BAZAROV Victor Borisovich, *Cand.Sci. (Hist.), Researcher at the Institute for Mongolian, Buddhist and Tibetan Studies, Siberian Branch of Russian Academy of Sciences (6 Sakh'yanovoj St, Ulan-Ude, Republic of Buryatia, Russia, 670047; bazarov_science@mail.ru)*

MONGOLIAN-AMERICAN STRATEGIC PARTNERSHIP IN THE CONTEXT OF NEW GEOPOLITICAL CHALLENGES

Abstract. *The article is devoted to modern Mongolian-American relations. The USA and Mongolia are strategic partners, whose relations became possible only after the fall of the USSR. The very nature of the strategic relationship is a direct consequence of the multi-pillar foreign policy pursued by Mongolia. The dynamics and trends in the bilateral relations of these countries in the context of new geopolitical challenges experienced by the world economy and politics in the 21st century are of great interest.*

Keywords: *Mongolia, USA, NATO, strategic partnership, foreign policy, military cooperation*

КИМ Антон Валерьевич – *аспирант кафедры социологии и социальных технологий Института философии Луганского государственного университета им. Даля (291034, Россия, ЛНР, г. Луганск, квартал Молодежный, 20-а; anikimon@yandex.ru)*

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОЙ СРЕДЫ: ОПЫТ КИТАЯ И США

Аннотация. *В статье представлен анализ подходов Китая и Соединенных Штатов Америки к безопасности информационной среды. Автор рассматривает методы ограничения граждан от нежелательной информации и сохранения государственного суверенитета, анализирует разницу в позициях стран, их возможностях и жесткости в отношении сохранения информационной среды.*

Ключевые слова: *информационная среда, кибербезопасность, Китай, США*

Сегодня безопасность информационной среды – один из важнейших факторов суверенности и социальной стабильности. Социальные сети (*Social Media*) способны влиять на население сильнее, чем традиционные СМИ.

Безопасность информационной среды – это комплекс мер по ограждению населения от нежелательной информации, которая способна вызвать социальную дестабилизацию, волнения или митинги. В статье представлен анализ опыта безопасности информационного пространства Китая и США.

Обе страны – медиагиганты, которые сегодня задают стандарты социальных медиа. Китай и США делят между собой мировое информационное пространство. Многие государства предлагают локальные альтернативы, но даже в таком случае им приходится конкурировать с продуктами США и КНР.

Китайская политика цифровой безопасности отличается централизованностью. Проблема фейк-ньюс, «мягкой силы» и мобилизационных качеств социальных сетей правительству КНР была понятна еще в конце прошлого века, поэтому в 1998 г. они открыли проект «Золотой щит», который назвали

«Великий китайский файрвол» [Поздняков, Ярулин 2022]. Это глобальная система фильтрации интернет-контента, который ограничивает доступ к зарубежным веб-сайтам и фильтрует внутренние ресурсы.

Одновременно с этим в 2019 г. Китай стал главным рынком социальных сетей – 1,007 млрд пользователей, т.е. 70% населения. При этом на территории материкового Китая запрещены практически все зарубежные соцсети и общественные ресурсы, такие как *Google*, *Wikipedia*, *Instagram*, *Facebook*, *WhatsApp*, *Twich*, *Twitter* и др.

Причины блокировки, за исключением ряда сервисов, связаны с внутренней безопасностью. Например, *Facebook* был заблокирован после террористических актов и беспорядков в Синьцзяне в 2011 г., когда выяснилось, что террористы общались с помощью соцсети [Подшибякина 2020].

В отличие от КНДР, Китай не стал ограничивать Интернет, но сильно его централизовал и создал жесткую систему цензуры. На сегодняшний день в КНР есть аналоги практически всех заблокированных ресурсов, но они адаптированы под китайский менталитет и политику правительства.

После блокировки Твиттера в июне 2009 г. в августе того же года китайская компания *Sina* представила свой аналог *Sina Weibo*, которая полностью повторяла функционал. По данным сервиса *DRM*, посещаемость *Weibo* даже выше, чем у *Twitter*[1]. Формально соцсеть принадлежит частной компании, но она контролируется государством. В частности, в 2023 г. все популярные блогеры *Weibo* получили сообщение от сервиса с предупреждением «избегать выражения пессимизма в отношении китайской экономики»[2].

Во многом политика кибербезопасности Китая построена на полном замещении иностранных продуктов собственными. На территории КНР запрещены все зарубежные мессенджеры. В январе 2011 г. разработчик *Tencent* представил собственный мессенджер *Weinix* и его глобальную версию *WeChat*. По данным *Slideshare*, на территории материкового Китая мессенджером пользуются порядка 810 млн чел.[3] Сервис объединяет в себе не только обмен мгновенными сообщениями, но и социальную сеть, мобильные платежи, покупки авиабилетов и пр.

Версия, которая работает на территории материкового Китая, подчиняется политике конфиденциальности *Weinix*, которая предполагает фильтрацию контента, «который ставит под угрозу национальную безопасность, разглашает государственные секреты или подрывает государственную власть и национальное единство». Китайское правительство может получить доступ к логам, текстовым сообщениям и местоположению своих пользователей для обеспечения государственной безопасности[4].

Аналогичная ситуация обстоит и с приложением *TikTok*. Локальная версия под названием «Доуинь» подчиняется требованиям государственной безопасности и цензурным ограничениям. Между собой версии не связаны, но имеют одинаковый функционал и возможности.

---

[1] Weibo Statistics and User Count for 2024. DRM. URL: https://expandedramblings.com/index.php/weibo-user-statistics/ (accessed 08.09.2024).

[2] В Китае попросили блогеров не критиковать экономику. – *RBK*. Доступ: https://www.rbc.ru/politics/15/12/2023/657c33de9a79478637c4da58?ysclid=luvlt7pzco439095718 (проверено 15.05.2024).

[3] WeChat Users by Country 2024. World Population Review. URL: https://worldpopulationreview.com/country-rankings/wechat-users-by-country (accessed 08.09.2024).

[4] Isobel Cockerell. 2019. Inside China's Massive Surveillance Operation. Доступ: https://www.wired.com/story/inside-chinas-massive-surveillance-operation/ (accessed 08.09.2024).

Важное отличие китайской парадигмы кибербезопасности – это открытость. Правительство открыто говорит, что блокировки происходят в целях государственной безопасности. На законодательном уровне прописаны ограничения к публикациям, например, запрет на цитирование и ссылки на зарубежные источники в СМИ без одобрения.

США, в отличие от Китая, провозглашают свободу слова, что гарантирует первая поправка к Конституции. Тем не менее в 2014 г. независимое объединение «Репортеры без границ» добавили США в список стран с самым высоким уровнем цензуры в Интернете.

Как и в Китае, в США действуют законы о цензуре в Интернете, такие как *CFAA*, *CDA*, *COPA DMCA* и др. Из-за первой поправки правительство и государственные службы не могут цензурировать посты в социальных сетях за исключением федеральных законов о защите детей, торговле с врагом и пр. В 2011 г. вышла Международная стратегия США для киберпространства, где администрация Б. Обамы рекомендовала следовать принципам свободы слова, а потоки информации не должны как-либо ограничиваться[1]. Управление критическими ресурсами должно представлять многоступенчатый процесс при участии частных организаций.

По этой причине службы безопасности США не могут ставить единый фильтр для информации, как поступают в КНР. Тем не менее Штаты играют лидирующую роль в управлении Интернетом и внутренним информационным пространством. Однако спецслужбы США используют другие инструменты для контроля и цензуры.

Организация «Репортеры без границ» в 2014 г. внесла США в список «Враги Интернета». В секции «АНБ символизирует злоупотребления спецслужб» организация указывает на контроль АНБ крупнейших поставщиков инфраструктуры и провайдеров *AT&T*, *Level* 3 и *Verizon*[2]. Доступ к сетевым гигантам позволяет АНБ контролировать Интернет на корневом уровне. За пределами страны у агентства есть доступ к подводным кабелям, через которые проходит около 99% всего мирового трафика.

Вопрос цензуры в США также стоит достаточно остро, как и в КНР. Первая поправка к Конституции запрещает правительству и государственным службам напрямую цензурировать контент, если он не подпадает под федеральные законы.

Вероятно, государственные спецслужбы США активно сотрудничают с такими социальными сетями, как *Twitter* и *Facebook*. В частности, издательство *MintPress* обнаружило, что в *Twitter* работает множество сотрудников из ФБР и ЦРУ, а также кадровых офицеров. Большинство из них задействованы в сфере безопасности[3]. Так, публицист Алан Маклауд отмечает: «Если бы службами доверия, безопасности и модерации контента российского приложения для социальных сетей управляли бывшие агенты КГБ или ФСБ и

---

[1] International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed 15.05.2024).

[2] Enemies of the Internet 2014 – USA: NSA symbolises intelligence services' abuses. UNHCR. URL: https://www.refworld.org/reference/annualreport/rsf/2014/en/98666 (accessed 15.05.2024).

[3] Alan Macleod. 2022. The Federal Bureau of Tweets: Twitter Is Hiring an Alarming Number of FBI Agents. URL: https://www.mintpressnews.com/twitter-hiring-alarming-number-spooks-secret-agents/281114/ (accessed 15.05.2024).

при этом настаивали бы на том, что это политически нейтральная платформа, весь мир бы рассмеялся»[1].

В конце 2022 г. Илон Маск признал, что большинство теорий заговора, которые ходили вокруг *Twitter*, оказались правдивыми. ЦРУ, Пентагон и Госдепартамент США принимали участие в цензуре площадки. Новый владелец *Twitter* опубликовал 9 «файлов Твиттера», где показал давление со стороны спецслужб.

Кроме прямой цензуры, социальные сети практиковали теневой бан (*shadowban*). Руководителем схемы был Джефф Карлтон – бывший офицер федеральной разведки. Из того же пакета «файлов Твиттера» стало ясно, что он был инициатором теневых банов консервативных аккаунтов[2]. Например, именно таким образом в *Twitter* не обнаруживалась статья *NY Post* о ноутбуке Хантера Байдена в преддверии президентских выборов 2020 г. За это был ответственным Джим Бейкер – бывший сотрудник ФБР[3].

Следует учитывать, что социальные сети, которые США не способны контролировать по ряду причин, вызывают волнения и призывы к блокировке. Так происходит, например, с китайской социальной сетью *TikTok* – приложение популярное, бесплатное, при этом порог входа у него минимальный.

Согласно данным *DateReportal* за апрель 2023 г., в США самая большая аудитория *TikTok*, за исключением материкового Китая – 116,5 млн чел. На тот момент это составляло около 35% всего населения[4].

В августе 2020 г. президент США Дональд Трамп предлагал запретить *TikTok* и *WeChat*. Действующий президент Джо Байден решение отменил как конфронтационное, но подозрение к китайской социальной сети никуда не исчезло [Подосокорский 2022].

Из этих данных видно, что у двух сверхдержав – Китая и США – абсолютно разная политика в отношении информационной безопасности. Китай предлагает открытую политику цензурирования, при которой есть четкий список правил и требований к информации. Как внутренние СМИ и *Social Media*, так и внешние источники прекрасно понимают принципы государственной фильтрации, поэтому способны адаптироваться к государственной цензуре.

Также для китайского подхода к безопасности информационного пространства характерны:

– замещение иностранных ресурсов местными;
– разграничение приложений на локальную и глобальную версию;
– популяризация собственных площадок;
– преемственность и улучшение иностранных площадок.

Спецслужбы и правительство США из-за первой поправки не могут установить фильтр для контроля информации. Управление информационной безопасностью значительно усложняется, но вот уровень контроля значительно выше, т.к. у них есть доступ к корневой инфраструктуре. Цензурирование происходит не напрямую спецслужбами, а благодаря давлению и сотрудничеству с руководством социальных сетей.

---

1 Ibid.

2 Shawn Fleetwood. 2022. Head of Twitter's Censorship Operation Was a Former FBI, CIA Operative. URL: https://thefederalist.com/2022/12/09/head-of-twitters-censorship-operation-was-a-former-fbi-cia-operative/ (accessed 15.05.2024).

3 Ibid.

4 TikTok Users, Stats, Data & Trends. – *DataReportal*. URL: https://datareportal.com/essential-tiktok-stats (accessed 08.09.2024).

Среди основных факторов безопасности информационного пространства США можно выделить:

– закрытую политику цензурирования;
– применение теневых технологий для цензурирования;
– контролирование корневых инфраструктур;
– контроль над международными площадками.

При этом Китай занимает свою позицию вынужденно, т.к. не имеет международного влияния. За исключением *TikTok*, КНР слабо представлен на международном рынке социальных сетей.

Список литературы

Подосокорский Н.Н. 2022. Мягкая сила Тиктока: соцсеть, которая покорила мир. – *Наука телевидения*. № 18(2). С. 117-145.

Подшибякина Т.А. 2020. «Золотой щит» Китая: политика управления мнемоническими интернет-практиками. – *Вестник РУДН*. Сер.: Политология. № 2. С. 194-204.

Поздняков Е.И., Ярулин И.Ф. 2022. Опыт Китайской Народной Республики по противодействию западным фейк-ньюс. – *Вестник Московского государственного областного университета*. Сер.: История и политические науки. № 3. С. 41-57.

KIM Anton Valer'evich, postgraduate student of the Chair of Sociology and Social Technologies, Institute of Philosophy, Luhansk State Dahl University (20-a Molodezny quart., Lugansk, LNR, Russia, 291034; anikimon@yandex.ru)

THE EXPERIENCE OF CHINA AND THE UNITED STATES OF AMERICA IN SHAPING THE SECURITY OF THE INFORMATION ENVIRONMENT

Abstract. *The article presents an analysis of the approaches of China and the United States of America to the security of the information environment. The author considers the methods of restricting citizens from unwanted information and preserving state sovereignty and analyzes the difference in the positions of the countries, their capabilities and rigidity regarding the preservation of the information environment.*

Keywords: *information environment, cybersecurity, China, USA*