.hk/info/review/2020/en/hkpf_eng05.html (дата обращения: 23.04.2022).

167. How China used Facebook, Twitter, and YouTube to spread disinformation about the Hong Kong protests // Vox URL: www.vox.com/recode/2019/8/20/20813660/china-facebook-twitter-hong-kong-protests-social-media (дата обращения: 20.02.2021).

168. Our Work. https://securingdemocracy.gmfus.org/our-work/.

169. Permanent suspension of @realDonaldTrump // Twitter URL: blog.twitter.com/en_us/topics/company/2020/suspension (дата обращения: 20.02.2022).

170. Removing Coordinated Inauthentic Behavior From China // Facebook URL: about.fb.com/news/2019/08/removing-cib-china/ (дата обращения: 20.02.2022).

171. Social media - Statistics & Facts // Statista URL: https://www.statista.com/topics/1164/social-networks/ (дата обращения: 20.02.2022).

172. January 13, 2022. // January 6th URL: january6th.house.gov/sites/democrats.january6th.house.gov/files/2022-1-13.BGT%20Letter%20to%20Twitter%20-%20Cover%20Letter%20and%20Schedule_Redacted.pdf (дата обращения: 20.02.2022).

173. Why China’s government is blocking the candle emoji // TechInAsia URL: https://www.techinasia.com/chinas-government-blocking-candle-emoji (дата обращения: 03.03.2022).