

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение
высшего образования**

**«Национальный исследовательский Нижегородский государственный
университет им. Н.И. Лобачевского» (ННГУ)**

На правах рукописи

Габриелян Гриша Робертович

Политика государственного регулирования Интернет-пространства КНР в условиях
цифровизации

Специальность 5.5.2. – Политические институты, процессы, технологии

Диссертация на соискание ученой степени
кандидата политических наук

Научный руководитель:
доктор политических наук,
профессор Старкин С.В.

Нижегород – 2026

Содержание

| | |
|---|-----|
| ВВЕДЕНИЕ | 3 |
| Глава I. Теоретико-методологические основы исследования интернет-пространства в контексте государственной информационной политики. | 30 |
| 1.1. Концептуальные подходы и методологии управления интернет-пространством. | 30 |
| 1.2. Понятие государственной информационной политики. | 44 |
| 1.3. Государственное регулирование в условиях цифровизации: анализ сущности и акторов | 60 |
| Глава II. Идеологические и законодательные аспекты политики государственного регулирования интернет-пространства в КНР | 73 |
| 2.1. Информационная политика КНР: теоретические и идеологические аспекты управления Интернетом | 73 |
| 2.2. Законодательные основания регулирования Интернет-пространства в КНР | 83 |
| 2.3. Адаптация государственной власти к развитию социальных сетей в Китае | 103 |
| Глава III. Управление Интернет-пространством в КНР: акторы, технологии и перспективы | 129 |
| 3.1. Государство и цифровые корпорации в КНР: интересы и сферы взаимоотношений | 129 |
| 3.2. Технологии и инструменты регулирования Интернет-пространства в КНР | 142 |
| 3.3. Перспективы развития информационной политики КНР в контексте внешних угроз | 152 |
| Заключение | 163 |
| Список использованных источников и литературы | 170 |

ВВЕДЕНИЕ

Современный мир переживает эпоху существенных изменений, которые вызваны протекающими процессами глобализации и стремительного развития цифровых технологий. Одним из ключевых факторов данных трансформаций стало активное распространение Интернета, оказывающего фундаментальное влияние на политические, социальные, экономические и культурные процессы. В условиях технологического развития и увеличения масштабов сетевого взаимодействия особую ценность приобретает информация и способность государства эффективно управлять информационными потоками в рамках защиты собственных национальных интересов.

В данных условиях Китайская Народная Республика (КНР), являясь одной из ведущих мировых держав, уделяет особое внимание вопросам реализации государственной политики по регулированию Интернета, которая направлена на обеспечение безопасности информации, развитие цифровых технологий и формирование благоприятного информационного климата внутри страны и за её пределами с учетом национальных и региональных особенностей. При этом Китай, учитывая как фактор внешних угроз, так и специфические национальные и региональные особенности, формирует собственную модель управления Интернет-пространством.

Государственная политика по регулированию Интернет-пространства рассматривается властями КНР не только в качестве эффективного инструмента обеспечения национальной безопасности и содействия дальнейшей экономической модернизации, но и инструмента в рамках поддержания политической стабильности внутри страны. С момента подключения КНР к глобальной сети Интернет власти страны уделяют особое внимание открытости и прозрачности появляющейся информации, что в свою очередь требует постоянной работы с законодательной и технологической базами. В последние годы КНР занимается активным внедрением цифровых технологий в различные

сферы жизни общества, что также создает дополнительные вызовы в вопросе управления информационными потоками и защиты данных. Развитие таких технологий, как искусственный интеллект, большие данные, Интернет вещей, а также активный рост цифровых корпораций, приводящий к появлению новых видов социальных сетей и платформ, требует от государства разработки новых подходов в области регулирования информационных потоков и формирования государственной информационной политики.

Актуальность темы исследования обусловлена стремительным развитием Интернет-пространства и изменением подходов властей КНР к реализации информационной политики, в том числе в рамках регулирования Интернета и обеспечения устойчивого развития цифровой среды. Стремительное усиление роли Интернета как политического ресурса приводит к формированию и постоянному обновлению в КНР комплексной системы государственных мер регулирования. Основные механизмы, идеологические основания и последствия для национальной безопасности и международной среды в рамках реализации мер регулирования цифрового пространства в Китае требует анализа и изучения.

В последние годы наблюдается тенденция, направленная на политизацию технологической сферы. Ввиду того, что Интернет оказывает значительное влияние на жизнь общества, он стал рассматриваться многими субъектами в качестве политического инструмента воздействия, а не просто достижения технического прогресса. В мире наблюдается активное соперничество ключевых игроков за возможность обладать самыми передовыми технологиями, связанными с Интернетом. Следует подчеркнуть, что помимо технологического усложнения функционирования Интернет-пространства важную роль в формировании современной цифровой среды играет взаимодействие государственных структур, IT-компаний, СМИ, граждан и других акторов. Изменения в цифровом и информационном пространстве побуждают власти

Китай находят новые подходы к управлению данными, информационными потоками, Интернет-пространством, что оказывает влияние также и на международную среду.

Таким образом, исследование политики государственного регулирования интернет-пространства КНР в условиях цифровизации является актуальным и значимым как с научной, так и с практической точки зрения.

Степень научной разработанности темы исследования. Важно подчеркнуть, что вопросы, связанные с изучением цифровизации, в частности, с влиянием Интернета на политические процессы, интересуют исследователей с конца XX века. Однако до середины 2000-х годов исследования в данной области можно охарактеризовать как фрагментарные. Лишь на протяжении последних двух десятилетий сфера изучения цифровых технологий и Интернета в качестве важных факторов, оказывающих влияние на процессы государственного управления, начала выделяться в самостоятельный раздел политических исследований. При этом стоит отметить, что на развитие этой сферы исследований существенное влияние оказали научные труды в сфере экономики, юриспруденции, культурологии.

Россия, являясь одним из ключевых участников системы глобального регулирования Интернет-пространства, проявляет большой интерес к развитию единого и равноправного подхода к управлению Интернетом. Многие российские исследователи уделяли в своих работах большое внимание изучению процессов регулирования Интернета. Среди них можно выделить Е.С. Зиновьеву¹, С.А. Васильковского², И.А. Быкова³, Н.А. Истомина⁴, П.А. Карасева⁵,

¹ Зиновьева Е.С. Международное управление Интернетом: проблемы, подходы, перспективы // Вестник МГИМО. 2010. № 6. С. 167–174.

² Васильковский С.А., Игнатов А.А. Управление Интернетом: системные диспропорции и пути их разрешения // Вестник международных организаций: образование, наука, новая экономика. 2020. Т. 15, № 4. С. 7–29

³ Быков И.А. Управление Интернетом как одна из проблем современных международных отношений // ПОЛИТЭКС. 2008. № 2. С. 164–174.

⁴ Истомин Н.А. Модель участия заинтересованных сторон в управлении Интернетом на международном уровне // Право и политика. 2020. № 5. С. 90–109.

С.Н. Косинову⁶, Э.Т. Куркемову⁷, С.В. Володенкова⁸.

Другие специалисты занимаются анализом механизмов реализации политики регулирования Интернета в различных странах. К подобным можно отнести работы А.А. Игнатова⁹, Д.А. Дегтерева¹⁰, С.Н. Федорченко¹¹, М.В. Шугурова¹².

В рамках изучения роли Интернета в современном политическом процессе некоторые специалисты рассматривают вопрос действия национального суверенитета в информационном пространстве. Исследования таких исследователей, как А.А. Ефремов¹³, Я.Н. Шевченко¹⁴, С.С. Шестопап¹⁵, Е.О. Гаврилов¹⁶, Е.А. Михалевич¹⁷, М.Б. Касенова¹⁸, Д.Н. Барышников¹⁹, А.П.

⁵ Карасев П.А. Управление интернетом – тенденции и перспективы // International Journal of Open Information Technologies. 2023. Т. 11, № 9. С. 59–65.

⁶ Косинова С.Н. Обеспечение безопасности интернет-пространства посредством новой многополярности // Национальная безопасность. 2022. № 1. С. 1–11.

⁷ Куркемова Э.Т. Интернет-технологии как ресурс активности политических акторов // Каспийский регион: политика, экономика, культура. 2016. № 2(47). С. 101–108.

⁸ Володенков С.В. Интернет-пространство в системе глобального политического управления: основные сценарии трансформации // Вестник Российской нации. 2017. № 4(56). С. 147–161.

⁹ Игнатов А.А. Управление Интернетом в повестке БРИКС // Вестник международных организаций: образование, наука, новая экономика. 2022. № 2. С. 86–109.

¹⁰ Дегтерев Д.А., Рамич М.С., Пискунов Д.А. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // Вестник международных организаций: образование, наука, новая экономика. 2021. Т. 16, № 3. С. 7–33.

¹¹ Федорченко С.Н. Эффект палладиума: ценности великих держав в эпоху искусственного интеллекта // Журнал политических исследований. 2023. Т. 7, № 4. С. 3–32.

¹² Шугуров М.В. «Группа восьми» (G8) и дилеммы глобального управления Интернетом: международно-правовой аспект // Право и политика. 2012. № 6. С. 1098–1127.

¹³ Ефремов А.А. Государственный суверенитет в условиях цифровой трансформации // Правоведение. 2019. Т. 63, № 1. С. 47–61.

¹⁴ Шевченко Я.Н. Цифровой суверенитет Европы в контексте политики глобального управления данными // Политическая наука. 2021. № 3. С. 251–270.

¹⁵ Шестопап С.С., Мамычев А.Ю. Суверенитет в глобальном цифровом измерении: современные тренды // Балтийский гуманитарный журнал. 2020. Т. 9, № 1(30). С. 398–403.

¹⁶ Гаврилов Е.О. Цифровой суверенитет в условиях глобализации: философский и правовой аспекты // Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки. 2020. Т. 4, № 2(14). С. 146–152.

¹⁷ Михалевич Е.А. Концепция киберсуверенитета Китайской Народной Республики: история развития и сущность // Вестник Российского университета дружбы народов. Серия: Политология. 2021. Т. 23, № 2. С. 254–264.

¹⁸ Касенова М.Б., Воронина Е.П. Европейский союз на пути к цифровому суверенитету? // Интернет изнутри. 2023. № 19. С. 41–44.

¹⁹ Барышников Д.Н., Туленков А.Ю. «Цифровая дипломатия» и государственный суверенитет в эпоху глобализации // Вестник Санкт-Петербургского университета. Серия 6. Философия. Культурология. Политология. Право. Международные отношения. 2012. № 4. С. 121–128.

Кочетков²⁰, В.А. Никонов²¹, фокусируются на рассмотрении феномена сетевого суверенитета.

Ряд исследователей при изучении политики управления Интернетом уделяют внимание проблеме кибербезопасности в своих работах. К ним относятся труды В.В. Штоля²², О.В. Кирилюка²³, И.Ю. Ткаченко²⁴, Т.А. Романовой²⁵, Т.В. Вершининой²⁶, Е.В. Разумова²⁷, Р.А. Полончука²⁸, Э.В. Горян²⁹.

К особой группе важных для данного исследования научных источников можно отнести и работы, исследующие конкретные технологии и способы поведения политических акторов, и в том числе государственных структур, в информационной сфере. Эта проблематика нашла свое отражение в трудах М.Г. Анохина³⁰, Е.В. Егоровой³¹, М.М. Кучерявого³² и других.

²⁰ Кочетков А.П., Мамычев А.Ю. Государственная политика России в цифровую эпоху: основные тренды, сценарии и регуляторные практики // Полис. Политические исследования. 2023. № 1. С. 96–113. DOI: 10.17976/jpps/2023.01.08; Кочетков А.П., Маслов К.В. Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе // Вестник Московского университета. Серия 12. Политические науки. 2022. № 2. С. 31–45.

²¹ Никонов В.А., Воронов А.С., Сажина В.А. [и др.] Цифровой суверенитет современного государства: содержание и структурные компоненты (по [нужно уточнить: материалам?] экспертного исследования) // Вестник Томского государственного университета. Философия. Социология. Политология. 2021. № 60. С. 206–216.

²² Штоль В.В., Задохин А.Г. Информационно-коммуникационные технологии и информационная безопасность России // Обозреватель. 2022. № 5–6(388–389). С. 66–78.

²³ Кирилюк О.В. Международно-правовые основы саморегулирования в киберпространстве // Право. Журнал Высшей школы экономики. 2016. № 1. С. 177–188.

²⁴ Ткаченко И.Ю. Проблемы развития цифровых технологий // Российский внешнеэкономический вестник. 2018. № 9. С. 76–87.

²⁵ Романова Т.А., Малова А.Н. Проблема применения категории «стрессоустойчивость» в политике кибербезопасности Евросоюза // Вестник Московского университета. Серия 25: Международные отношения и мировая политика. 2019. Т. 11, № 1. С. 20–46.

²⁶ Вершинина Т.В., Карпович О.Г., Ногмова А.Ш. Проблемы кибербезопасности в эпоху COVID-19 // Вестник ученых-международников. – 2022. – № 1(19). – С. 12–27.

²⁷ Разумов Е.А. Политика КНР по обеспечению кибербезопасности // Россия и АТР. – 2017. – № 4(98). – С. 156–170.

²⁸ Полончук Р.А. Политика КНР по обеспечению кибербезопасности в условиях нарастающего противодействия со стороны США // Информационные войны. 2019. № 2(50). С. 60–63.

²⁹ Горян Э.В. Нормативно-правовая основа обеспечения национальной безопасности в киберпространстве: опыт Китайской Народной Республики // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2021. Т. 13, № 1. С. 115–124.

³⁰ Современные технологии эффективной политики: учеб. пособие. М.: УДН, 2008. 239 с.

³¹ Егорова-Гантман Е.В., Плешаков К.В. Политическая реклама. М., 1999. 240 с.

³² Кучерявый М.М. Государственная политика информационного суверенитета России в условиях современного глобального мира // Управленческое консультирование. 2015. № 2. С. 8–15.

Среди иностранных исследователей, изучающих управление Интернет-пространством, можно выделить Л. ДеНардис³³, Ф. Мусиани³⁴, М. Мюллер³⁵. Данные авторы рассматривают регулирование Интернета не только с точки зрения принимаемых законов, но и точки зрения борьбы за контроль над инфраструктурой и цифровой архитектурой.

Ряд иностранных авторов, таких как Л. Келли³⁶, Т. Рид³⁷, Б. Валериан, Б. Йенсен, Р. Манесс³⁸, Дж. Най³⁹, уделяют особое внимание исследованию понятия «кибербезопасность» и киберпространства как новой среды взаимодействия основных акторов международных отношений.

Кроме того, некоторые исследователи анализируют сущность цифровой среды, ее влияние на общественные институты и необходимость введения институциональных ограничений для государства и корпораций в цифровой среде. Так, например, Р. Дейберт⁴⁰ отмечает, что базовым принципом управления в сети Интернет должен быть принцип сдерживания, чтобы не позволять отдельным акторам аккумулировать неограниченные ресурсы и оказывать влияние на поведение других в цифровой среде. Другие авторы исследуют особенности свободы высказываний в сети, систему модерации в социальных сетях, формирование цифрового гражданского общества и другие

³³ DeNardis L. *The Global War for Internet Governance*. New Haven: Yale University Press, 2014. – 288 p.

³⁴ DeNardis L., Musiani F. *Governance by Infrastructure // The Turn to Infrastructure in Internet Governance*. London: Palgrave Macmillan, 2014. P. 3–21.

³⁵ Mueller M. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: The MIT Press, 2010. 320 p.

³⁶ Kello L. *The Virtual Weapon and International Order*. New Haven: Yale University Press, 2017. 336 p.

³⁷ Rid T. *Cyber War Will Not Take Place*. Oxford: Oxford University Press, 2013. 218 p.

³⁸ Valeriano B., Jensen B., Maness R. *Cyber Strategy: The Evolving Character of Power and Coercion*. New York: Oxford University Press, 2018. 288 p.

³⁹ Nye J. *Cyber Power*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010. 24 p.

⁴⁰ Deibert R. *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. Toronto: Signal (McClelland & Stewart), 2013. 336 p.

аспекты формирования, развития и регулирования цифровой среды: Д. Лайон⁴¹, Д. Э. Коэн⁴², Д. Кэй⁴³, З. Туфекчи⁴⁴, Х. Ниссенбаум⁴⁵.

Отдельный интерес представляет исследование Ш. Зубофф⁴⁶ в рамках изучения влияния цифровых корпораций на общество и их роли в формировании особой экономической и политической модели. Автор вводит понятие «надзорный капитализм», согласно которой технологические компании получают прибыль из систематического сбора и обработки поведенческих данных пользователей. Таким образом сбор статистики и ее анализ происходят не только для улучшения работы алгоритмов и сервисов, но также и для выявления интересов пользователей, прогнозирования их будущих действий. В данном контексте стоит выделить Н. Срничека⁴⁷, который исследовал «платформенный капитализм» и возросшую роль цифровых корпораций как новых политических акторов, оказывающих влияние на формирование экономической и политической действительности.

Многие иностранные исследователи уделяют особое внимание механизмам регулирования Интернета в КНР, институциональному оформлению системы цифрового контроля, регулирования платформ, управлению информационными потоками в сети, взаимосвязи государства и цифровых корпораций в КНР и др. К таким авторам можно отнести: Р. Кремерс⁴⁸, С. Сакс⁴⁹, Г. Костка⁵⁰, Ф. Шнайдер⁵¹, Э. Эсари⁵², Дж. Салливан⁵³, Г.

⁴¹ Lyon D. *Surveillance Studies: An Overview*. Cambridge: Polity Press, 2007. 243 p.

⁴² Cohen J.E. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford: Oxford University Press, 2019. 366 p.

⁴³ Kaye D. *Speech Police: The Global Struggle to Govern the Internet*. New York: Columbia Global Reports, 2019. 142 p.

⁴⁴ Tufekci Z. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven; London: Yale University Press, 2017. 360 p.

⁴⁵ Nissenbaum H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press, 2009. 304 .

⁴⁶ Зубофф Ш. Эпоха надзорного капитализма: битва за человеческое будущее на новых рубежах власти / пер. с англ. А.Ф. Васильева; под науч. ред. Я. Охонько, А. Смирнова. М.: Издательство Института Гайдара, 2022. 781 с.

⁴⁷ Срничек Н. Капитализм платформ / пер. с англ.; под науч. ред. М. Добряковой. М.: Изд. дом ВШЭ, 2019. 128 с.

⁴⁸ Creemers R. *Cybersecurity Law and Regulation in China: Securing the Smart State* // *China Law and Society Review*. 2023. Vol. 6, no. 2. P. 111–145.

Гринлиф⁵⁴.

На сегодняшний день Китайская Народная Республика является одним из наиболее активных участников процесса по глобальному регулированию Интернет-пространства. Работы китайских исследователей важны с точки зрения понимания подходов, которыми руководствуются власти КНР при реализации политики управления цифровым пространством, а также понимания стратегического видения Пекина в этом вопросе. Китайские ученые в своих трудах исследуют все аспекты процесса регулирования Интернета. Так, особую важность имеют труды Ци Шанцай⁵⁵, Ло Синь и Цай Юйтин⁵⁶, Куан Вэньбо и Фаньюань⁵⁷, Ван Сяовэй и Яо Юй⁵⁸, Чэнь Хунмэй⁵⁹, Цзоу Сюйи⁶⁰, Цзоу Цзюнь⁶¹,

⁴⁹ Sacks S. Addressing the Data Security Risks of US-China Technology Entanglement [Электронный ресурс]. Washington, DC: Brookings Institution, 2020. URL: <https://www.brookings.edu/wp-content/uploads/2020/11/Samm-Sacks.pdf> (дата обращения: 12.02.2023).

⁵⁰ Kostka G. China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval // *New Media & Society*. 2019. Vol. 21, no. 7. P. 1565–1593.

⁵¹ Schneider F. China's Digital Nationalism. New York: Oxford University Press, 2018. 291 p.

⁵² Esarey A., Kluver R. The Internet in China: Cultural, Political, and Social Dimensions (1980s–2000s). Great Barrington, MA: Berkshire Publishing Group, 2015. 272 p.

⁵³ Sullivan J. A Tale of Two Microblogs in China // *Media, Culture & Society*. 2012. Vol. 34, no. 6. P. 773–783.

⁵⁴ Greenleaf G. China's Completed Personal Information Protection Law: Rights Plus Cyber-security // *Privacy Laws & Business International Report*. 2021. No. 172. P. 20–23.

⁵⁵ Ци Шанцай (Qi Shangcai). 全球互联网治理困境：制度缺失与治理赤字 (Дилемма глобального управления Интернетом: институциональные недостатки и недоработки в управлении) // *廊坊师范学院学报(社会科学版)* (Журнал педагогического университета Ланфан. Издание по социальным наукам). 2020. № 36(04). С. 19–27.

⁵⁶ Ло Синь, Цай Юйтин (Luo Xin, Cai Yuting). 全球互联网治理规则制定的分布格局与中国进路 (Структура распространения нормотворческой деятельности в области глобального управления Интернетом и подход Китая) // *现代传播(中国传媒大学学报)* (Современные коммуникации. Журнал Коммуникационного университета Китая). 2022. № 44(03). С. 68–75.

⁵⁷ Куан Вэньбо, Фаньюань (Kuang Wenbo, Fang Yuan). 网络空间命运共同体理念下的全球互联网治理体系变革 (Трансформация глобальной системы управления Интернетом в соответствии с концепцией Сообщества судьбы в киберпространстве) // *武汉大学学报(哲学社会科学版)* (Журнал Уханьского университета. Издание по философии и социальным наукам). 2023. № 76(05). С. 38–46.

⁵⁸ Ван Сяовэй, Яо Юй (Wang Xiaowei, Yao Yu). 网络主权与全球互联网治理 (Сетевой суверенитет и глобальное управление Интернетом) // *哲学分析* (Философский анализ). 2018. № 9(01). С. 116–125, 198.

⁵⁹ Чэнь Хунмэй (Chen Hongmei). 全球互联网治理法治化思考 (Размышления о легализации глобального управления Интернетом) // *湘潭大学学报(哲学社会科学版)* (Журнал Сянтаньского университета. Издание по философии и социальным наукам). 2019. № 43(01). С. 82–86.

⁶⁰ Цзоу Сюйи (Zou Xuyi). 全球互联网治理困境与网络空间命运共同体构建的价值取向 (Дилемма глобального управления Интернетом и ценностная ориентация построения сообщества судьбы в киберпространстве) // *天津社会科学* (Тяньцзиньские социальные науки). 2020. № 2. С. 83–87.

⁶¹ Цзоу Цзюнь (Zou Jun). 全球互联网治理:未来趋势与中国议题 (Глобальное управление Интернетом: будущие тенденции и проблемы Китая) // *新闻与传播研究* (Журналистика и коммуникационные исследования). 2016. № 23(S1). С. 5–13, 125.

Ли Чжи и Тан Жуньхуа⁶², Чжан Тэнцзюнь⁶³, Ян Фэн⁶⁴, Чжан Синьбао и Сюй Кэ⁶⁵, Цуй Баого⁶⁶.

Некоторые исследования направлены на анализ отдельных аспектов регулирования цифрового пространства. Среди них можно отметить работы Лан Пин⁶⁷, С. Кутюр⁶⁸, Н. Билотта⁶⁹, И. Рау⁷⁰, П. Мейор⁷¹.

Важно подчеркнуть, что в вопросе изучения деятельности китайских средств массовой информации можно выделить достаточное количество научных работ, которые посвящены истории развития СМИ в КНР. Но в то же время недостаточно исследований, раскрывающих взаимосвязь и дающих описание отношениям политической власти и СМИ в КНР. В частности, не изучены в полной мере роль китайских медиа в политическом процессе, а также перспективы их развития. Несмотря на это ряд китайский исследователей в своих работах затрагивают такую проблематику, как роль и место средств

⁶² Ли Чжи, Тан Жуньхуа (Li Zhi, Tang Runhua). 多利益攸关方模式:构建全球互联网治理体系的路径研究 (Модель участия многих заинтересованных сторон: исследование пути к созданию глобальной системы управления Интернетом) // 传媒观察 (Наблюдение за СМИ). 2020. № 12. С. 21–28.

⁶³ Чжан Тэнцзюнь (Zhang Tengjun). 再论国际电信联盟在全球互联网治理中的地位和作用 (Еще одна дискуссия о статусе и роли Международного союза электросвязи в глобальном управлении Интернетом) // 改革与开放 (Реформа и открытость). 2019. № 16. С. 14–16.

⁶⁴ Ян Фэн (Yang Feng). 全球互联网治理、公共产品与中国路径 (Глобальное управление Интернетом, общественные блага и путь Китая) // 教学与研究 (Преподавание и научные исследования). 2016. № 9. С. 51–58.

⁶⁵ Чжан Синьбао, Сюй Кэ (Zhang Xinbao, Xu Ke). 网络空间主权的治理模式及其制度构建 (Модель управления суверенитетом в киберпространстве и ее институциональное построение) // 中国社会科学 (Китайские общественные науки). 2016. № 8. С. 139–158, 207–208.

⁶⁶ Цуй Баого (Cui Baoguo). 网络空间治理模式的争议与博弈 (Противоречивая и игровая модель управления киберпространством) // 新闻与写作 (Журналистика и писательство). 2016. № 10. С. 23–26.

⁶⁷ Лан Пин (Lang Ping). 网络空间国际治理与博弈 (Международное управление и игры в киберпространстве). Пекин: China Social Sciences Press, 2022.332 с.

⁶⁸ Кутюр С., Тоупин С. Что означает понятие «суверенитет» в цифровом мире? // Вестник международных организаций: образование, наука, новая экономика. 2020. Т. 15, № 4. С. 48–69.

⁶⁹ Bilotta N. Beyond the Digital Tax: The Challenges of the EU's Scramble for Technological Sovereignty // International Organisations Research Journal. 2020. Vol. 15, no. 4. P. 30–47.

⁷⁰ Рау И. К вопросу о новых геополитических тенденциях в свете перехода к технологиям 5G (2013–2021) // Современная научная мысль. 2021. № 3. С. 117–126.

⁷¹ Major P. Internet Governance: Trends and Realities. Part 1 // Biznes-Informatika. 2015. № 4(34). P. 7–14. DOI: 10.17323/1998-0663.2015.4.7.14; Major P. Internet Governance: Trends and Realities. Part 2 // Biznes-Informatika. 2016. № 1(35). P. 20–25.

массовой информации в условиях реформ и открытости в Китайской Народной Республике: Е Хао⁷², Ли Сигуан⁷³ и другие.

В рамках написания данного исследования большую роль сыграли также работы, которые были посвящены анализу характера взаимодействия политических акторов и прессы. К подобным материалам можно отнести работы Лю Хуанжун⁷⁴, Засурского Я.Н.⁷⁵, Рихтера А.Г.⁷⁶, Прохорова Е.П.⁷⁷ и др.

В настоящее время над изучением теоретических аспектов государственной информационной политики работают В.Д. Попов, А.В. Манойло, В.Ф. Ницевич, Ю.А. Нисневич, А.И. Кондратенко и др.

Изучением различных особенностей информационной политики занимались К.В. Маркелов⁷⁸, А.Н. Петрунин⁷⁹, В.В. Мистюков⁸⁰, М.Г. Дмитриев⁸¹ и другие.

Кроме того, для всестороннего изучения заданной в данном исследовании темы необходимо было также проанализировать работы, посвященные функционированию новых медиа на территории КНР и их регулированию. Так, например, в работах Я.В. Лексютиной⁸², А.В. Сахарова и А.В. Шелепова⁸³, О.Н.

⁷² Е Хао (Ye Hao). 政府新闻学: 传媒管理新办法 (Дела правительственной журналистики: новые методы правительства в отношении СМИ). Нанкин: Издательство Университета Фудань, 2007. 192 с.

⁷³ Ли Сигуан (Li Xiguang). 畸形的媒体 (Аномальная пресса). Шанхай: Издательство Университета Фудань, 2003. 345 с.

⁷⁴ Лю Хуажун (Liu Huarong). 大众传媒与政治 (СМИ и политика). Пекин: Издательство Пекинского университета, 2001. 284 с.

⁷⁵ Засурский Я.Н. Журналистика и мир на рубеже тысячелетий. М.: Изд-во Московского университета, 2000. 384 с.

⁷⁶ Свобода массовой информации в постсоветском пространстве. М.: Изд. ВК, 2007. 336 с.

⁷⁷ Прохоров Е. П. Журналистика и демократия. М., Изд. Аспект Пресс, 2001. - 352 с.

⁷⁸ Маркелов К.В. Общественный идеал как объект информационной политики: дис. ... д-ра полит. наук: 10.01.10. М., 2006. 350 с.

⁷⁹ Петрунин А.Н. Институт связей с общественностью Министерства обороны России в государственной информационной политике: особенности и направления оптимизации: автореф. дис. ... канд. полит. наук: 23.00.02. М., 2011. 22 с.

⁸⁰ Мистюков В.В. Информационная политика современной России в контексте формирующегося гражданского общества: дис. ... канд. полит. наук. М., 2012. 166 с.

⁸¹ Дмитриев М.Г. Региональная информационная политика как фактор формирования информационного пространства: дис. ... канд. полит. наук. М., 2004. 137 с.

⁸² Лексютина Я.В. Политика китайского руководства в вопросах контроля и регулирования Интернета // Проблемы Дальнего Востока. 2014. № 2. С. 202–214.

⁸³ Сахаров А.В., Шелепов А.В. Политика Китайской Народной Республики в сфере регулирования цифровых платформ // Вестник международных организаций. 2024. Т. 19, № 2. С. 145–160.

Глазунова и В.В. Авдеенко⁸⁴, Р.Р. Вильданова и Э.Н. Кутушевой⁸⁵, Ли Сяо⁸⁶ подробно раскрываются различные аспекты регулирования Интернет-пространства в КНР, в том числе законодательная база, регламентирующая деятельность граждан в информационном пространстве.

В ряде других работ отдельное внимание уделяется изучению национальных социальных сетей в КНР, их влияния на политический курс КПК, а также их роли в качестве одного из инструментов реализации государственной информационной политики китайскими властями. К таким работам можно отнести исследования Чжан Шуана⁸⁷, Цзинь Ханя⁸⁸, Ли Личи⁸⁹, Ли Сяо⁹⁰, Е.С. Надежкиной⁹¹ и др.

Важное место занимают исследования, посвященные цензуре в информационном пространстве и контролю информации в китайском сегменте Интернета. Механизмы интернет-цензуры и политики китайского руководства по контролю информационных потоков в своих работах описывают А.Г.

⁸⁴ Глазунов О.Н., Авдеенко В.В. Специфика правового регулирования сети Интернет в Китайской Народной Республике // Общество: политика, экономика, право. [нужно уточнить: год]. № 2. С. 93–96.

⁸⁵ Вильданов Р.Р., Кутушева Э.Н. Система государственного регулирования интернета в Китайской Народной Республике // Вестник УГНТУ. Наука, образование, экономика. Серия: Экономика. 2021. № 3. С. 115–122.

⁸⁶ Ли Сяо. Китайские новостные приложения на мировом рынке новых медиа: магистерская диссертация / Санкт-Петербургский государственный университет. 2017. 116 с.

⁸⁷ Чжан Шуан. Роль социальных сетей в формировании имиджа Китая // Вестн. Амурского гос. ун-та. 2014. Вып. 2(140). С. 257–260.

⁸⁸ Цзинь Хань. Влияние новых медиа на социализацию подростков Китая: дис. ... канд. филол. наук. М.: Российский университет дружбы народов, 2024. 215 с.

⁸⁹ Ли Личи. Роль новых медиа в создании имиджа правительства Китая: магистерская диссертация. СПб.: Санкт-Петербургский государственный университет, 2020. 124 с.

⁹⁰ Ли Сяо. Китайские новостные приложения на мировом рынке новых медиа: магистерская диссертация. СПб.: Санкт-Петербургский государственный университет, 2017. 130 с.

⁹¹ Надежкина Е.С. Имидж России в Китае в XXI веке на основе анализа медиа-платформ китайского сегмента сети Интернет: дис. ... канд. полит. наук. М.: Московский государственный университет, 2023. 210 с.

Людина и Е.С. Ефименко⁹², Е.Н. Щербакова и Т.Л. Гурулева⁹³, Чжан Сун⁹⁴, Т.А. Подшибякина⁹⁵, А.Г. Верник⁹⁶, А.П. Федоров⁹⁷, Лю Янь⁹⁸ и др.

Важно подчеркнуть, что китайские исследователи в рамках изучения подходов КНР к управлению цифровым пространством уделяют значительное внимание проблематике суверенитета и национальной безопасности в киберпространстве. Авторы из КНР анализируют условия распространения государственного суверенитета на цифровое пространство, подходы китайских властей к межгосударственному сотрудничеству по глобальному управлению Интернетом, а также концепцию киберсуверенитета в контексте выработки единых норм и правил по контролю сетевого пространства. Изучением данных вопросов занимаются: Чжу Шибин⁹⁹, Сюн Гуанцин и Ван Жуй¹⁰⁰, Ван Хухуа и Чжан Лэй¹⁰¹, Чжан Синьбао¹⁰², Ху Ли и Ци Айминь¹⁰³, Ян Линьюй¹⁰⁴, Чжан

⁹² Людина А.Г., Ефименко Е.С. Интернет-цензура в современном Китае: жесткий контроль и гибкая система урегулирования // Вестник Российского университета дружбы народов. Серия: Всеобщая история. 2022. Т. 14, № 2. С. 175–188.

⁹³ Щербакова Е.Н., Гурулева Т.Л. Интернет-цензура в Китае // Успехи современного естествознания. 2013. № 11. С. 197.

⁹⁴ Чжан Жун. СМИ и власть в Китае: проблемы взаимодействия: на примере анализа содержания газеты «Пекинская молодежь»: дис. ... канд. филол. наук: 10.01.10. М., 2011. 217 с.

⁹⁵ Подшибякина Т.А. «Золотой щит» Китая: политика управления мнемоническими интернет-практиками // Вестник Российского университета дружбы народов. Серия: Политология. - 2020. - Т. 22. - №2. - С. 194-204.

⁹⁶ Верник А.Г. Цензура в интернете: исторический аспект, современный опыт и перспективы [Электронный ресурс] // Дискуссия. 2015. № 11(52). С. 174–182. URL: <https://cyberleninka.ru/article/n/senzura-v-internete-istoricheskiy-aspekt-sovremennyyu-opyt-i-perspektivy> (дата обращения: 17.01.2023).

⁹⁷ Федоров А.П. Об опыте Китая по противодей-

ствию манипуляционным технологиям в социальных сетях Интернета // Вестник Московского государственного областного университета. Электронный журнал. 2018. № 2. С. 179–188.

⁹⁸ Лю Я. Публичная сфера под контролем: современный опыт регулирования Интернет-журналистики в КНР // Ойкумена. Регионоведческие исследования. 2016. № 2. С. 32–43.

⁹⁹ Чжу Шибин (Zhu Shibing). 世界范围内网络主权的主要观点综述 (Обзор основных взглядов на сетевой суверенитет в мировом масштабе) // 中国工程科学 (Инженерные науки Китая). 2016. № 18(06). С. 89–93.

¹⁰⁰ Сюн Гуанцин, Ван Жуй (Xiong Guangqing, Wang Rui). 全球互联网治理中的网络主权:历史演进、国际争议和中国立场 (Сетевой суверенитет в глобальном управлении Интернетом: историческая эволюция, международные споры и позиция Китая) // 学习与探索 (Обучение и исследования). 2024. № 4 (总第 345 期). С. 24–33.

¹⁰¹ Ван Хухуа, Чжан Лэй (Wang Huhua, Zhang Lei). 国家主权与互联网国际行为准则的制定 (Государственный суверенитет и разработка международных правил поведения в Интернете) // 河北法学 (Хэбэйская юридическая наука). 2015. № 33(12). С. 11–20.

¹⁰² Чжан Синьбао (Zhang Xinbao). 网络空间主权的治理模式及其制度构建 (Модель управления суверенитетом киберпространства и институциональное построение) // 中国社会科学 (Китайские общественные науки). 2016. № 8. С. 319–339.

¹⁰³ Ху Ли, Ци Айминь (Hu Li, Qi Aimin). 论“网络疆界”的形成与国家领网主权制度的建立 (Формирование «сетевых границ» и создание системы государственного сетевого суверенитета) // 法学论坛 (Юридический форум). 2016. № 2 (общ. № 164). С. 59–66.

Шудянь¹⁰⁵, Чэнь Чуньянь¹⁰⁶, Лу Вэй¹⁰⁷,

Кроме того, ряд авторов уделяли отдельное внимание вопросам рассмотрения процессов создания электронного правительства и его дальнейшего функционирования, в том числе и в КНР. Вопросы, связанные с формированием структур электронного правительства в КНР, в своих работах затрагивают Д. Шлегер¹⁰⁸ и Д.У. Зейферт¹⁰⁹. Значительный вклад в рассмотрение данной проблемы внесли и такие исследователи, как Пинь Ду, Шан Ю, Даолин Ян¹¹⁰; Йинь Ян¹¹¹, А. Оберхайдман¹¹².

Общие вопросы развития систем электронного правительства и факторов, которые оказывают значительное влияние на данные процессы, находят отражение в трудах П. Мартина¹¹³, Д.Э. Хиллмана¹¹⁴, Р.Э. Брауна¹¹⁵.

¹⁰⁴ Ян Линьюй (Yang Linyu). 网络主权视野下的互联网建设、运用、管理——“谷歌事件”的理性解读及其启示 (Строительство, использование и управление Интернетом в перспективе сетевого суверенитета: рациональная интерпретация «инцидента Google» и его значение) // 云南行政学院学报 (Вестник Административного института Юньнани). 2011. № 1. С. 105–108.

¹⁰⁵ Чжан Шудянь, Линь Жуйсинь (Zhang Shudian, Lin Ruixin). 论互联网对国家主权的侵蚀和强化 (Влияние Интернета на эрозию и укрепление государственного суверенитета) // 科技与法律 (Наука, технологии и право). 2005. № 4. С. 71–74.

¹⁰⁶ Чэнь Чуньянь (Chen Chunyan). 试析《俄罗斯互联网主权法》的背景与影响 (Анализ предпосылок и влияния «Закона об интернет-суверенитете России») // 传媒: MEDIA (Медиа). 2020. № 12. С. 50–55.

¹⁰⁷ Лу Вэй (Lu Wei). 坚持尊重网络主权原则 推动构建网络空间命运共同体——学习习近平总书记在第二届世界互联网大会上重要讲话精神的体会与思考 (Придерживаться принципа уважения сетевого суверенитета и содействовать формированию сообщества единой судьбы в киберпространстве: размышления о ключевых положениях выступления Генерального секретаря на Второй Всемирной интернет-конференции) // 中国信息安全 (Информационная безопасность Китая). 2016. № 3. С. 34–35.

¹⁰⁸ Shlaeger J. E-Government in China: Technology, Power and Local Government Reform. China Policy Series. London: Routledge, 2020. 184 p.

¹⁰⁹ Seifert J.W., Chung J. Using E-Government to Reinforce Government Citizen Relationships: Comparing Government Reform in the United States and China. London: Routledge, 2020. 184 p.

¹¹⁰ Du Ping, Yu Shiyang, Yang Daoling. The Development of E-Governance in China: Improving Cybersecurity and Promoting Informatization as Means for Modernizing State Governance. Research Series on the Chinese Dream and China's Development Path. New York: Springer, 2019. 357 p.

¹¹¹ Jiang Y. Social Media and e-Diplomacy in China: Scrutinizing the Power of Weibo. New York: Palgrave Pivot, 2017. 159 p.

¹¹² Oberheitmann A., Heupel T., Yang J., Wang Z. German and Chinese Contributions to Digitalisation: Opportunities, Challenges and Impacts. München: Springer Gabler, 2020. 383 p.

¹¹³ Martin P. China's Civilian Army: The Making of Wolf Warrior Diplomacy. Oxford: Oxford University Press, 2021. 320 p.

¹¹⁴ Hillman J.E. The Digital Silk Road: China's Quest to Wire the World and Win the Future. New York: Harper Business, 2021. 368 p.

¹¹⁵ Brown R.E. The Global Foundations of Public Relations: Humanism, China and the West. Abingdon-on-Thames: Routledge, 2021. 232 p.

Таким образом, можно сделать вывод, что проблематика государственного регулирования Интернета, управления киберпространством в КНР, влияния цифровизации на отношения государства и цифровых корпораций получила существенную научную разработку: сформирован широкий корпус работ, посвященных данным вопросам. Вместе с тем, несмотря на большое количество исследований, в ряде публикаций в недостаточной степени широко раскрыта и проанализирована нормативно-правовая база, регулирующая мировую сферу. Это особенно актуально после 2017 года, когда принятие Закона КНР о Кибербезопасности существенно изменило правовые рамки контроля за Интернет-пространством. В настоящее время нормативно-правовая база КНР, направленная на регулирование цифрового пространства ежегодно обновляется, что требует проведения новых исследований для выявления качественно новых подходов китайских властей к регулированию киберпространства. Кроме того, во многих работах практически не анализируются внутренние документы и регламенты цифровых платформ, которые позволяют проследить, каким образом государственные нормы и требования реализуются в практической плоскости.

Объектом исследования являются политические аспекты регулирования Интернет-пространства.

Предметом исследования является политика государственного регулирования Интернет-пространства КНР в условиях цифровизации.

Целью данной диссертационной работы является всестороннее исследование государственной политики КНР по регулированию Интернет-пространства, выявление ключевых направлений и инструментов ее реализации, а также определение факторов, оказывающих влияние на её формирование и реализацию.

Для достижения поставленной цели были сформулированы следующие **задачи**:

1. Выявить основные концептуальные подходы и методологии управления интернет- пространством.
2. Определить основные подходы к интерпретации понятия «государственная информационная политика» в научном дискурсе.
3. Исследовать условия цифровизации политики и раскрыть сущность ключевых акторов государственного регулирования.
4. Выделить идеологическую базу политики КНР по регулированию Интернет-пространства.
5. Определить законодательные основания государственной информационной политики КНР в сфере регулирования Интернета.
6. Изучить процессы адаптации государственной власти Китая к развитию и трансформации социальных сетей.
7. Охарактеризовать механизмы взаимодействия государства и цифровых корпораций в КНР в рамках реализации политики регулирования Интернета.
8. Исследовать технологии и механизмы реализации государственной интернет-цензуры в КНР, определить их роль в обеспечении информационной безопасности.
9. Рассмотреть перспективы трансформации государственной информационной политики Китая под влиянием внешних цифровых угроз.

Хронологические рамки исследования охватывают период с 2009 по настоящее время. Нижний предел обоснован датой начала реализации блокировки доступа к западным социальным сетям и сайтам, а также последующей активизации процесса создания собственных национальных платформ. Верхний предел обусловлен продолжающимся активным развитием цифровых технологий, включая внедрение 5G, искусственного интеллекта, появление различных социальных сетей и платформ, что позволяет проследить

актуальные тенденции в развитии информационного пространства КНР и адаптации государственной политики к ним.

Теоретико-методологические основы исследования составляет ряд теоретических подходов и методов политической науки, а также смежных дисциплин, что определяет междисциплинарность данного исследования.

Основой для формирования системы регулирования Интернета служит *теория управления*. Важно подчеркнуть, что управление Интернетом является составной частью более широкой теории глобального управления. теория управления акцентирует внимание на том, что современное регулирование осуществляется не только через иерархические государственные институты и правовые нормы, но и через механизмы координации, взаимодействия и распределения функций между государством, цифровыми платформами, экспертным сообществом и другими участниками. Применительно к интернет-пространству данный подход позволяет анализировать государственное регулирование как систему многоуровневого управления, включающую законодательные и административные меры, технические инструменты контроля и практики платформенного саморегулирования, что особенно важно в условиях цифровизации и трансграничного характера сетевой среды.

При проведении данного исследования автор опирался также на основы *мир-системного подхода* И. Валлерстайна. Так, изучение механизмов функционирования Интернета и его регулирования предполагает, что одни государства являются лидерами в технологической гонке и определяют векторы развития Интернета, а другие лишь пользуются достижениями технологического прогресса.

Кроме того, в рамках проведения анализа политики государственного регулирования Интернет-пространства в КНР автор исходил из *теории «надзорного капитализма»* Шошаны Зубофф, согласно которой систематический сбор аналитических данных и статистики на различных

платформах и цифровых ресурсах направлен на прогнозирование поведения пользователей. Так, это может быть использовано для направления фокуса внимания пользователей на те или иные явления или услуги как в экономических целях, так и в политических. Также автор рассматривал теорию «*платформенного капитализма*» Н. Срничека, согласно которой в современной экономике одним из ключевых акторов цифровые платформы, которые организуют и контролируют потоки данных для получения прибыли. В рамках данного исследования данная теория адаптирована под внутриполитические процессы: цифровые корпорации КНР рассматриваются в качестве важных акторов реализации политики регулирования Интернета как с точки зрения адаптации законодательной базы, так и с точки зрения имплементации решений, принятых государственными ведомствами.

Важную роль при анализе подходов стран к регулированию Интернет-пространства играет *системный подход*, в рамках которого Интернет рассматривается как единая система с большим количеством горизонтальных и вертикальных связей как внутри государств, так и на международном уровне.

В процессе проведения исследования в рамках диссертационной работы были применен ряд методов.

Одним из методов исследования выступает *компаративный анализ*. Применение этого метода позволило определить характерные, уникальные для Китая особенности системы регулирования Интернета, а также показать специфику взаимодействия государства, цифровых платформ и пользователей в условиях цифровой трансформации.

Для определения динамики формирования и реализации государственной политики в сфере регулирования интернет-пространства применялся *метод ивент-анализа*.

Для изучения официальных нормативно-правовых актов, выступлений политических лидеров, информации, публикуемой на различных цифровых площадках, был применен *контент-анализ*.

При подготовке данного исследования также был использован такой метод, как *case-study*, что позволило рассмотреть конкретные примеры цензуры и блокировки контента в китайских социальных сетях для того, чтобы проследить, каким образом законы, регулирующие Интернет-пространство КНР, применяются на реальных ситуациях.

Эмпирическую базу исследования составили официальные документы, регламентирующие правила пользования Интернетом на территории КНР и регулирующие деятельность пользователей, различные статистические данные по активности пользователей, выступления официальных лиц, различные публикации в социальных сетях, конкретные примеры реализации тех или иных решений в рамках государственной информационной политики Китая и прочее.

Так, при проведении данного исследования были проанализированы различные **нормативно-правовые акты КНР**, регулирующие киберпространство. К таковым можно отнести: Закон КНР «О кибербезопасности»¹¹⁶, Закон КНР «О национальной безопасности»¹¹⁷, Закон КНР «О национальной разведывательной деятельности»¹¹⁸, Закон КНР «О противодействии терроризму»¹¹⁹, Закон КНР «О безопасности данных»¹²⁰, Закон

¹¹⁶ 中华人民共和国网络安全法 (Закон КНР о кибербезопасности) [Электронный ресурс] // Центральная комиссия по вопросам киберпространства КНР. URL: https://www.cac.gov.cn/2016-11/07/c_1119867116.htm (дата обращения: 19.06.2022).

¹¹⁷ 中华人民共和国国家安全法 (Закон КНР «О национальной безопасности») [Электронный ресурс] // Официальный сайт Постоянного комитета ВСНП КНР. URL: http://www.npc.gov.cn/zgrdw/npc/xinwen/2015-07/01/content_1940614.htm (дата обращения: 21.06.2022).

¹¹⁸ 中华人民共和国国家情报法 (Закон КНР «О национальной разведывательной деятельности») [Электронный ресурс] // Официальный сайт Постоянного комитета ВСНП КНР. URL: http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-06/12/content_2055873.htm (дата обращения: 15.06.2022).

¹¹⁹ 中华人民共和国反恐怖主义法 (Закон КНР «О противодействии терроризму») [Электронный ресурс] // Официальный сайт Министерства юстиции КНР. URL: https://www.moj.gov.cn/pub/sfbgw/flfggz/flfggzflty/fltysfxzxxgflfg/201812/t20181225_151327.html (дата обращения: 15.06.2022).

КНР «О защите персональной информации»¹²¹, Закон КНР «О безопасности сетевой инфраструктуры и сети интернет»¹²², Закон «О защите государственной тайны»¹²³, Закон КНР «О защите статуса, прав и законных интересов военнослужащих»¹²⁴, «Правила управления безопасностью сетевых данных»¹²⁵, «Правила по борьбе с кибернасилием»¹²⁶, «Правила управления сервисами интернет-комментариев»¹²⁷, «Правила управления оценкой безопасности новых технологий и приложений в новостных интернет-сервисах»¹²⁸, «Положение об административных процедурах правоприменения в сфере управления интернет-контентом»¹²⁹, «Порядок управления услугами интернет-информации»¹³⁰ и другие.

¹²⁰ 中华人民共和国数据安全法 (Закон КНР «О безопасности данных») [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: https://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm (дата обращения: 24.01.2025).

¹²¹ 中华人民共和国个人信息保护法 (Закон КНР «О защите персональной информации») [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: https://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm (дата обращения: 24.01.2026).

¹²² 中华人民共和国网络安全法 (Закон КНР «О кибербезопасности» в редакции 2025 г.) [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: https://www.cac.gov.cn/2025-12/29/c_1768735112911946.htm (дата обращения: 24.11.2025).

¹²³ 中华人民共和国保守国家秘密法 (Закон КНР «О защите государственной тайны») [Электронный ресурс] // Официальный сайт Постоянного комитета ВСНП КНР. URL: http://www.npc.gov.cn/npc/c2/c30834/202402/t20240227_434859.html (дата обращения: 24.11.2025).

¹²⁴ 中华人民共和国军人地位和权益保障法 (Закон КНР «О защите статуса, прав и законных интересов военнослужащих») [Электронный ресурс] // Официальный сайт Министерства по делам ветеранов КНР. URL: https://www.mva.gov.cn/sy/xx/bnxx/202106/t20210611_48036.html (дата обращения: 20.11.2024).

¹²⁵ «网络数据安全条例» (Положение об управлении безопасностью сетевых данных) [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/gongbao/2024/issue_11646/202410/content_6980863.html (дата обращения: 20.11.2024).

¹²⁶ «网络暴力信息治理规定» (Правила по борьбе с кибернасилием) [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: https://www.cac.gov.cn/2024-06/14/c_1720043894161555.htm (дата обращения: 24.11.2024).

¹²⁷ «互联网跟帖评论服务管理规定» (Положение об управлении сервисами интернет-комментариев) [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: https://www.cac.gov.cn/2022-11/16/c_1670253725725039.htm (дата обращения: 24.11.2024).

¹²⁸ «互联网新闻信息服务新技术新应用安全评估管理规定» (Положение об управлении оценкой безопасности новых технологий и новых приложений в сервисах интернет-новостей и информации) [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: https://www.cac.gov.cn/2017-10/30/c_1121878049.htm (дата обращения: 24.11.2024).

¹²⁹ «互联网信息服务内容管理行政执法程序规定» (Положение об административных процедурах правоприменения в сфере управления интернет-контентом) [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: https://www.cac.gov.cn/2017-05/02/c_1120902931.htm (дата обращения: 24.11.2024).

¹³⁰ «互联网信息服务管理办法» (Порядок управления услугами интернет-информации) [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: https://www.cac.gov.cn/2000-09/30/c_126193701.htm (дата обращения: 24.11.2024).

Также были исследованы **документы стратегического планирования в сфере регулирования Интернета в КНР**: План государственной информатизации в рамках 9-й пятилетки и перспективные цели до 2010 г.¹³¹, План национальной стратегии инновационного развития¹³², Государственная стратегия по развитию информатизации на период с 2006 по 2020 г.¹³³, Национальная стратегия кибербезопасности¹³⁴, Белая книга «Развитие правовой системы управления интернетом в Китае в новую эпоху»¹³⁵, Белая книга «Совместное формирование сообщества единой судьбы в киберпространстве»¹³⁶, XIV пятилетний план: «Национальная информатизация»¹³⁷, «Стратегия развития национальной информатизации на 2006—2020 годы»¹³⁸ и другие.

К материалам, формирующим эмпирическую базу исследования, можно также отнести **выступления и заявления руководства КНР, включая**

¹³¹ 中华人民共和国国民经济和社会发展“九五”计划和2010年远景目标纲要 (План государственной информатизации в рамках 9-й пятилетки и перспективные цели до 2010 г.) [Электронный ресурс] // Официальный сайт Государственного комитета по развитию и реформам КНР. URL: <https://www.ndrc.gov.cn/fggz/fzzlgh/gjzgh/200709/P020191029595686994247.pdf> (дата обращения: 24.11.2024).

¹³² 中共中央 国务院印发《国家创新驱动发展战略纲要》 (План национальной стратегии инновационного развития) [Электронный ресурс] // Официальный сайт Государственного комитета по развитию и реформам КНР. URL: <https://www.ndrc.gov.cn/fggz/fzzlgh/gjzgh/200709/P020191029595686994247.pdf> (дата обращения: 17.02.2023).

¹³³ 2006—2020年国家信息化发展战略 (Государственная стратегия по развитию информатизации на период с 2006 по 2020 г.) [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/gongbao/content/2006/content_315999.htm (дата обращения: 05.09.2023).

¹³⁴ 《国家网络空间安全战略》 (Национальная стратегия кибербезопасности) [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: https://www.cac.gov.cn/2016-12/27/c_1120195926.htm (дата обращения: 19.01.2024).

¹³⁵ 《新时代的中国网络法治建设》白皮书 (全文) (Белая книга «Развитие правовой системы управления интернетом в Китае в новую эпоху», полный текст) [Электронный ресурс] // Официальный сайт Пресс-канцелярии Государственного совета КНР. URL: http://www.scio.gov.cn/zfbps/zfbps_2279/202303/t20230320_709278.html (дата обращения: 24.11.2024).

¹³⁶ 《携手构建网络空间命运共同体》白皮书 (Белая книга «Совместное формирование сообщества единой судьбы в киберпространстве») [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: https://www.cac.gov.cn/2022-11/07/c_1669457523014880.htm (дата обращения: 02.09.2025).

¹³⁷ 《“十四五”国家信息化规划》 (Национальный план информатизации в рамках XIV пятилетки) [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: http://www.cac.gov.cn/2021-12/27/c_1642205314518676.htm (дата обращения: 24.01.2025).

¹³⁸ 《中共中央办公厅 国务院办公厅关于印发〈2006—2020年国家信息化发展战略〉的通知》 (Уведомление Канцелярии ЦК КПК и Канцелярии Государственного совета КНР о публикации «Стратегии развития национальной информатизации на 2006—2020 годы») [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/gongbao/content/2006/content_315999.htm (дата обращения: 26.04.2025).

председателя КНР Си Цзиньпина, о важности регулирования Интернета, о киберсуверенитете и кибербезопасности и др.

К следующей группе документов, использованных в рамках данного исследования, относятся различные **статистические и аналитические материалы**. К таким материалам относятся: серия статистических докладов «О развитии Интернета в Китае» (серия докладов China Internet Network Information Center (CNNIC))¹³⁹, 53-й статистический отчет о развитии интернета в Китае¹⁴⁰, «Доклад о развитии цифрового Китая (2022)»¹⁴¹, «Доклад о развитии интернета в Китае 2025» и «Доклад о развитии мирового интернета 2025»¹⁴², Статистический ежегодник Китая (2021 г.)¹⁴³, Статистический ежегодник Китая (2022 г.)¹⁴⁴, Статистический ежегодник Китая (2023 г.)¹⁴⁵, Статистический ежегодник Китая (2024 г.)¹⁴⁶, Статистический ежегодник Китая (2025 г.)¹⁴⁷,

¹³⁹ The 55th Statistical Report on China's Internet Development (55-й статистический доклад о развитии Интернета в Китае) [Электронный ресурс] // China Internet Network Information Center (CNNIC). 62 p. URL: <https://www.cnnic.com.cn/IDR/ReportDownloads/202505/P020250514564119130448.pdf> (дата обращения: 24.05.2025).

¹⁴⁰ 第53次《中国互联网络发展状况统计报告》发布：我国网民规模达10.92亿人 (Публикация 53-го статистического отчета о развитии Интернета в Китае: численность интернет-пользователей достигла 1,092 млрд человек) [Электронный ресурс] // Официальный сайт газеты «Жэньминь жибао». URL: <http://finance.people.com.cn/n1/2024/0322/c1004-40201311.html> (дата обращения: 24.01.2025).

¹⁴¹ 国家互联网信息办公室发布《数字中国发展报告（2022年）》 (Национальное управление по делам киберпространства опубликовало «Доклад о развитии цифрового Китая (2022)») [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: https://www.cac.gov.cn/2023-05/22/c_1686402318492248.htm (дата обращения: 24.01.2025).

¹⁴² 《中国互联网络发展报告2024》和《世界互联网发展报告2024》蓝皮书发布 (Публикация синих книг «Доклад о развитии Интернета в Китае 2024» и «Доклад о развитии мирового Интернета 2024») [Электронный ресурс] // Официальный сайт Всемирной интернет-конференции. URL: https://cn.wicinternet.org/node_158585.htm (дата обращения: 24.01.2026).

¹⁴³ 中国统计年鉴2021 (Статистический ежегодник Китая 2021 г.) [Электронный ресурс] // Официальный сайт Национального бюро статистики КНР. URL: <https://www.stats.gov.cn/sj/ndsj/2021/indexch.htm> (дата обращения: 24.01.2025).

¹⁴⁴ 中国统计年鉴2022 (Статистический ежегодник Китая 2022 г.) [Электронный ресурс] // Официальный сайт Национального бюро статистики КНР. URL: <https://www.stats.gov.cn/sj/ndsj/2022/indexch.htm> (дата обращения: 24.01.2025).

¹⁴⁵ 中国统计年鉴2023 (Статистический ежегодник Китая 2023 г.) [Электронный ресурс] // Официальный сайт Национального бюро статистики КНР. URL: <https://www.stats.gov.cn/sj/ndsj/2023/indexch.htm> (дата обращения: 24.01.2025).

¹⁴⁶ 中国统计年鉴2024 (Статистический ежегодник Китая 2024 г.) [Электронный ресурс] // Официальный сайт Национального бюро статистики КНР. URL: <https://www.stats.gov.cn/sj/ndsj/2024/indexch.htm> (дата обращения: 24.01.2025).

¹⁴⁷ 中国统计年鉴2025 (Статистический ежегодник Китая 2025 г.) [Электронный ресурс] // Официальный сайт Национального бюро статистики КНР. URL: <https://www.stats.gov.cn/sj/ndsj/2025/indexch.htm> (дата обращения: 24.01.2026).

«Ежегодник информационной индустрии Китая»¹⁴⁸, Статистический ежегодник электронной и информационной промышленности Китая¹⁴⁹, Доклад «О развитии информационного общества в Китае»¹⁵⁰, Доклад об индексе развития цифровой экономики Китая 2023 г.¹⁵¹, Доклад о развитии цифрового Китая (2024 г.)¹⁵², Отчёт компании Baidu в области экологии, социальной ответственности и корпоративного управления за 2023 год¹⁵³, Отчёт компании Baidu в области экологии, социальной ответственности и корпоративного управления за 2024 год¹⁵⁴, Годовой отчёт компании Tencent за 2023 год¹⁵⁵, Годовой отчёт компании Tencent за 2024 год¹⁵⁶, Годовой отчёт Национального

¹⁴⁸ 2024 年版《中国信息产业年鉴》出版发行 (Публикация издания 2024 года «Ежегодник информационной индустрии Китая») [Электронный ресурс] // Официальный сайт Национального исследовательского центра по промышленной информационной безопасности. URL: https://www.cics-cert.org.cn/webapp/webpage/articlecontent_103005_1995786318059147265.html (дата обращения: 27.01.2025).

¹⁴⁹ 中国电子信息产业统计年鉴 (Статистический ежегодник электронной и информационной промышленности Китая) [Электронный ресурс] // Информационный ресурс по отраслевой статистике КНР. URL: <https://www.shujuku.org/electronic-information-industry-statistical-yearbook.html> (дата обращения: 12.01.2026).

¹⁵⁰ 中国信息社会发展报告 2016 (Доклад о развитии информационного общества в Китае, 2016 г.) [Электронный ресурс] // Официальный сайт Государственного информационного центра КНР. URL: https://www.sic.gov.cn/sic/82/566/0518/6358_pc.html (дата обращения: 24.01.2026).

¹⁵¹ 中国数字经济发展指数报告 2023 (Доклад об индексе развития цифровой экономики Китая 2023 г.) [Электронный ресурс] // Официальная публикация Пятого исследовательского института Министерства промышленности и информатизации КНР. URL: <https://13115299.s21i.faiusr.com/61/1/ABUIABA9GAAG1c2ypwYotKiqzQQ.pdf> (дата обращения: 24.01.2026).

¹⁵² «数字中国发展报告 (2024 年)» (Доклад о развитии цифрового Китая, 2024 г.) [Электронный ресурс] // Официальный сайт Национального управления по делам данных КНР. URL: <https://www.nda.gov.cn/sjj/zhuanti/sjzgzxd/szzgbg/0605/ff808081-96b465bf-0197-3dd5a76f-05c7.pdf> (дата обращения: 24.01.2026).

¹⁵³ Baidu 2023 Environmental, Social and Governance Report (Отчет Baidu в области экологии, социальной ответственности и корпоративного управления за 2023 год) [Электронный ресурс] // Официальный сайт компании Baidu. URL: <https://esg.baidu.com/Uploads/File/2024/05/17/Baidu%202023%20Environmental,%20Social%20and%20Governance%20Report.20240517150706.pdf> (дата обращения: 24.01.2025).

¹⁵⁴ Baidu 2024 Environmental, Social and Governance Report (Отчет Baidu в области экологии, социальной ответственности и корпоративного управления за 2024 год) [Электронный ресурс] // Официальный сайт компании Baidu. URL: <https://esgs.cdn.bcebos.com/2025/04/28/a2/39a2aaa4f728f4e2d0aebaff346c045e.pdf> (дата обращения: 24.05.2025).

¹⁵⁵ Tencent Annual Report 2023 (Годовой отчет компании Tencent за 2023 год) [Электронный ресурс] // Официальный сайт компании Tencent. URL: <https://static.www.tencent.com/uploads/2024/04/08/e95c902973fc282be3b3e285c6245281.pdf> (дата обращения: 24.05.2024).

¹⁵⁶ Tencent Annual Report 2024 (Годовой отчет компании Tencent за 2024 год) [Электронный ресурс] // Официальный сайт компании Tencent. URL: <https://static.www.tencent.com/uploads/2025/04/08/1132b72b565389d1b913aea60a648d73.pdf> (дата обращения: 24.04.2025).

бюро статистики за 2023 год¹⁵⁷, Статистический отчет компании Alibaba за 2023 год¹⁵⁸ и другие.

Эмпирическую базу данного исследования также составляют **материалы китайских и зарубежных СМИ, интернет-платформ** на русском, китайском и английском языках.

Научная новизна исследования: в исследовании раскрыта специфика политики государственного регулирования интернет-пространства КНР в условиях цифровизации, где Китай представлен как уникальный пример формирования цифрового суверенитета.

Впервые комплексно проанализированы механизмы киберуправления в КНР, сочетающие жесткий контроль над инфраструктурой (физический уровень), создание национальных стандартов и платформ (логический уровень) и нормативное регулирование данных и контента (прикладной уровень).

Уточнена роль идеологии в цифровом управлении: Интернет в КНР выступает не только как технологическая система, но и как инструмент партийного контроля и укрепления государственной власти.

В данном исследовании концептуально проанализирован ряд терминов и теоретических конструкций, которые используются китайскими исследователями и которые и анализ которых в русскоязычной литературе носит фрагментарный характер. К таким терминам можно отнести: «сетевой гегемонизм» (网络霸权主义), «право на сетевую территорию» (领网权), «сетевая власть» (网络权/网络权力), «инфраструктурная власть» (信息基础权

¹⁵⁷ Годовой отчет Национального бюро статистики КНР [Электронный ресурс] // Официальный сайт Национального бюро статистики КНР. URL: https://www.stats.gov.cn/zt_18555/tjz/tjzjs/fzjstdt/202406/t20240607_1954458.html (дата обращения: 24.03.2025).

¹⁵⁸ Alibaba Group Holding Limited Annual Report 2023 (Годовой отчет компании Alibaba Group за 2023 год) [Электронный ресурс] // Официальный сайт компании Alibaba Group. URL: <https://static.alibabagroup.com/reports/fy2023/ar/ebook/en/16/index.html> (дата обращения: 26.10.2024).

力), «право на данные» (数据权). В исследовании выявлены и охарактеризованы особенности взаимодействия государства и цифровых платформ в КНР.

Кроме того, введен в научный оборот комплекс ранее не использовавшихся в российской политологической литературе источников: в исследовании впервые на русском языке сопоставлены правила и режимы модерации контента на платформах Weibo, Douyin и WeChat с действующей нормативно-правовой базой и стратегическими установками КНР в сфере регулирования Интернет-пространства.

Практическая значимость исследования политики Китайской Народной Республики по регулированию Интернет-пространства состоит в том, что результаты данного исследования могут найти применение в практической деятельности сотрудниками различных аналитических институтов, а также могут быть использованы для подготовки аналитических записок и доколов по соответствующей теме. Кроме того, выводы, сделанные в данном исследовании могут быть взяты в качестве рекомендаций для разработки стратегий и механизмов реализации инерционной политики различными российскими государственными ведомствами. Результаты исследования могут быть применены представителями бизнес-среды для адаптации стратегии выхода в китайское информационное пространство. Также материалы данного исследования могут быть взяты в качестве основы при подготовке спецкурса или серии лекции по соответствующей дисциплине.

Апробация работы. Основные положения и выводы данной диссертации отражены в 5 статьях соискателя, опубликованных в периодических изданиях, включенных в перечень российских рецензируемых научных журналов, а также были отражены в рамках выступлений автора на всероссийских и международных научных конференциях.

Основные положения, выносимые на защиту:

- Интернет-пространство следует рассматривать в качестве особой сферы реализации публичного управления, в рамках которой теории сетевого управления, платформенного капитализма, киберсуверенитета и сетевого гегемонизма позволяют определить интернет в качестве многоуровневой среды для политической коммуникации и самостоятельного объекта политики.
- Государственная информационная политика в условиях цифровизации эволюционирует от простого регулирования содержания к управлению цифровыми средами, включая алгоритмическую модерацию, архитектуру платформ и циркуляцию данных, что позволяет государству задавать условия формирования общественного восприятия.
- Цифровизация приводит к расширению перечня акторов, вовлеченных в государственные политические процессы, и одновременно изменяет характер их взаимодействия, формируя модели управления.
- Согласно идеологическим основам политики КНР по регулированию Интернет-пространства, цифровая среда рассматривается в качестве нового измерения, на которое распространяется государственный суверенитет и действие национальных интересов. Меры, предпринимаемые китайскими властями, основаны на концепциях киберсуверенитета (网络主权) и всеобъемлющей национальной безопасности (总体国家安全观), стратегическая цель построения «сетевой державы» (网络强国) и принципе управления интернетом на основе закона» (依法治网).
- Законодательные основания государственной политики КНР по регулированию Интернет-пространством определены широким спектром нормативно-правовых актов, которые создают комплексную систему

контроля за распространением данных и функционирование цифровых платформ и СМИ, основной целью которого является обеспечение политической и общественной стабильности.

- Происходит институционализация присутствия органов государственной власти на ключевых цифровых площадках (Weibo, WeChat, Douyin) и использование этих площадок как инструментов политической коммуникации, мобилизации и мониторинга общественных настроений.
- Национальные китайские цифровые платформы, такие как Wechat, Weibo, Douyin, Bilibili, Kuaishou и др., играют роль не только инструментов для коммуникации, но и ключевых инструментов реализации государственной информационной политики.
- Механизм цензуры в Китае основан на сочетании автоматизированных систем (искусственный интеллект, машинное обучение) и человеческого фактора, что обеспечивает высокую эффективность фильтрации и блокировки нежелательного контента, а также оперативное реагирование на информационные угрозы.
- Под влиянием внешних цифровых угроз и международной технологической конкуренции политика КНР по регулированию информационной среды демонстрирует тенденцию к дальнейшему усилению «безопасностного» компонента, углублению контроля над трансграничными потоками данных и стремлению к формированию независимого цифрового информационного пространства.

Соответствие паспорту научной специальности. Данная работа соответствует паспорту научной специальности 5.5.2 «Политические институты, процессы, технологии» по следующим пунктам:

1. Глобализация, сетевизация и цифровизация: политические аспекты;
2. Информационные процессы и управление политическими коммуникациями: традиционные СМИ, социальные медиа и сети;

3. Политические технологии и специфика их применения;
4. Этапы, механизмы и технологии принятия политических решений, критерии их эффективности.

Структура данного диссертационного исследования соответствует поставленным исследовательским задачам. Работа состоит из введения, трех глав, заключения, списка источников и литературы. Первая глава посвящена теоретико-методологическим основам исследования интернет-пространства и государственной информационной политики. Вторая глава посвящена анализу идеологических и законодательных аспектов политики КНР по регулированию интернет-пространства. Третья глава посвящена описанию инструментов, акторов и тенденций развития государственной информационной политики КНР по регулированию Интернетом.

Глава I. Теоретико-методологические основы исследования интернет-пространства в контексте государственной информационной политики.

1.1. Концептуальные подходы и методологии управления интернет-пространством.

Слово «управление» имеет греческие корни и происходит от глагола «kubernaein», что означает управлением плавательным судном, контроль и руководство экипажем судна.

В настоящее время данный термин применим к процессам, связанным с целенаправленным воздействием на систему или группу лиц для того, чтобы достичь определенных целей.

В рамках государства и его деятельности отдельное внимание следует уделить термину «государственное управление». Это деятельность государственных органов власти, лиц, наделенных властью, а также соответствующих органов по реализации разработанный государством стратегии для того, чтобы достигнуть целей, имеющих общественную значимость. Другими словами, это имплементация решений, которые принимаются на государственном уровне, действия органов власти по решению тех или иных вопросов, результаты которых оказывают влияние на жизнь общества и государства. Важно подчеркнуть, что термины «государственное управление» и «политика» не идентичны. Так, если политика подразумевает принятие решений, которые основаны на текущем состоянии дел внутри государства и на международной арене, то государственное управление направлено на обеспечение успешной и эффективной реализации этих решений.

Так, появление теории управления в XX веке в определенной степени обусловлено неэффективностью рыночных механизмов и государственного регулирования. Несмотря на то, что рыночная система позволяет обеспечивать эффективное распределение ресурсовой базы, она склонна к сбоям: монополия,

безработица, неравномерное распределение ресурсов и прочее. Кроме того, после окончания Второй мировой войны роль международного правительства значительно возросла, в то время как национальные государственные структуры перестали быть эффективны. Этот фактор в том числе может рассматриваться в качестве одной из причин кризиса в сфере государственного управления. Правительство стран не справлялись с решением транснациональные проблем и избежать международной анархии.

Теория управления стала формироваться в том числе и во время кризиса парадигмы социальных наук в 1970-х - 1980-х годах: используемые ранее теоретические подходы перестали объяснять комплексные процессы, происходившие в обществе. На протяжении долгого времени подходы к мышлению и восприятию действительности в данной сфере основывались на сравнении противоположностей: между государственными и рыночными механизмами или между центральной властью и местными объединениями. Именно тогда теория управления привнесла новый подход, который заключался в рассмотрении двух процессов или явлений не с точки зрения конфликта, а с точки зрения возможностей для взаимодействия. Данная теория рассматривала необходимость координировать усилия государственных структур, рынка и гражданского общества. Такой подход показал свою эффективность в вопросе урегулирования социальных и экономических проблем.

В 1989 году Всемирным банком был использован термин «кризис управления» в отношении событий, происходящих в Африке. Таким образом можно сделать вывод, что данный термин получил политологическое применение¹⁵⁹.

Комиссией по глобальному управлению было сформулировано определение термина «управление», согласно которому это «ряд подходов,

¹⁵⁹ Brautigam D. Governance and Economy: A Review. Policy Research Working Paper Series. No. 815. The World Bank, 1991. P. 48.

которые используются государственными и частными лицами и учреждениями для того, чтобы управлять общими делами»¹⁶⁰. Как уточняется, это процесс, в рамках которого непрерывно сталкиваются различные интересы и предпринимаются усилия для того, чтобы одни процессы не мешали другим.

Так, например, американский политолог Ф. Шмиттер интерпретирует управление как «подход, в рамках которого решение задач обязывает субъектов находить компромиссы при взаимодействии друг с другом, находить пути решения проблемы и реализовывать их»¹⁶¹. Б. Колер-Кох рассматривает управление в качестве процесса, который предполагает принятие конкретных решений, при котором учитываются пожелания гражданского общества, что позволяет реализовать наиболее эффективную политику, соответствующую социальным интересам¹⁶². Дж. Койман и М. Ван Влит отмечают, что управление представляет собой «результат вовлечения в функционирование общественно-политической системы всех сторон»¹⁶³. Японский исследователь Акиёси Хосино определяет управление как «множество подходов, при использовании которых общество и государство совместно работают над решением актуальных проблем»¹⁶⁴. Китайский ученый У Чжичэн рассматривает управление в качестве «процесса, в ходе которого государство и гражданские структуры управляют обществом с целью сохранения внутренней стабильности и удовлетворения общественных потребностей»¹⁶⁵.

¹⁶⁰ The Commission on Global Governance. *Our Global Neighbourhood*. Oxford: Oxford University Press, 1995. P. 47.

¹⁶¹ Schmitter P.C. *Participation in Governance Arrangements: Is There Any Reason to Expect It Will Achieve Sustainable and Innovative Policies in a Multilevel Context?* // *Participatory Governance: Political and Societal Implications* / ed. by J.R. Grote, B. Gbikpi. Opladen: Leske & Budrich, 2002. P. 64.

¹⁶² Kohler-Koch B., Eising R. (eds.). *The Transformation of Governance in the European Union*. London: Routledge, 1999. P. 14.

¹⁶³ Kooiman J. *Social-political Governance: Overview, Reflection and Design* // *Public Management Review*. 1999. No. 1. P.83.

¹⁶⁴ Акиеси Хосино (Akiyoshi Hoshino). *全球政治学 (Глобальная политология)*. Пекин: Издательство Синьхуа Пресс, 2000. С. 132.

¹⁶⁵ Юй Кепин (Yu Keping). *全球治理引论 (Введение в глобальное управление) // 马克思主义与现实 (Марксизм и реальность)*. 2002. № 1. С. 22.

Таким образом, можно определить ряд основных подходов, на основании которых выделяются различные типы управления:

1. Субъекты, реализующие управленческие решения могут принадлежать к различным сферам и уровням власти: правительственные структуры и другие государственные ведомства, а также различные организации или отдельные взятые индивиды. Это говорит о том, что в настоящее время государство больше не является единственным субъектом в вопросе реализации управленческих решений. Наоборот, власть должна тесно взаимодействовать с другими субъектами данного процесса для того, чтобы эффективно управлять государством.
2. Управление может реализовываться в различных формах: принудительная имплементация решений, которая сопровождается ограничительными мерами со стороны государственных органов, или компромиссный подход, в рамках которого стороны находят совместные пути решения без или иных вопросов.
3. Еще одним фактором, на основании которого выделяются различные типы управления является цель управления. Цель управления может заключаться в использовании властных ресурсов для того, чтобы руководить, регулировать и контролировать деятельность граждан¹⁶⁶. Конечной целью управления обществом или государством является создание условий для обеспечения стабильного развития и поддержания безопасности.

В XXI веке с учетом постоянно нарастающих темпов глобализации проблемы, с которыми сталкивается международное сотрудничество, также становятся глобальными и более комплексными, а управление перестает ограничиваться национальным уровнем. Современные проблемы не могут быть решены отдельно взятым государством, поэтому особую важность приобретает необходимость налаживания межгосударственного взаимодействия, которое

¹⁶⁶ У Чжичэн (Wu Zhicheng). 西方治理理论述评 (Комментарий к западной теории управления) // 教学与研究 (Преподавание и исследования). 2004. № 6. С. 63.

основано на компромиссах и обоюдном желании решить возникающие проблемы. Одновременно с тем, что проблемы стали характеризоваться своей глобальностью, состав субъектов, которые принимают участие в процессах управления, также стал расширяться: в один ряд с государственными учреждениями и правительственными структурами встали транснациональные корпорации (ТНК), СМИ, частные компании и прочее. Несмотря на широкий состав участников, управляющих глобальными процессами, государство в лице различных ведомств и органов остается ключевым актором.

К основным вопросам глобального управления можно отнести международную безопасность (вооруженные конфликты, незаконное распространение оружия, фактор ядерной войны), экологию, международную экономику (монетная политика, транспарентность международного экономического сотрудничества, распределение ресурсов), преступность, контроль над распространением наркотиков и др. Еще одним фактором, который оказывает влияние на изменение подходов к управлению, является цифровизация. С учетом данного фактора управление и регулирование Интернета также является одной из составляющих частей глобального управления.

На сегодняшний день количество активных пользователей Интернета в мире насчитывает более 5,5 млрд человек, что демонстрирует широкое распространение подключения к сети в мире, хотя уровень проникновения имеет различия в зависимости от региона мира. Стоит отметить, что постоянный рост количества интернет-пользователей обоснован активным развитием мобильной связи, сетей 3G, 4G и 5G, а также снижением стоимости услуг связи. Благодаря унифицированным стандартам и подходам Интернет можно рассматривать в качестве глобальной системы взаимосвязанных компьютерных сетей. Технической основой функционирования интернета

является работа протоколов TCP/IP и механизм адресами DNS, которые обеспечивают маршрутизацию и обмен данными между любыми узлами сети.

Интернет характеризуется не только технологической составляющей, но и социальной, что превращает его в социотехнический феномен: среда, в рамках которой пересекаются техническая инфраструктура и деятельность людей. Глобальная сеть включает в себя не только компьютерные технологии, но и пользовательские сообщества, а также большое количество источников информации. Таким образом результатом функционирования Интернета - технической составляющей, деятельности пользователей и появления огромных объемов информации - становится образование глобального киберпространства. Киберпространство - это еще одна сфера общественной жизни, в которой пользователи активно взаимодействуют, публикуют различного рода информацию, большинство СМИ также функционируют в сети Интернет, появляются новые форматы медиа и прочее. Таким образом, Интернет представляет собой сферу общественного взаимодействия, которая оказывает значительное влияние на политику, экономику и культуру и требует особого подхода в управлении.

Регулирование Интернета - это комплексный процесс, который требует от государства одновременно реализации тех задач, которые стоят перед соответствующими органами, и обеспечения свободы слова и свободы доступа граждан к информации¹⁶⁷. Таким образом, управление Интернетом, являясь составляющей жизни общества, имеет особую важность с точки зрения общегосударственного регулирования.

Одним из факторов, который осложняет процесс управления Интернетом, является широкий перечень субъектов, участвующих в функционировании этой системы. К субъектам, которые оказывают влияние на работу сети Интернет,

¹⁶⁷ Коршунов И.Л. Регулирование в интернете: защита личности или ограничение свободы // Известия Санкт-Петербургского государственного экономического университета. 2019. Вып. 4. С. 121.

можно отнести: компании-производители технического оборудования; компании, занимающиеся строительством всей необходимой инфраструктуры; специалисты, разрабатывающие программное обеспечение для бесперебойной работы глобальной сети; онлайн-платформы и социальные сети, а также компании, которые владеют данными сервисами; компании-провайдеры, которые отвечают за предоставление услуг связи; компании, занимающиеся онлайн-бизнесом; пользователи и др.

Активное развитие цифровых технологий и Интернета приводит к возникновению ряда положительных и отрицательных факторов. С одной стороны, благодаря развитию Интернета ускорилось экономическое развитие стран, повышение качества жизни граждан, а также углубилось взаимодействие стран и глобальные процессы стали более транспарентными. С другой стороны, появились такие проблемы, как хакерские атаки и необходимость обеспечения информационной безопасности, интеллектуальная собственность, необходимость контроля процессов в рамках цифровой экономики и др. В связи с чем следует отметить, для того, чтобы регулирование Интернета удовлетворяло потребности граждан всех государств мира и соответствовало задачам государственной национальной политики, особую важность приобретает необходимость создать единую глобальную систему по регулированию Интернета.

Вопрос формирования единого подхода в управлении Интернетом начал обсуждаться еще в конце 90-х годов XX века. Так, в 2003 году в рамках форума Всемирной встречи на высшем уровне по вопросам информационного общества (World Summit on the Information Society) в Женеве было предложено создать Работу группу по управлению Интернетом для дальнейшей работы над формулировкой концептуальных подходов к регулированию Интернета¹⁶⁸.

¹⁶⁸ План действий Всемирной встречи на высшем уровне по вопросам информационного общества [WSIS: Plan of Action] [Электронный ресурс] // Официальный сайт Международного союза электросвязи (International

Далее в 2005 году Рабочая группа Организации объединенных наций по вопросам регулирования Интернета выдвинула следующую интерпретацию термину «управление Интернетом»: «разработка и применение властями, частными компаниями и гражданами правил и механизмов функционирования Интернета при условии, что каждый субъект данного процесса будет полноценно выполнять необходимые функции»¹⁶⁹.

В 2013 году после того, как стало известно о том, что Соединенные Штаты организовали беспрецедентную слежку за лидерами более 30 государства, вопросы создания глобальной международной системы управления Интернетом стали обсуждаться интенсивнее¹⁷⁰. Генеральной ассамблеей ООН была принята резолюция «Право на неприкосновенность частной жизни в век технологий», рекомендовавшая всем правительствам «приложить усилия для создания открытой, справедливой и безопасности цифровой среды, функционирование которой будет основано на нормах международного права и Устава ООН»¹⁷¹.

Процесс регулирования Интернета осложняется тем, что он децентрализован и состоит из нескольких уровней. Операционную часть работы Интернета контролирует государство, а содержательная, связанная с распространением информационных потоков, зависит в большей степени от пользователей. Таким образом, в рамках регулирования Интернет-пространства трудно сформировать единый центр имплементации решений, а также единые унифицированные подходы.

Telecommunication Union, ITU). URL: <https://www.itu.int/net/wsis/docs/geneva/official/poa.html> (дата обращения: 22.03.2024).

¹⁶⁹ Bossey C.D. Report of the Working Group on Internet Governance [Электронный ресурс] // U.S. Department of State Archive. URL: <https://2001-2009.state.gov/e/eeb/rls/rpts/othr/49653.htm> (дата обращения: 27.03.2024).

¹⁷⁰ NSA spied on phones of 35 world leaders [Электронный ресурс] // Официальный сайт RT (Russia Today). URL: <http://rt.com/usa/nsa-monitored-world-leaders-692/> (дата обращения: 28.03.2024).

¹⁷¹ Резолюция Совета ООН по правам человека A/HRC/34/L.7/Rev.1 «Право на неприкосновенность личной жизни в цифровой век» [Электронный ресурс] // Официальный сайт Управления Верховного комиссара ООН по правам человека. URL: https://ap.ohchr.org/documents/R/HRC/d_res_dec/A_HRC_34_L7_rev1.pdf (дата обращения: 24.06.2024).

На сегодняшний день в мире практически отсутствуют государства, где на законодательном уровне не были бы приняты меры, которые ограничивают деятельность физических и юридических лиц в Интернете. Важно подчеркнуть, что управление Интернетом имеет стратегическую важность для государства, поэтому в зависимости от задач и целей, которые преследуют правительства в рамках реализации национальной политики, степень регулирования Интернета и применяемые меры будут меняться. В зависимости от того, каким образом реализуется регулирование Интернет-пространства, можно выделить три основных подхода: либеральный, авторитарный и авторитарно-тоталитарный¹⁷². Так, либеральный подход не подразумевает введение каких-либо ограничений в отношении деятельности субъектов в сети Интернет и участия государства в контроле контента по политической теме. Авторитарный подход рассматривает регулирование Интернета только как инструмент фильтрации материалов политического содержания, направленный на поддержание общественной стабильности и сохранения устойчивости действующей политической системы. Авторитарно-тоталитарный подход направлен на полный контроль Интернета, фильтрацию любых материалов, которые публикуются в информационном пространстве, а также на создание независимого, национального и закрытого Интернет-пространства. Следует отметить, что на практике правительствами стран ни один из вышеперечисленных подходов практически не применяется в чистом виде¹⁷³.

Одним из ярких примеров того, что подход к регулированию Интернета и политика государства в отношении данного вопроса многогранны и зависят от ряда факторов, являются США. Несмотря на то, что в Соединенных Штатах заявляется о либеральном подходе в вопросе регулирования Интернета,

¹⁷² Коршунов И.Л. Регулирование в интернете: защита личности или ограничение свободы // Известия Санкт-Петербургского государственного экономического университета. 2019. Вып. 4. С. 121.

¹⁷³ Малькевич А. Как регулируется интернет в разных странах мира [Электронный ресурс] // Центр прикладных исследований и программ. URL: <http://www.prisp.ru/opinion/1801-malkevich-o-regulirovanii-interneta-v-mire-1802> (дата обращения: 21.03.2024).

который основан на принципе свободы слова, в последнее время все чаще случаются инциденты, связанные с цензурой и блокировками аккаунтов в социальных сетях.

Так, в 2021 году, после беспорядков в здании Капитолия ряд социальных сетей и платформ подвергли блокировке аккаунты Дональда Трампа, сославшись на угрозы насильственных действия, распространения дезинформации, а также якобы причастности Трампа к данным событиям¹⁷⁴. Например, Twitter 9 января 2021 года навсегда заблокировал аккаунт Трампа, обосновав это тем, что в ответ на призыв платформы удалить три публикации, связанные со штурмом Капитолия, не было предпринято никаких действий со стороны Трампа. После этого аккаунт Трампа был заблокирован также и в Facebook. Основатель данной социальной сети пояснил, что аккаунт мог быть использован Трампом для того, чтобы инициировать протесты движения против избранного на тот момент президента США Джо Байдена, полномочия которого еще не вступили в силу¹⁷⁵. Кроме того, аккаунты, которые были связаны с Трампом, подверглись блокировке также на YouTube, Discord, Pinterest и других площадках. Ситуация, связанная с аккаунтами Дональда Трампа привела к бурным обсуждениям в американском обществе о том, насколько правомерно блокировать аккаунты пользователей и могут ли частные компании вмешиваться в процессы, связанные со свободой выражения мнения.

Другим ярким примером, демонстрирующим, что социальные сети в США регулируются с учетом интересов государства и не всегда в интересах граждан, это ситуация с блокировкой социальной сети TikTok на территории страны. В 2020 году в связи с ухудшением отношений между Вашингтоном и Пекином американские политики заговорили об угрозе, исходящей со стороны

¹⁷⁴ Трампа заблокировали в соцсетях. Законно ли это? [Электронный ресурс] // Официальный сайт РБК. URL: https://www.rbc.ru/technology_and_media/11/01/2021/5ffc13cb9a794777cf0cbb13 (дата обращения: 22.03.2024).

¹⁷⁵ Trump banned from Facebook indefinitely, CEO Mark Zuckerberg says [Электронный ресурс] // Официальный сайт газеты The Washington Post. URL: <https://www.washingtonpost.com/technology/2021/01/07/trump-twitter-ban/> (дата обращения: 24.03.2024).

социальной сети. Основные опасения, которые высказывались законодателями США, были связаны с безопасностью конфиденциальной информации пользователей, которая якобы могла быть передана китайским властям. Позже американские власти потребовали от китайской компании Bytedance, которая владеет TikTok, продать долю в социальной сети американским компаниям, угрожая заблокировать платформу на территории Соединенных Штатов.

Другим примером неоднозначного подхода властей при управлении интернет-пространством может послужить подход стран ЕС. Так, в Евросоюзе постоянно заявляют о свободе слова, возможности самовыражаться и отсутствии ограничений для граждан при получении информации. Несмотря на это в ряде стран Евросоюза активно запрещают деятельность СМИ, материалы которых приносят альтернативный взгляд на события, происходящие в мире и в регионе. Так, например со 2 марта 2022 года на территории всего Евросоюза на законодательном уровне запрещена деятельность международного телеканала RT и новостного агентства Sputnik¹⁷⁶. Как отмечалось в опубликованном властями ЕС заявлении, RT и Sputnik «играют важную роль в продвижении и поддержке военной агрессии против Украины, а также в дестабилизации соседних с ней стран».

Данные примеры иллюстрируют тот факт, что подход в регулировании Интернет-пространства в государствах характеризуется комплексностью и невозможностью применения унифицированных решений.

В последние годы процессы, происходящие в сфере регулирования Интернета, демонстрируют неготовность стран к совместному управлению глобальной сетью. Так, в 2022 году Госдепартамент США опубликовал «Декларацию о будущем Интернета», в которой заявлялось о необходимости

¹⁷⁶ ЕС запретил вещание телеканала RT и работу агентства Sputnik на территории Союза [Электронный ресурс] // Официальный сайт RT на русском. URL: <https://russian.rt.com/world/news/970290-es-zapret-veschanie-rt> (дата обращения: 26.03.2024).

рассмотреть проект управления глобальной сетью от 1994 года в качестве допустимого¹⁷⁷. Важно подчеркнуть, что согласно проекту 1994 года США должны были занять доминирующее положение в вопросе регулирования Интернета для удовлетворения своих национальных интересов. Публикация данной декларации привела к возникновению ситуации, когда глобальные игроки заняли противоположные позиции. С одной стороны, США и их партнеры подписали данную декларацию, подчеркнув тем самым свою готовность монополизировать процесс управления Интернетом и глобальным информационным пространством. С другой стороны, данную декларацию проигнорировали страны БРИКС, почти все страны африканского континента, большая часть стран Ближнего Востока и Азии.

Кроме того, летом 2022 года американским Советом по международным отношениям был опубликован документ «Противостояние реальности в цифровом пространстве»¹⁷⁸. В данном докладе подчеркивается, что Вашингтон стремился сформировать открытую глобальную сеть, но все усилия властей США не принесли ожидаемого результата, в связи с чем США не смогут повлиять на процессы фрагментации в рамках процесса управления Интернетом и ведения странами независимой политики по регулированию информационного пространства, основанной на национальных интересах. Авторы данного доклада рассматривают три основных аспекта, на основании которых может быть сформулирован подход по управлению Интернетом:

1. Общий подход союзнических государств по сохранению единой платформы по управлению Интернетом, основанной на тесной коммуникации всех сторон;

¹⁷⁷ A Declaration for the Future of the Internet [Электронный ресурс] // U.S. Department of State. URL: <https://www.state.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet.pdf> (дата обращения: 30.03.2024).

¹⁷⁸ Fick N., Miscik J., Segal A., Goldstein G.M. Confronting Reality in Cyberspace [Электронный ресурс] // Council on Foreign Relations. URL: https://www.cfr.org/report/confronting-reality-in-cyberspace/download/pdf/2022-07/CFR_TFR80_Cyberspace_Full_SinglePages_06212022_Final.pdf (дата обращения: 12.11.2024).

2. Политическое и экономическое давление на другие страны, а также проведение специальных операций в киберпространстве, направленных на борьбу с противниками;
3. Тесная связка между политикой цифровой борьбы и политикой национальной безопасности. В рамках данного аспекта предлагается активнее взаимодействовать с партнерами для укрепления превосходства в сфере технологий.

В 2023 году в США была опубликована «Национальная стратегия кибербезопасности». ¹⁷⁹ В документе подчеркивается, что Вашингтон приложит все усилия для того, чтобы функционирование Интернета было безвозмездным, открытым, равноправным, безопасным, основанным на уважении прав и свобод человека и праве свободы слова. Кроме того, в стратегии отмечается, что цифровые технологии должны быть инструментом для углубления сотрудничества людей во всем мире, а не инструментом, который используется для борьбы с другими странами и продвижения своих собственных интересов. На фоне подобных заявлений, зафиксированных в официальном документе, политика США по использованию Интернета в качестве средства достижения своих собственных целей, борьбы с противниками, принуждения отдельно взятых граждан и государств к определенным действиям, блокировки аккаунтов в социальных сетях является неоднозначной и противоречит тому подходу, о котором говорится в «Национальной стратегии кибербезопасности» США.

В этой связи особо актуальны концептуальные подходы Китая к регулированию Интернетом, согласно которым развитие Интернета должно проводиться совместными усилиями всего человечества, но при этом страны должны уважать суверенитет друг друга в цифровом пространстве.

¹⁷⁹ The National Cybersecurity Strategy [Электронный ресурс] // Официальный сайт Белого дома. URL: <https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/> (дата обращения: 29.03.2024).

В 2022 году Госсовет КНР опубликовал Белую книгу «Совместное создание сообщества единой судьбы в цифровом пространстве»¹⁸⁰. Данный подход к регулированию Интернет-пространства получил развитие еще в 2015 году, когда председатель КНР Си Цзиньпин в рамках Второй Всемирной конференции по управлению Интернетом озвучил пять ключевых тезисов, связанных с построением сообщества единой судьбы в цифровом пространстве¹⁸¹:

1. Способствовать ускорению строительства инфраструктуры во всем мире для широкого доступа к Интернет-технологиям;
2. Создать платформы для того, чтобы делиться и совместно пользоваться информацией в глобальной сети, а также обмениваться накопленными знаниями и опытом;
3. Создать условия для развития цифровой экономики в интересах всего международного сообщества;
4. Обеспечить информационную безопасность для ускоренного развития Интернет-технологий;
5. Направить усилия на создание системы регулирования Интернет-пространством, которая будет основана на равенстве и справедливом подходе.

Важно подчеркнуть, что в рамках процесса регионализации Интернета Россия и Китай могут объединить усилия для создания единой информационной экосистемы и единого подхода по регулированию глобальной сети, что позволит укрепить цифровой суверенитете обеих стран¹⁸².

¹⁸⁰ Jointly Build a Community with a Shared Future in Cyberspace [Электронный ресурс] // Информационное агентство «Синьхуа». URL: <https://english.news.cn/20221107/fba9dd1afb7e47f08c863d5d18afac55/c.html> (дата обращения: 01.04.2024).

¹⁸¹ Совместное создание сообщества единой судьбы в киберпространстве: о международном положении и дипломатической стратегии [Электронный ресурс] // China.org.cn. URL: http://russian.china.org.cn/china/China_Key_Words/2016-12/08/content_39874088.htm (дата обращения: 01.04.2024).

¹⁸² Карасев П.А. Управление интернетом – тенденции и перспективы // International Journal of Open Information Technologies. 2023. № 9. С. 62.

1.2. Понятие государственной информационной политики.

В странах с демократической системой управления информация определяется как ключевой элемент в рамках взаимодействия между государством и обществом. В настоящее время активное развитие технологий позволяет сократить расстояние между государством и представителями гражданского общества. В контексте принятия решений в политической сфере информация является ресурсом, обладание которым говорит о наличии политической воли. Активное развитие Интернет-технологий, появление социальных сетей и платформ, широкая доступность мобильных устройств, отсутствие границ в сети Интернет - всё это привело к необходимости адаптации государства и выработке качественно новых механизмов регулирования. Так активное развитие получило одно из самых молодых направлений государственного управления - информационная политика.

Важно подчеркнуть, что сам процесс реализации информационной политики не является новым явлением, он существовал и в XX веке. Но технологический прогресс, которого достигло современное общество, качественно меняет суть информационной политики. Термин «информационная политика» в зависимости от сферы применения характеризуется по-разному. Можно выделять такие виды информационной политики, как: корпоративная информационная политика, информационная политика СМИ, государственная информационная политика и т.д.

В сферах научных исследований и законодательной деятельности прочно закрепились понятия «государственная информационная политика» и «государственная политика информатизации». Важно подчеркнуть, что в настоящее время в науке есть несколько подходов к пониманию данных терминов.

Так, некоторые специалисты дают следующее определение: «направление государственной политики, которое связано с созданием и дальнейшим

распространением информации, направленной на удовлетворение государственных и общественных интересов и поддержание диалога между властью и гражданским обществом».

В настоящее время над изучением теоретических аспектов государственной информационной политики работают В.Д. Попов, А.В. Манойло, В.Ф. Ницевич, Ю.А. Нисневич, А.И. Кондратенко и др.

Термину «информационная политика» можно дать также и следующее определение: «деятельность, направленная на достижение своих интересов в обществе путем формирования, изменения, распространения различных видов информации»¹⁸³.

В.Д. Попов рассматривает государственную информационную политику как «сочетание политических, организационных, правовых, экономических инструментов государства, направленное на возможность обеспечить право населения на свободный доступ к информации и источникам ее распространения». Кроме того, он дал и следующее определение: «государственная информационная политика - это особая сфера жизни общества, которая связана с воспроизводством и распространением информации, которая создана для удовлетворения интересов государства и гражданского общества и направлена на поддержание взаимодействия между ними».

¹⁸³ Манойло А.В. Государственная информационная политика в особых условиях. М.: МИФИ, 2003. С. 123.

Изучением различных особенностей информационной политики занимались К.В. Маркелов¹⁸⁴, А.Н. Петрунин¹⁸⁵, В.В. Мистюков¹⁸⁶, М.Г. Дмитриев¹⁸⁷ и другие.

По мнению К.В. Маркелова, государственная информационная политика - это «способность государственных органов власти воздействовать на информационную сферу общества»¹⁸⁸.

В.В. Мистюков характеризует информационную политику как «деятельность государства по системному программированию общественного прогресса посредством применения различных цифровых технологий»¹⁸⁹.

Необходимо отметить, что реализация информационной политики должна включать не только процесс распространения информации среди населения, но и получение обратной связи от представителей гражданского общества. Подобными механизмами по получению обратной связи могут являться: проведение опросов общественного мнения, деятельность СМИ, активность населения в сети Интернет и т.д.

В.О. Богомолов рассматривает государственную информационную политику с точки зрения технологической составляющей и подчеркивает, что этот процесс связан с определением различных принципов и механизмов интеграции ИКТ в основные сферы общественной жизни¹⁹⁰.

¹⁸⁴ Маркелов К.В. Общественный идеал как объект информационной политики: дис. ... д-ра полит. наук: 10.01.10. М., 2006. С.228.

¹⁸⁵ Петрунин А.Н. Институт связей с общественностью Министерства обороны России в государственной информационной политике: дис. ... канд. полит. наук. М., 2011.С.76.

¹⁸⁶ Мистюков В.В. Информационная политика современной России в контексте формирующегося гражданского общества: дис. ... канд. полит. наук. М., 2012.С.87.

¹⁸⁷ Дмитриев М.Г. Региональная информационная политика как фактор формирования информационного пространства: дис. ... канд. полит. наук. М., 2004.С.112.

¹⁸⁸ Маркелов К.В. Общественный идеал как объект информационной политики: дис. ... д-ра полит. наук: 10.01.10. М., 2006. С. 7.

¹⁸⁹ Мистюков В.В. Информационная политика современной России в контексте формирующегося гражданского общества: дис. ... канд. полит. наук. М., 2012. С. 8.

¹⁹⁰ Богомолов В.О. Проблемы выработки и реализации информационной политики в современной России. М.: ИИП, ФГОУ РАКО АПК, 2008. С. 38.

Некоторые специалисты, такие как С.В. Коновченко¹⁹¹, А.Г. Киселев, В.Д. Попов¹⁹², связывают реализацию государственной информационной политики с деятельностью СМИ и подчеркивают, что основной проблемой государственной информационной политики будет являться проблема взаимодействия государства и прессы.

Как отмечается, если приравнивать деятельность средств массовой информации к «информационной власти», то государственная информационная политика - это способность политических субъектов оказывать воздействие на поведение граждан при помощи информации.

Специалист И.И. Пашкевич рассматривает термин «государственная политика информатизации» и определяет ее, как политико-правовая деятельность государства, которая ставит своей целью трансформацию информационной сферы общества¹⁹³. При том подчеркивается, что речь идет не только о распространении, но и об обработке и хранении информации.

Российский исследователь Ю.А. Гончаров отмечает, что государственная информационная политика - это «деятельность, направленная на реализацию прав и свобод граждан в информационной сфере»¹⁹⁴. В рамках изучения государственной информационной политики автор выделяет три ее основных направления: политика информатизации, политика, регулирующая деятельность СМИ, а также меры по обеспечению информационной безопасности.

Ю.А. Нисневич рассматривает государственную информационную политику, как «комплекс задач и целей в рамках национальных интересов в

¹⁹¹ Коновченко С.В., Киселев А.Г. Информационная политика в России: моногр. М.: Изд-во РАГС, 2004. С. 376–419, 476–492.

¹⁹² Информационная политика: учеб. / П.В. Беспалов [и др.]; под общ. ред. В.Д. Попова. М.: Изд-во РАГС, 2003. С. 383-384.

¹⁹³ Пашкевич И.И. Специфика и приоритеты государственной политики информатизации в Республике Беларусь как подсистемы политического процесса. Минск: Веды, 2001. С. 4.

¹⁹⁴ Гончаров Ю.А. Государственная информационная политика в условиях модернизации политической системы России: автореф. дис. ... канд. полит. наук: 23.00.02 / Ярослав. гос. ун-т им. П.Г. Демидова. Ярославль, 2004. С. 14.

сфере распространения информации¹⁹⁵. Это включает в себя разработку стратегий, тактик и решений в сфере государственного управления. Целью информационной политики является регулирование и совершенствование процессов цифровизации и распространения информации во всех областях жизни общества и государства.

Е.К. Алияров рассматривает государственную информационную политику как деятельность государства в информационной сфере, направленную на формирование интеллектуального потенциала государства.

Государственная информационная политика представляет собой регулирующую деятельность государственных органов, направленную на развитие информационной сферы общества, которая охватывает телекоммуникации, информационные системы и средства массовой информации»¹⁹⁶. Данное направление государственной политики включает в себя регулирование Интернета, телекоммуникационных систем и деятельности СМИ.

Таким образом, термину «государственная информационная политика» можно дать следующее определение: это возможность и способность государственных органов власти способствовать развитию информационно-технологической сферы жизнедеятельности общества, контролировать распространение информации и обеспечивать права и свободы граждан в сети Интернет.

В рамках рассмотрения государственной информационной политики можно определить три основных подхода к формулировке определения данного вида политики, которые связаны с объектом государственной информационной политики.

¹⁹⁵ Нисневич Ю.А. Системно-методологические основы государственной информационной политики // НТИ. Сер. 1, Орг. и методика информ. работы. 2001. № 3. С. 1–2.

¹⁹⁶ Алияров Е.К. Государственная информационная политика в Республике Казахстан в условиях глобальной информатизации: автореф. дис. ... д-ра полит. наук: 23.00.02 / Каз. нац. ун-т им. аль-Фараби. Алматы, 2006. С.15.

Согласно первому подходу, объектом государственной информационной политики является процесс информационного развития общества. Вторым подходом рассматривается основным объектом государственной информационной политики обеспечение прав и свобод человека в информационном пространстве и возможность свободного доступа к любым источникам информации. Третьим подходом делается основной акцент на технологическом развитии общества и создании соответствующей инфраструктуры, которая позволит обеспечить гражданам бесперебойный доступ к информации.

Последний подход, технологический, раскрыт В.Д. Поповым, рассматривающим развитие компонентов информационной среды (строительство инфраструктуры, доступность мобильной и компьютерной техники, широкая сеть мобильной связи и т.д.) как неотъемлемый процесс реализации государственной информационной политики.

Кроме того, информационную политику также можно разделить на внутреннюю и внешнюю. Такое деление основано на том, какая аудитория станет объектом действия органов, реализующих информационную политику. Так, в случае с внутренней информационной политикой речь идет о населении страны, а в рамках внешней информационной политики основным объектом являются другие страны и их граждане.

Важно отметить, что информационная политика государства в первую очередь направлена на деятельность субъектов в информационном пространстве или так называемом «медиапространстве», интернет-пространстве. Некоторые специалисты, как например Д. Белл, также рассматривают такое понятие, как информационное общество¹⁹⁷. В рамках изучения этой концепции основным фактором, влияющим на общественное развитие, являются достижения научно-

¹⁹⁷ Белл Д. Социальные рамки информационного общества // Новая технократическая волна на Западе. М.: Прогресс, 1986. С. 338.

технической революции, которые изменили формат производственных процессов, а также ускорили обработку и потребление информации¹⁹⁸.

Белл ввел понятие «постиндустриальное общество» в его современном значении, выделяя следующие особенности, присущие ему:

1. Теоретические знания стали определяющими в рамках развития общества;
2. Технологические достижения могут помочь в поиске более эффективных средств для решения проблем экономического, социального и даже политического характера;
3. Приоритет отдается производству услуг, а не товаров;
4. Автоматизация производства;
5. Увеличение числа людей, принадлежащих к среднему классу.

Государственная информационная политика может рассматриваться как деятельность государства по регулированию распространения информации в рамках механизма, основанного на нормативно-правовых актах. Можно отметить, что это включает два основных направления деятельности государственных органов власти: управление информационными потоками и создание и поддержание условий для технологического развития общества и его цифровизации.

К субъектам информационной политики можно отнести: государство, СМИ, транснациональные корпорации, институты гражданского общества, граждане, распространяющие информацию в социальных сетях и т.д.

Важно отметить, что несмотря на то, что главным актором в рамках имплементации информационной политики остается государство, некоторые специалисты, среди которых Г. Трессен, Е. Максвел, С. Вальграф, отмечают возрастающую роль СМИ в данной сфере. Как подчеркивается, в настоящее время средства массовой информации оказывают все больше внимания на

¹⁹⁸ Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования. М.: Academia, 1999. С.787.

политические процессы, в частности, на внутреннюю и внешнюю политику тех или иных государств.

Так, например в США существует несколько подходов к управлению потоками информации: освещение происходящего для международной аудитории и подача информации с точки зрения принципов внутривластного курса.

Американские СМИ активно участвуют в процессе принятия государством внешнеполитических решений, являясь не только наблюдателем, но участником этих процессов.

А. И. Кондратенко сформулировал несколько целей государственной информационной политики¹⁹⁹:

- Обеспечение широкого доступа к информации и формирование демократического информационного общества;
- Распространение общегосударственных идей и ценностей политического, экономического и культурного характера;
- Участие государственных средств массовой информации в процессе формирования общественного сознания;
- Создание механизмов взаимодействия между государством и гражданским обществом и обеспечение диалога между ними;
- Развитие аспектов становления информационного государства (Интернет вещей, информационные услуги, облачные хранилища, 5G и т.д.).

Итак, изучив различные подходы к определению целей государственной информационной политики, можно выделить следующие основные ее цели:

- Обеспечение гражданам непрерывного и полного доступа к информации;
- Создание и поддержание диалога между государством и гражданским обществом;

¹⁹⁹ Кондратенко А.И. Информационная политика: учебно-методическое пособие. Орел: Издательство ОРАГС, 2003. С. 12–13.

- Устранение угроз в рамках обеспечения информационной безопасности страны;
- Разработка нормативно-правовых документов, регулирующих деятельность государства и граждан в информационной сфере;
- Технологическое развитие общества.

Рассмотрев основные цели реализации государственной информационной политики, следует изучить ее функции.

Специалисты определяют такие функции государственной информационной политики, как:

- Содействие развитию личности, общества и государства;
- Участие в процессе регулирования отношений в обществе;
- Создание условий для того, чтобы упростить взаимодействие между государством и обществом;
- Формирование нормативно-правовой базы функционирования информационного пространства;
- Трансляция ценностей, приоритетов и стратегических установок, которые соответствуют национальным интересам государства;
- Противодействие внешним угрозам в целях обеспечения информационной безопасности;
- Обеспечение общественной и политической стабильности;
- Использование информационных ресурсов для повышения эффективности государственного управления и принятия политических решений.

Важно подчеркнуть, что государственная информационная политика направлена не только на решение вопросов, связанных с обеспечением гражданам доступа к информации или технологическим развитием общества. Данное направление государственной политики должно также реализовывать меры, направленные на обеспечение информационной безопасности всей страны в рамках национальной безопасности.

Термин «национальная безопасность» был введен в оборот президентом США Теодором Рузвельтом, который использовал его в письме конгрессу Соединенных Штатов. В 1994 году в ООН предложили новый подход к пониманию термина «безопасность» в XXI веке, согласно которому:

- Понятие «безопасность» применительно как к государству в целом, так и к его населению;
- Обеспечение безопасности определяется не только военным потенциалом государства, но и уровнем развития;
- Безопасность должна обеспечиваться на уровне личности, общества и государства.

Уровень безопасности государства определяется тем, насколько защищены интересы личности (соблюдение конституционных прав и свобод, улучшение жизненных условий, возможность для физического, интеллектуального и духовного развития), интересы общества (построение демократического общества и правового государства, стабильность в общественных настроениях) и интересы государства (нерушимость конституционного строя, сохранение суверенитета и территориальной целостности, создание условий для стабильного развития, экономический рост, установление взаимовыгодных связей с другими государствами, обеспечение внутренней стабильности и соблюдения законов).

В рамках изучения государственной информационной политики также необходимо рассмотреть такое понятие, как «суверенизация», так как в настоящее время общественные отношения можно охарактеризовать именно с помощью данного термина.

В конце XX - начале XXI вв. регулирование взаимодействия ключевых акторов на международной арене было основано на подходе, в рамках которого лежали принципы глобализации. В настоящее время данный подход постепенно сменяется переходом к национально-правовому регулированию действий

государства, в том числе и в контексте внешней политики. Подобные процессы обусловлены суверенизацией - желанием и реализацией государством возможности принимать самостоятельные решения в рамках внешней и внутренней политики в пределах своей территории.

При рассмотрении понятия «информационный суверенитет» следует отметить, что в настоящее время расширение мирового цифрового пространства приводит к тому, что взаимосвязь информации и государственных границ становится все более слабой. Так, М.М. Кучерявый подчеркивает, что транспарентность государственных границ для потоков информации может привести к ситуации, когда произойдет снижение уровня информационной безопасности общества и всего государства²⁰⁰. Кроме того, важно подчеркнуть, что в настоящее время одним из наиболее актуальных вопросов является необходимость государственного контроля и регулирующих механизмов в информационной среде.

В большей части исследовательских работ определение понятия «информационный суверенитет» связано с государственными механизмами по защите от различных угроз в цифровой сфере.

Л. Ю. Черняк отмечает, что информационный суверенитет включает в себя информационный суверенитет государства и информационный суверенитет личности²⁰¹.

Российский специалист А.В. Россошанский подчеркивает, что информационный суверенитет - это желание, способность и возможность конкретного политического субъекта создавать и распространять информацию, опираясь на личные политические цели и мотивы, и применять

²⁰⁰ Кучерявый М.М. Государственная политика информационного суверенитета России в условиях современного глобального мира // Управленческое консультирование. 2015. № 2. С. 12.

²⁰¹ Черняк Л.Ю. О понятии информационного суверенитета: теоретический и сравнительно-правовой аспекты // Сибирский юридический вестник. 2012. № 3(58). С. 119.

информационный ресурс как инструмент политического влияния²⁰². В свою очередь, Д.Г. Балувев считает, что в настоящее время отсутствует единая теория, в рамках которой было бы возможно определить критерии оценки роли информационного суверенитета государства в обеспечении национальной безопасности²⁰³.

М.М. Кучерявый определяет государственный информационный суверенитет как способность государства формировать и реализовывать независимую информационную политику как во внутреннем, так и в глобальном информационном пространстве²⁰⁴. То есть любое государство, обладающее суверенитетом в цифровом поле, вправе самостоятельно определять и контролировать механизмы распространения информации, ее цензуры и средств по обеспечению информационной безопасности.

Важно подчеркнуть, что информационный суверенитет включает в себя два основных компонента: технологическая и идеологическая базы. С точки зрения технологического развития государство должно создать развитую цифровую инфраструктуру, в том числе национальное программное обеспечение, национальные социальные сети и платформы, системы поиска информации, систему электронного банкинга и платёжные системы и т.д. Идеологическая составляющая информационного суверенитета сводится к наличию единого подхода к определению национальной информационной стратегии, популярности национальной массовой культуры, созданию механизмов пропаганды и соответствующей нормативно-правовой базе.

Информационный суверенитет обеспечивается в рамках реализации государственной информационной политики при помощи таких методов, как

²⁰² Россошанский А.В. Политический и информационный суверенитет в контексте процессов глобализации // Симбирский научный вестник. 2011. № 4(6). С. 185.

²⁰³ Балувев Д.Г. Влияние современных социальных медиа на информационный суверенитет России: основные подходы к исследованию // Государственное и муниципальное управление. Ученые записки СКАГС. 2015. № 3. С. 142.

²⁰⁴ Кучерявый М.М. Государственная политика информационного суверенитета России в условиях современного глобального мира // Управленческое консультирование. 2015. № 2. С. 12.

«информационный меч» и «информационный щит». И.С. Ашманов определяет «информационный щит» как средств, в том числе технических, идеологических, культурных, которые используются для противодействия распространению недостоверной информации, а также для недопущения утечек информации государственной важности. «Информационный меч» - это методы, применяемые субъектом для подрыва информационного суверенитета оппонента.

К основным инструментам обеспечения информационного суверенитета государства можно отнести:

1. Технологическая обеспеченность государства: наличие компьютерной базы, на основе которой будет реализовываться независимая информационная политика;
2. Наличие национального программного обеспечения и национальных систем безопасности данных. При отсутствии у государства возможности эффективно защищать стратегически важную информацию и данные граждан уровень информационного суверенитета крайне низок. В том случае, если государство с технологической точки зрения находится в зависимости от внешних поставок, то можно делать вывод о том, что информационная безопасность страны также находится в зависимости от других акторов;
3. Четко сформулированная национальная идеология, в рамках которой и будет отстаиваться информационный суверенитет страны. Как отмечает В.Н. Шилов, общая национальная идея направлена на определение целей существования данного государства, высокого уровня интеграционных процессов внутри общества, а также на мобилизацию населения²⁰⁵.
4. Создание национальных интернет-ресурсов: поисковые системы, социальные сети и платформы, широкая сеть официальных сайтов органов

²⁰⁵ Идеология для современной России: необходимость и предпосылки // Научные ведомости. 2015. Вып. 34. С. 187.

государственной власти и т.д. Развитая интернет-инфраструктура позволяет государству контролировать цифровое пространство, а национальные интернет-компании могут вступать в конкуренцию с иностранными игроками.

5. Нормативно-правовая база, которая будет являться основой для реализации государственной информационной политики²⁰⁶. В том случае, если информационное пространство недостаточно регулируется законодательством, высока вероятность совершения различных информационных преступлений как против государства, так и против личности (распространение недостоверной информации в Сети Интернет, кража личных данных, публикация в открытый доступ секретных государственных документов и т.д.). При этом, при отсутствии нормативно-правовой базы, государственные органы будут неспособны предотвращать совершение подобных преступлений.

Китайские исследователи рассматривают информационный суверенитет в качестве «новой формы государственного суверенитета, которая возникла в условиях информационной трансформации и глобализации». Так, например, Жэн Минъянь определяет информационный суверенитет как «право и способность государства защищать и управлять информацией, которая распространяется в пределах его юрисдикции»²⁰⁷. Китайский автор выделяет три основных элемента информационного суверенитета: информационный контроль, информационное управление и право на совместное использование информационных ресурсов. Так, под информационным контролем понимается «способность государства обеспечивать контроль над трансграничными потоками информации и обеспечивать защиту от утечки данных»; информационное управление - это «право государства регулировать

²⁰⁶ Слесарчук О.М. Современное состояние информационной сферы России // Изв. РГПУ им. А.И. Герцена. 2009. Вып. 93. С. 145.

²⁰⁷ Жэнь Минъянь (Ren Mingyan). 互联网背景下国家信息主权问题研究 (Исследование проблемы национального информационного суверенитета в условиях Интернета) // 河北法学 (Хэбэйская юридическая наука). 2007. Т. 25, № 6. С. 72.

информационно пространства посредством принятия законов, норм и правил»; право на совместное использование информационных ресурсов рассматривается как «участие государства в международном обмене данными им формировании глобальных правил управления цифровой средой на равноправной основе». В своих исследованиях Жэн Минъянь подчеркивает, что информационный суверенитет является основным фактором для реальной независимости государства. Отмечается, что потеря контроля над информационными потоками является причиной подрыва политического управления, экономической стабильности и культурной идентичности²⁰⁸.

Рассматривая исследования иностранных, в том числе китайских специалистов, можно сказать, что всеобъемлющего исследования по вопросу регулирования интернет-пространства в Китае пока не существует, что мешает как всестороннему пониманию этой темы, так и взаимодействию между различными работами. Авторы каждого исследования рассматривают разные аспекты цензуры, однако, общая картина остается неполной. Так, например, работы King Gary²⁰⁹²¹⁰, Liu Jun и Zhao Jingyi²¹¹, Qin Bei и Wu Yanhui²¹² дают представление об отдельных аспектах цензуры в китайском интернете.

Китайские исследователи уделяют отдельное внимание вопросам безопасности киберпространства КНР. Так, например, Тянь Лицзя и Ван Гуанхоу отмечают, что Китай, развивая кибербезопасность, сталкивается с давлением со стороны США и Запада, включая борьбу за влияние в сети, информационное доминирование и обвинения в «киберугрозах», что требует

²⁰⁸ Жэнь Минъянь (Ren Mingyan). 互联网背景下对国家主权的思考 (Размышления о государственном суверенитете в условиях Интернета) // 时代法学 (Право эпохи / Presentday Law Science). 2006. Т. 4, № 6. С. 107.

²⁰⁹ King G., Pan Jennifer, Roberts M.E. How Censorship in China Allows Government Criticism but Silences Collective Expression // American Political Science Review. 2013. Vol. 107, no. 2. P. 337.

²¹⁰ King G., Pan Jennifer, Roberts M.E. How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument // American Political Science Review. 2017. Vol. 111, no. 3. P. 493.

²¹¹ Liu Jun, Zhao Jingyi. More Than Plain Text: Censorship Deletion in the Chinese Social Media // Journal of the Association for Information Science and Technology. 2021. Vol. 72, no. 1. P. 25.

²¹² Qin Bei, Strömberg D., Wu Yanhui. Why Does China Allow Freer Social Media? Protests Versus Surveillance and Propaganda // Journal of Economic Perspectives. 2017. Vol. 31, no. 1. P. 132.

сбалансированной стратегии защиты национальных интересов²¹³. Другие специалисты анализируют международное соперничество государств за лидерство в киберпространстве. Так, в исследовании Лю Божана и Хуан Фэнчжи делается вывод, что киберпространство стало одной из сфер геополитического противостояния с моделью «одна сверхдержава (США) и несколько центров силы», где Китай, действуя в логике контроля, сдерживания и выборочного сотрудничества, стремится усилить свои позиции, что требует комплексных стратегий для баланса безопасности и глобального влияния²¹⁴.

Некоторые эксперты изучают особенности китайского подхода к регулированию Интернета: Ван Жун в своих работах подчеркивает, что китайское интернет-регулирование прошло несколько этапов развития, отличается комплексным многоуровневым подходом, и в будущем будет ориентировано на дальнейшую адаптацию к технологическим и геополитическим вызовам²¹⁵.

В России тему регулирования информационного пространства и обеспечения информационной безопасности рассматривали такие авторы, как Г. Ибрагимова²¹⁶, К. Антипов²¹⁷, А. Булавин²¹⁸ и другие. Следует отметить, что эти исследования дают общую характеристику системы кибербезопасности Китая, а источниковая база в основном состоит из работ американских ученых.

²¹³ Тянь Лицзя, Ван Гуанхоу (Tian Lijia, Wang Guanghou). 中国网络空间安全现状研究 (Исследование текущей ситуации с безопасностью киберпространства в Китае) // Journal of Shanxi Datong University. Social Science. 2015. [нужно уточнить: номер выпуска]. С. 12–14.

²¹⁴ Лю Борань, Хуан Фэнчжи (Liu Boran, Huang Fengzhi). 网络空间国际政治权力博弈问题探析 (Анализ международной политической игры за власть в киберпространстве) // 社会主义研究 (Исследования социализма). 2013. [нужно уточнить: номер выпуска]. С. 124.

²¹⁵ Ван Жун (Wang Rong). 中国互联网监管的历史发展、特征和重点趋势 (Историческое развитие, особенности и основные тенденции регулирования Интернета в Китае) // 北京通信法制研究会 (Пекинское общество исследований права в сфере коммуникаций). 2017. С. 58.

²¹⁶ Ибрагимова Г. Стратегия КНР в киберпространстве: вопросы управления интернетом и обеспечение информационной безопасности // Индекс безопасности. 2013. № 1(104). С. 174.

²¹⁷ Антипов К. Киберконфликт в китайско-американских отношениях и поиски диалога // Проблемы Дальнего Востока. 2013. № 6. С. 47.

²¹⁸ Булавин А.В. О подходах США и Китая к обеспечению кибербезопасности // Общество: политика, экономика и право. 2014. № 1. С. 43.

Как отмечают китайские исследователи Ян Чжи и Тянь Юехун, творческое единство и цельность китайской журналистики обусловлены ее историческими и духовно-культурными корнями²¹⁹.

Таким образом, государственная информационная политика представляет собой комплексную и многоуровневую деятельность государства, направленную на регулирование информационного пространства, развитие цифровой и коммуникационной инфраструктуры, обеспечение прав и свобод граждан, а также защиту национальных интересов в условиях нарастающих внешних и внутренних информационных угроз. Современное понимание данной политики выходит за рамки исключительно медиарегулирования и включает технологические, правовые, идеологические и управленческие компоненты, ключевым результатом взаимодействия которых становится укрепление информационного суверенитета и информационной безопасности государства.

1.3. Государственное регулирование в условиях цифровизации: анализ сущности и акторов

В настоящее время появление различных технологий кардинально меняет образ жизнедеятельности человечества: от структуры функционирования рынков до методов взаимодействия государственных органов власти с гражданами. В широком смысле слова цифровизация – это процесс повсеместного перехода от механических или аналоговых технологий к цифровым. Этот процесс начался в 80-х годах XX века и продолжается до сих пор. Важно отметить, что в иностранных исследованиях применяется три термина: digitization, digitalization, digital transformation.

Digitization можно дословно перевести как «оцифровка», т.е. процесс в рамках которого происходит преобразование объектов из физического формата

²¹⁹ Ян Чжи, Тянь Юехун Современная журналистика Китая: вечерняя пресса, региональное радио. – Минск, 2011. – С. 176.

в электронный. Примером оцифровки может послужить процесс сканирования различных документов, в результате которого текст, напечатанный на бумаге, переносится в цифровой формат. В результате оцифровки посредством преобразования в биты происходит кодирование аналоговой информации, которую можно обрабатывать и распространять при помощи компьютера. Нельзя не отметить, что оцифровка является важной составляющей процесса цифровизации, так как с помощью нее происходит процесс записи данных, которые являются основой цифровых технологий.

Digitalization переводится как цифровизация, но при этом важно подчеркнуть, что в отличие от процесса оцифровки в узком смысле слова цифровизация направлена на создание механизмов и инструментов обработки оцифрованных данных. Другими словами, в рамках процесса оцифровки (digitization) происходит перенос информации из аналогового формата в цифровой, а процесс цифровизации направлен на обработку и анализ цифровых данных.

Digital transformation – это термин, который можно дословно перевести как «цифровая трансформация». Данный процесс намного шире и комплекснее процесса цифровизации: его основная суть заключается в комплексной трансформации систем взаимодействия, управления, продаж с помощью различных цифровых инструментов.

Таким образом, можно сделать вывод о том, что процессы оцифровки, цифровизации и цифровой трансформации различаются по своей сущности, но являются взаимосвязанными. В процессе оцифровки происходит переход информации из аналогового формата в электронный, далее в рамках процесса цифровизации переведенные в цифровой формат данные можно анализировать и обрабатывать для того, чтобы оптимизировать те или иные процессы, а цифровая трансформация направлена на внедрение оптимизированных процессов и инструментов для достижения лучших результатов.

Среди китайских исследователей большое внимание уделяется термину «цифровая трансформация». Так, некоторые специалисты из КНР определяют цифровую трансформацию как процесс, который начинается с создания инфраструктуры цифровых технологий, цифровых продуктов и цифровых платформ и приводит к изменениям на различных уровнях: индивидуальном, организационном, промышленном и государственном²²⁰.

В большей степени в цифровых технологиях заинтересованы представители экономической сферы и деловых элит. Корпорации по всему миру предпринимают усилия по внедрению технологий, которые будут направлены на автоматическую оптимизацию процессов, сбор и анализ информации, централизованное управление всеми цепочками производства и т.д. Применение цифровых технологий помогает крупному бизнесу эффективно распределять ресурсы и сокращать время на принятие тех или иных операционных решений.

Современное общество вступило в эпоху цифровой экономики, и развитие новых информационных технологий, представленных искусственным интеллектом, большими данными, облачными хранилищами, побуждает предприятия постоянно рассматривать различные пути трансформации, чтобы получить новые конкурентные преимущества. Цифровые технологии оказывают разрушительное воздействие на традиционные методы производства ведения хозяйственной деятельности, в результате чего возникает ряд вопросов, таких как необходимость проведения трансформации и возможность ее успешного осуществления.

²²⁰ Цзэн Делинь, Цай Цзявэй, Оуян Таохуа (Zeng Delin, Cai Jiawei, Ouyang Taohua). 数字化转型研究: 整合框架与未来展望 (Исследование цифровой трансформации: интеграционная рамка и перспективы будущего) // 外国经济与管理 (Foreign Economics & Management). 2021. Т. 43, № 5. С. 68.

Процесс, обусловленный переходом к цифровым технологиям и происходящий в настоящее время, связан с феноменом «цифровой революции», результаты которой оказывают колоссальное влияние на окружающий нас мир и структурные составляющие его развития. В рамках цифровой революции происходит цифровизация производства, общества и политических систем. Эти изменения связаны с активным применением таких технологий, как: искусственный интеллект, Интернет вещей (Internet of Things), нейротехнологии, автоматический сбор и анализ большого массива данных (Big data), биометрические технологии, облачные сервисы и хранилища, умные устройства и объекты промышленности (smart everything), социальные сети и различные Интернет-платформы, сфера Интернет-услуг и государственных сервисов и т.д.

Активное развитие подобных технологий и их внедрение в повседневную жизнедеятельность человечества, а также в систему государственного управления создают ряд правовых проблем. Так, например, в связи с отсутствием международной нормативно-правовой базы возникают вопросы по обеспечению конфиденциальности персональных данных граждан, обеспечению легального статуса различных электронных сервисов, защиту серверов, которые используются в системах облачных хранилищ и системах больших данных, от хакерских атак и т.д. Таким образом, можно отметить, что распространение цифровых технологий меняет традиционные методы контроля и регулирования распространения информации и личных данных и требует принятия качественно новых нормативно-правовых решений, которые будут соответствовать современным реалиям общественных отношений в условиях цифровизации.

Применение современных информационных технологий характеризуется отсутствием нормативно-правовой базы, определяющей право государств на регулирование внутреннего информационного пространства и механизмы

контроля потоков информации, в частности в национальном сегменте сети Интернет. Данный вопрос является одним из самых актуальных, ведь государства развиваются и все чаще используют цифровые технологии в рамках государственного регулирования. Но важно отметить, что без общего подхода к определению таких понятий, как сетевое государство, кибербезопасность, Интернет-суверенитет, кибертерроризм и т.д., будет невозможно определить, где начинается и заканчивается суверенитет государства на принятие тех или иных решений в рамках государственного регулирования.

Несмотря на то, что цифровизация в большей степени относится к экономическим процессам, в последние годы этот термин стал чаще использоваться в отношении государства и государственной политики. Влияние процессов цифровизации на государственную политику было неизбежно: вследствие изменений в способах передачи информации и распространении цифровых технологий государство было вынуждено адаптироваться.

При рассмотрении объектов влияния процессов цифровизации в политической сфере следует выделить два основных понятия: это цифровизация политики и политика цифровизации. Цифровизация политики – это процесс внедрения цифровых технологий и инструментов в механизмы государственного администрирования, а также в процесс взаимодействия институтов власти и граждан. Политику цифровизации можно охарактеризовать как шаги государства по внедрению цифровых технологий в различные сферы общества, а также по регулированию данного процесса.

Влияние процессов цифровизации на политическую сферу жизнедеятельности общества требует тщательного изучения, так как данный предмет исследований формируется в настоящее время.

Как считается, первым исследователем, который в 1995 году использовал термин «цифровизация», является Николас Негропонтэ, специалист Массачусетского технологического института. В работе «Being Digital» автор

проводит аналогию между битами и атомами, которые рассматриваются в качестве мельчайших частиц цифрового и материального миров, соответственно. Как отмечает Негропонтэ, то, что состоит из атомов, можно будет создать и из битов²²¹.

Важно отметить, что процесс цифровизации политики различается в зависимости от конкретной страны или региона. Это связано с отличиями в темпах развития ИКТ, в технологическом развитии, в степени массовости использования мобильных телефонов и Интернета и т.д. В 2019-2020 гг. во время пандемии коронавирусной инфекции перед правительствами многих государств встала необходимость ускорить цифровизацию социальной, политической и экономической сфер жизни и использовать во взаимодействии с населением различные цифровые платформы, приложения и сервисы, на базе которых оказывались бы государственные услуги.

Рассматривая причины проникновения цифровых технологий в политику, можно выделить несколько основных: расширение площади покрытия сети Интернет, доступность мобильных телефонов, появление Интернет-СМИ, облачных технологий и технологий Big Data, стремительное развитие цифровых корпораций и т.д. Появление социальных сетей, видео-платформ, электронных СМИ привело к неконтролируемому распространению информации: каждый человек или организация, в том числе политическая, обладая доступом к Интернету, могла транслировать и доносить собственное мнение до общества, в том числе и недостоверную информацию.

Увеличение количества пользователей социальных сетей и Интернета, в целом, и публикация ими большого объема информации, в том числе и политического характера, подтолкнуло государства к созданию с помощью технологий Big Data механизмов контроля и цензуры публикуемой в сети

²²¹ Negroponte N. Being Digital. New York: Knopf, 1995. P. 173.

Интернет информации. При этом в рамках цифровизации политики начала расти роль цифровых корпораций, которые являлись лидерами в сфере Интернет-услуг, мобильной связи, цифровых технологий, социальных сетей и т.д. Именно подобные компании занимались созданием механизмов и алгоритмов, которые помогали бы фильтровать, цензурировать и контролировать информацию, публикуемую в различных социальных сетях и онлайн-площадках.

Примерами цифровизации политики могут послужить следующие примеры:

- электронное правительство, основная цель которого заключается в эффективном использовании цифровых технологий при взаимодействии с гражданами;
- система электронного голосования, обеспечивающая автоматизацию избирательного процесса и предотвращающая риски по фальсификации;
- цифровой суверенитет;

В последние годы формирование электронного правительства стало важной тенденцией развития систем государственного управления во многих странах. Это связано с решением задач по снижению затрат, повышению качества оказываемых государственных услуг, улучшению работы органов государственной власти. Важно отметить, что цель формирования электронного правительства заключается не только в преобразовании аналоговой информации в цифровой формат, публикации данной информации на государственных сайтах, автоматизация некоторых процессов. Функционирование электронного правительства также требует от властей переосмысления традиционных форматов работы государственных органов, создание инфраструктуры, которая позволит оказывать услуги для граждан в электронном формате, а также трансформация механизмов принятия решений и их реализации. В большинстве стран наиболее успешные примеры функционирования электронного

правительства начинались с реализации небольших проектов, на основе которых в дальнейшем и строилась вся инфраструктура²²².

Существуют различные подходы к определению термина электронное правительство. Некоторые специалисты определяют электронное правительство, как «способ предоставления правительственной информации и услуг посредством Интернета и других электронных платформ»²²³. Кроме того, даётся такое определение: «применение ИКТ для качественного изменения взаимодействия между государством, гражданами и бизнесом»²²⁴. Также электронное правительство рассматривается как «способ модернизации механизмов государственного управления»²²⁵.

В исследовании Бенчмаркинг электронного правительства: Глобальная перспектива, оценка прогресса стран-членов ООН», проведенном в 2001 году, « сформулированы пять основных этапов, позволяющие охарактеризовать степень развития электронного правительства²²⁶.

Этап 1. Присутствие правительственных органов в сети Интернет ограничивается наличием нескольких официальных сайтов. Информирование характеризуется ограниченностью и статичностью.

Этап 2. Количество официальных государственных сайтов увеличивается, а размещаемый на них контент регулярно обновляется. Информирование становится более динамичным.

²²² Alshehri M., Drew S. Implementation of E-Government: Advantages and Challenges // Proceedings of IASK E-ALT2010 Conference. 2010. P. 84.

²²³ Nwambuko, Temple C., Eyikorogha, Q., Chigozie, Joy N. (2025). Digital Governance and E-Government Transformation in Public Service Delivery in Nigeria. International Journal of Current Science Research and Review, 8(10), P. 5040.

²²⁴ West D.M. E-Government and the Transformation of Service Delivery and Citizen Attitudes // Public Administration Review. 2004. Vol. 64, no. 1. P. 18.

²²⁵ Barroca J., Kishnani P., Eggers W.D., Manstof J. Seven pivots for government's digital transformation: How COVID-19 proved the importance of "being" digital [Электронный ресурс] // Deloitte Insights. URL: <https://www.deloitte.com/us/en/insights/industry/government-public-sector-services/government-digital-transformation-strategy.html> (дата обращения: 12.04.2024)

²²⁶ United Nations Division for Public Economics and Public Administration. Benchmarking E-government: A Global Perspective - Assessing the Progress of the UN Member States, 2001.

Этап 3. В рамках функционирования правительственных интернет-ресурсов добавляется возможность интерактивного взаимодействия пользователей и чиновников путем написания писем по электронной почте.

Этап 4. Граждане могут получать государственные услуги через онлайн-сервисы правительства, а также проводить различные финансовые операции.

Этап 5. Правительство полностью интегрировало все оказываемые услуги посредством онлайн-сервисов.

В 2024 году в рамках институтов ООН было проведено исследование, под названием “Электронное правительство. Обзор 2024: Ускорение цифровой трансформации для устойчивого развития”²²⁷. Авторы пришли к следующим выводам, связанным с текущим состоянием развития и внедрения систем электронного правительства:

1. *Цифровизация стала не техническим, а управленческим вопросом.* Речь идет не о порталах как таковых, а о новой модели государственного управления — более быстрой, прозрачной, ориентированной на данные и потребности граждан.
2. *Цифровой разрыв сокращается, но не исчезает.* Несмотря на общий рост EGDI, Африка, Океания, наименее развитые страны, малые островные государства и страны без выхода к морю по-прежнему нуждаются в целевой поддержке.
3. *Наличие онлайн-сервиса не равно полноценной цифровой услуге.* Во многих странах сервисы представлены как информация или формы, но не как завершенная цифровая процедура.

²²⁷ Электронное правительство. Обзор 2024: Ускорение цифровой трансформации для устойчивого развития. [Электронный ресурс] // Официальный сайт ООН. Департамент ООН по экономическим и социальным вопросам. 205 p. URL: <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024> (дата обращения: 27.03.2025).

4. *Локальный уровень требует отдельного внимания.* Национальные цифровые стратегии не всегда доходят до муниципального уровня, а именно там гражданин чаще всего сталкивается с государственными услугами.

5. *Электронное участие пока остается ограниченным.* Страны создают каналы обратной связи, но далеко не всегда включают мнение граждан в реальные решения.

6. *ИИ может ускорить цифровое государство, но без регулирования усилит неравенство.* Особенно опасен разрыв между странами, которые уже имеют инфраструктуру, данные и кадры, и странами, которые только формируют цифровую базу.

7. *Главный приоритет на будущее — инклюзивная цифровая трансформация.* Государствам нужно развивать инфраструктуру, цифровую грамотность, законодательство, защиту данных, доступность услуг и участие граждан, чтобы цифровое правительство не стало преимуществом только для сильных экономик и крупных городов.

Переход к системам электронного правительства несет в себе преимущества как для развитых стран, так и для развивающихся стран²²⁸. Важно отметить, что непосредственно для населения стран польза введения систем электронного правительства будет заключаться в доступе к приложениям и сервисам, через которые можно будет получить государственные услуги. Так, через различные онлайн-сервисы граждане, представители бизнеса могут иметь доступ к различной государственной публичной информации в круглосуточном режиме, что повышает качество и ускоряет процесс оказания государственных услуг. Кроме того, наличие единой базы хранения государственной информации позволит своевременно обновлять и дополнить ее, что также окажет положительное влияние на взаимодействие

²²⁸ Ndou V. E-Government for Developing Countries: Opportunities and Challenges // The Electronic Journal of Information Systems in Developing Countries. 2004. Vol. 18, no. 1. P. 18.

государства и граждан. Внедрение электронного правительства также позволяет властям оптимизировать работы органов государственной власти, сократить издержки и повысить прозрачность функционирования.

К преимуществам электронного правительства также можно отнести следующие:

- повышение удовлетворенности граждан от оказанных государственных услуг;
- создание новых возможностей для бизнеса посредством упрощения процедуры оформления документации;
- укрепление доверия между правительственными структурами и гражданами;
- активное вовлечение граждан в политические процессы в стране.

В то же время внедрение систем электронного правительства сопровождается большим числом вызовов и трудностей, среди которых проблемы технического, организационного, общественного и финансового характера.

Функционирование механизмов электронного правительства связано с решением таких проблем технического характера, как отсутствие инфраструктуры, программного обеспечения, систем, позволяющих обеспечивать конфиденциальность обрабатываемой информации, а также высокая стоимость техники, в частности серверов и компьютеров.

К трудностям при попытке цифровизации систем государственного управления такж можно отнести отсутствие архитектуры ИКТ, то есть полноценно функционирующей системы из ИКТ-инфраструктуры, программного обеспечения, моделей взаимодействия этих систем и т.д. Необходимо отметить, что в данном вопросе важное место занимает и уровень цифровизации общества: уровень распространения Интернета по стране, Интернет-грамотность населения, возможность приобрести мобильные устройства. Для использования различных приложений и сервисов, которые оказывают госуслуги, необходимо иметь мобильной устройство или компьютер,

стабильное подключение к Интернету, а также навыки пользования данными ресурсами. Для решения данной проблемы правительства стран должны тесно взаимодействовать с ИТ-компаниями для строительства современной национальной ИТ-инфраструктуры²²⁹.

Еще одной проблемой на пути реализации проектов, связанных с электронным правительством, является необходимость защиты частной жизни и обеспечения конфиденциальности личной информации граждан, такой как паспортные данные, информация о доходах, регистрации, информация о владении недвижимостью и т.д.²³⁰ Эффективная система защиты личных данных граждан играет важную роль с точки зрения взаимодействия граждан и правительства: использование приложений электронного правительства требует передачи персональных данных граждан. При решении данного вопроса также важны и политические механизмы: необходимо принятие законов, обеспечивающих выполнение всех условий по сохранению конфиденциальности личных данных населения.

Внедрение электронного правительства потребует также и постепенной реформации бюрократической государственной системы и механизмов функционирования органов государственной власти²³¹.

Таким образом, цифровизация выступает системным фактором трансформации государственного регулирования, затрагивающим формы управления, механизмы взаимодействия власти и общества, а также распределение ролей между государством и цифровыми акторами. В условиях цифровой революции государство одновременно становится инициатором политики цифровизации и объектом цифровой трансформации, что требует выработки новых регуляторных подходов, развития электронного

²²⁹ Zhou Q., Ge E., Chen X., Xu X. Digital Government Leads to Economic Development: Mechanism and Evidence // Journal of Management Science China. 2023. Vol. 40. P. 56.

²³⁰ Hoti L., Dermaku K., Klaiqi S., Dermaku H. Protection and Exchange of Personal Data on the Web in the Registry of Civil Status // Emerging Science Journal. 2023. Vol. 7. P. 42.

²³¹ A. F. Realini, G2G E-Government: The Big Challenge for Europe. University of Zurich, 2004.

правительства и учета рисков, связанных с технологической зависимостью, защитой данных и обеспечением цифрового суверенитета.

* * *

Таким образом, по итогам анализа теоретических подходов и научной литературы выявлены ключевые особенности функционирования Интернет-пространства и реализации государственной информационной политики.

Установлено, что современное управление трансформируется в многоуровневую систему взаимодействия государства, частного сектора и гражданского общества. Интернет-пространство при этом обладает социотехнической природой и характеризуется децентрализованностью, что обуславливает сложность его регулирования и отсутствие единого центра принятия решений.

Показано, что государственная информационная политика выходит за рамки регулирования СМИ и приобретает комплексный характер, включая правовые, технологические и организационные механизмы воздействия. Важным элементом данной политики выступает информационный суверенитет, уровень которого определяется технологической независимостью государства и развитостью нормативно-правовой базы.

Выявлено усиление тенденции к суверенизации интернет-пространства на фоне отсутствия эффективных глобальных механизмов регулирования, а также противоречивый характер национальных моделей, сочетающих принципы открытости с ограничительными мерами.

Так, полученные результаты формируют основу для дальнейшего анализа механизмов государственного регулирования интернет-пространства.

Глава II. Идеологические и законодательные аспекты политики государственного регулирования интернет-пространства в КНР

2.1. Информационная политика КНР: теоретические и идеологические аспекты управления Интернетом

Начиная с 2010-х годов политический курс руководства КНР в отношении Интернет-пространства начал претерпевать изменения: наравне с модернизацией также укреплялся политико-правовой контроль. Так, в официальном дискурсе в Китае Интернет помимо «технологии» или «рынка услуг» определяется также как: новое измерение государственной власти, зона национальной безопасности, сфера конкурентной борьбы между международными факторами, пространство для распространения идеологического влияния.

Так, многими китайскими исследователями Интернет рассматривается в качестве составляющей части киберпространства. Под киберпространством понимается искусственно созданная, поддерживаемая информационно-коммуникационными технологиями виртуальная среда, в которой хранятся, обрабатываются и передаются различные данные, а также взаимодействуют люди, организации и государства. В КНР киберпространство относят к новому измерению государственного суверенитета («пятое пространство») наравне с сушей, морем, воздухом и космосом²³². Как отмечают в своей работе китайские исследователи Ху Ли, Ци Айминь, Хэ Цзиньхай распространение государственного суверенитета на киберпространство обусловлено глубоким проникновением информационной среды в политическую, экономическую, научно-техническую, культурную и военную сферы и его прямым влиянием на национальную безопасность государства. Китайские специалисты определяют суверенитет в информационном пространстве как «право и способность

²³² Ху Ли, Ци Айминь, Хэ Цзиньхай (Hu Li, Qi Aimin, He Jinhai). 国家网络空间主权战略 (学者建议稿) (Стратегия национального суверенитета в киберпространстве: проект научного предложения) // 河北法学 (Хэбэйская юридическая наука). 2018. Т. 36, № 6. С. 83.

государства самостоятельно управлять своей сетевой инфраструктурой, информационными ресурсами, процессами в сети, обеспечивать защиту интересов и прав граждан, а также предотвращать возникновение внешних угроз и их деструктивного воздействия на киберпространство страны.

Кроме того, в рамках теоретического обоснования регулирования Интернет-пространства в КНР выдвигается необходимость противостояния «сетевому гегемонизму» (网络霸权主义), который определяется как одна из ключевых угроз национальному суверенитету государств в эпоху цифровизации. «Сетевой гегемонизм» - это практика, в рамках которой отдельно взятые государства, обладающие технологическим и инфраструктурным преимуществом в цифровом пространстве, пользуются своим превосходством для того, чтобы вмешиваться во внутреннюю политику других стран и навязывать собственные ценности и ориентиры. В Китае некоторыми исследователями критикуется глобальный подход к пониманию границ киберпространства. Так, например» в своих исследованиях Ху Ли, Ци Айминь и Хэ Цзиньхай подчеркивают, что заявления о «надсуверенном» и «безграничном» характере Интернета направлены на оправдание сетевого гегемонизма, и выдвигают принцип «противодействия сетевому гегемонизму», который рассматривается как один из базовых принципов суверенитета в цифровом пространстве²³³. Согласно китайскому подходу, все страны обладают равными правами на суверенитет в киберпространстве.

Важно подчеркнуть, что защита цифрового суверенитета является одним из предварительных условий для достижения стратегической цели национального развития КНР: превращения в «кибердержаву» (网络强国).

²³³ Ху Ли, Ци Айминь, Хэ Цзиньхай (Hu Li, Qi Aimin, He Jinhai). 国家网络空间主权战略 (学者建议稿) (Стратегия национального суверенитета в киберпространстве: проект научного предложения) // 河北法学 (Хэбэйская юридическая наука). 2018. Т. 36, № 6. С. 87.

Впервые данный термин был использован председателем КНР Си Цзиньпином в феврале 2014 года в рамках первого заседания Центральной руководящей группы кибербезопасности и информатизации²³⁴. Китайские исследователи определяют, что превращение в кибердержаву означает не просто достижения высокого уровня развития Интернет-технологий, но и способность государства самостоятельно и стабильно управлять киберпространством, основанная на наличии национального суверенитета в цифровом пространстве²³⁵. Понятие «кибердержава» предусматривает сильную позицию государства в цифровом пространстве: технологическую, законодательную, идеологическую. Сетевая держава должна сформировать свою собственную технологическую базу, чтобы не зависеть от других стран, развивать инфраструктуру, построить комплексную систему обеспечения безопасности в киберпространстве. Стоит подчеркнуть, что одно из важнейших мест в концепции построения сильной сетевой державы занимает подход «управление интернетом на основе закона» (依法治网): цифровое пространство не должно существовать без координации со стороны государственных органов и соответствующей нормативно-правовой базы, регулирующей деятельность цифровых компаний и пользователей в интернете²³⁶. Также немаловажной составляющей рассматриваемой кондиции является идеологическое измерение понятия «кибердержава»: «сильная» интернет-держава должна уметь поддерживать «здоровую» онлайн-среду, управлять общественным мнением, продвигать «позитивную» ценностную повестку и противодействовать

²³⁴ 习近平: 把我国从网络大国建设成为网络强国 (Си Цзиньпин: превратить Китай из крупной интернет-страны в подлинную сетевую державу) [Электронный ресурс] // Официальный сайт агентства «Синьхуа». URL: http://www.xinhuanet.com/politics/2014-02/27/c_119538788.htm (дата обращения: 21.07.2024).

²³⁵ 徐 莉, 齐 艾 敏, 何 晋 海 (Hu Li, Qi Aimin, He Jinhai). 国家网络空间主权战略 (学者建议稿) (Стратегия национального суверенитета в киберпространстве: проект научного предложения) // 河北法学 (Хэбэйская юридическая наука). 2018. Т. 36, № 6. С. 84.

²³⁶ 张 慧 (Zhang Hui). 新时代中国共产党网络战略论析——学习习近平总书记关于网络战略讲话的精神 (Обсуждение и анализ сетевой стратегии Коммунистической партии Китая в новую эпоху: изучение духа речей генерального секретаря Си Цзиньпина о сетевой стратегии) // 新闻传播 (Новостные коммуникации / News Dissemination). 2019. № 7. С. 142.

дезинформации для обеспечения политической стабильности и безопасности общества.

Кроме того, некоторые китайские специалисты в рамках изучения киберпространства выделяют различные типы власти, свойственные только власти в цифровом пространстве. Так, например, Лю Чуаньин в своих исследованиях выделяет 4 основные формы проявления власти в сети²³⁷:

1. Принудительная сетевая власть (强制性网络权). Власть основанная на наступательных и оборонных действиях в цифровой среде. Автор приводит в качестве примера атаку Stuxnet по Ирану. Как подчеркивается, данный тип власти является источник эскалаций и неправомерных действий, так как отсутствуют общие нормы атрибуции для подобных действий.
2. Институциональная сетевая власть (制度性网络权). Власть, основанная на управлении Интернет-пространством через формальные и неформальные институты и ведомства. Примерно может послужить ситуация, когда в 2001 году перед войной в Ираке Соединенные Штаты Америки посодействовали прекращению обслуживания домена «.iq», что привело к серьезным сбоям в работе иракских сайтов.
3. Структурная сетевая власть (结构性网络权). Автор рассматривает источником данного типа власти отношения между государственными структурами и негосударственными акторами, к которым можно отнести различные компании, НПО, академические центры и другое.
4. Интерпретативная сетевая власть (解释性网络权). Власть, основанная на возможности давать объяснения и интерпретации политическим событиям и

²³⁷ Лю Чуаньин (Lu Chuanying). 主权概念的演进及其在网络时代面临的挑战 (Эволюция концепции суверенитета и вызовы, с которыми она сталкивается в эпоху Интернета) // 国际关系研究 (Исследования международных отношений). 2014. № 1. С. 77.

идеологиям. Вне цифрового пространства данную функцию реализует государство, но с появлением Интернета все негосударственные акторы получили возможность делиться своей интерпретацией происходящих событий. Как подчеркивает автор, политические субъекты будут стремиться получить и удерживать именно данный тип власти, так как «борьба в цифровом пространстве идёт не просто за инфраструктуру, а за способность задавать рамку смысла в политике».

Киберсуверенитет рассматривается в КНР как базовый принцип международного подхода к управлению Интернет-пространством²³⁸. В рамках этого подхода подчеркивается, что любое государство обладает правом самостоятельного регулирования цифрового пространства внутри своих границ, а также обеспечения сетевой безопасности и социальной стабильности. В Китае выступают за многосторонний подход к управлению Интернетом под эгидой ООН.

Современная внешнеполитическая деятельность КНР основана на нерушимости границ, отстаивании собственного и уважении к суверенитету других государств, а также на невмешательстве во внутренние процессы в других странах. Эти принципы направлены на отстаивание национальных интересов: безопасность внешняя и внутренняя, территориальная целостность, стабильность экономического развития, а также благоприятная ситуация на международной арене. Стоит подчеркнуть, что Пекин при реализации политики регулирования Интернет-пространства и цифровой дипломатии исходит из тех же принципов. После того, как неприкосновенность государственной границы стала одной из центральных проблем в вопросе контроля цифрового пространства, Китай начал предпринимать попытки к определению того, что

²³⁸ Сюн Гуанцин, Ван Жуй (Xiong Guangqing, Wang Rui). 全球互联网治理中的网络主权：历史演进、国际争议和中国立场 (Сетевой суверенитет в глобальном управлении Интернетом: историческая эволюция, международные споры и позиция Китая) // 学习与探索 (Обучение и исследования). 2024. № 4. С. 28.

такое киберсуверенитет и как он определяет права и обязанности государств в рамках глобального управления Интернетом²³⁹.

Руководство КНР исходит из того, что цифровая безопасность является важной составляющей национальной безопасности, поэтому отстаивание киберсуверенитета расстраивается китайскими властями как залог обеспечения внутренней стабильности страны, а также защиты от внешних угроз. Все идеологические разработки и институциональные реформы по управлению Интернет-пространством, которые прирабатывались и продолжают реализовываться в Китае, обоснованы недовольством Пекина сложившимся киберпорядком и гегемонией США в цифровом пространстве²⁴⁰.

Впервые термин «киберсуверенитет» или так называемый «сетевой суверенитет» (网络主权) был применен в пятой части Белой книги «Состояние Интернета в Китае», которая была опубликована Госсоветом КНР в 2010 году²⁴¹. В соответствии с содержанием данного документа, Китай рассматривает Интернет в качестве части национальной инфраструктуры и заявляет о своем суверенном праве управлять им в рамках собственной юрисдикции. Появление понятия «киберсуверенитет» и определение права китайских властей на его отстаивание стало частью развития концепции «информационного суверенитета» (信息主权), согласно которой государство обладает правом на защиту и контроль любой информации в пределах своей территории²⁴².

²³⁹ Янькова А.Д. Архитектура концепции киберсуверенитета КНР (по материалам докладов Всемирной интернет-конференции «Киберсуверенитет: теория и практика») // Проблемы Дальнего Востока. 2023. № 4. С. 1–14.

²⁴⁰ Хань Жуйся, Сюй Цзянь (Han Ruixia, Xu Jian). 网络主权视域下当前互联网治理的主要问题、成因及监管对策 (Основные проблемы, причины и регулятивные контрмеры текущего управления Интернетом с точки зрения киберсуверенитета) // 南京邮电大学学报(社会科学版) (Вестник Нанкинского университета почты и телекоммуникаций. Серия: Социальные науки). 2020. № 22. С. 42.

²⁴¹ «中国互联网状况» 白皮书 (Белая книга «Состояние Интернета в Китае») [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/zhengce/2010-06/08/content_2615774.htm (дата обращения: 10.08.2025).

²⁴² Ян Цзэвэй (Yang Zewei). 国际法析论: 第3版 (Анализ международного права: 3-е изд.). Пекин: Издательство Китайского народного университета, 2012. С. 247.

19 ноября 2014 года Генеральный секретарь КНР Си Цзиньпин, выступая на открытии первой Всемирной интернет-конференции, впервые официально заявил о китайской концепции киберсуверенитета. Китайский лидер отметил, что тенденции развития цифрового пространства приводят к появлению новых угроз и вызовов для государственного суверенитета и национальной безопасности, обеспечение которой теперь становится невозможным без сетевой безопасности²⁴³.

В 2015 году прошла вторая Всемирная Интернет-конференция, в рамках которой была подчеркнута важность кибербезопасности на фоне терактов в Париже в 2015 году. Во время данного мероприятия председатель КНР Си Цзиньпин определил киберсуверенитет как «принцип суверенного равенства, который применяется в цифровом пространстве и подразумевает право государств на независимый подход в управлении Интернетом. Как подчеркнул китайский лидер, странам следует уважать плюрализм подходов управления Интернет-пространством, в том числе формат с участием государства. Согласно обоснованию китайской стороны киберсуверенитет напрямую связан с национальной безопасностью, а цифровое пространство является «пятой границей» (新疆域) наряду с сухопутными, морскими, воздушными и космическими границами²⁴⁴.

Кроме того, в рамках второй Всемирной Интернет-конференции Си Цзиньпин выдвинул «пять предложений» и «четыре принципа» для формирования механизмов, позволяющих эффективно и на равноправной основе управлять Интернетом²⁴⁵. К основным принципам управления Интернет-

²⁴³ Си Цзиньпин (Xi Jinping). 让互联网发展成果惠及 13 亿中国人民 (Пусть плоды развития Интернета принесут пользу 1,3 млрд китайцев) [Электронный ресурс] // Официальный новостной сайт Всемирной интернет-конференции 2014. URL: http://www.cac.gov.cn/2014-11/19/c_1113314465.htm (дата обращения: 10.08.2025).

²⁴⁴ Лю Хань, Е Кайжу (Liu Han, Ye Kaigu). 网络主权的分层法律形态 (Иерархическая правовая форма киберсуверенитета) // 华东政法大学学报 (Вестник Восточно-Китайского университета политологии и права). 2020. № 4. С. 80.

²⁴⁵ Remarks by H.E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference (Выступление Си Цзиньпина на церемонии открытия Второй Всемирной интернет-

пространством председатель КНР отнес: уважение киберсуверенитета, поддержание мира и безопасности, содействие открытости и сотрудничеству и формирование надлежащего порядка. Киберсуверенитету и необходимости его защиты было уделено отдельное внимание. Си Цзиньпин подчеркнул, что принцип суверенного равенства, сформулированный в Уставе ООН охватывает все сферы международных отношений, в том числе цифровое пространство.

Китайская сторона неоднократно подчеркивала, что страны должны уважать право государств самостоятельно определять направление своего развития в киберпространстве, модель и подходы к регулированию Интернета, а также принимать участие в глобальном управлении Интернет-пространством, исходя из принципа равноправия. В КНР рассматривают киберсуверенитет как один из важнейших факторов устойчивого развития государств и отмечают, что страны не должны стремиться к гегемонии в цифровом пространстве, а также осуществлять вмешательство во внутренние дела других суверенных государств в киберпространстве.

Концепция киберсуверенитета последовательно развивалась китайскими властями и исследователями, начиная с 2015 года. Важными вехами в рамках систематизации подходов к обеспечению кибербезопасности стали шестая, седьмая и восьмая Всемирные Интернет-конференции 2019, 2020 и 2021 года. Кроме вопроса формирования теоретической и идеологической базы понятия «киберсуверенитет» внимание также было уделено построению «сообщества единой судьбы человечества в цифровом пространстве».

В ноябре 2022 года в КНР была опубликована Белая книга «Совместное построение сообщества единой судьбы в киберпространстве», которая формулирует подход Китая к совместному управлению Интернет-пространством, а также закрепляет концепцию «Сообщества единой судьбы в

конференции) [Электронный ресурс] // Официальный сайт Министерства иностранных дел КНР. URL: https://www.mfa.gov.cn/eng/xw/zyjh/202405/t20240530_11341037.html (дата обращения: 11.08.2025).

киберпространстве»²⁴⁶. Данный документ формирует концептуальную рамку, которая рассматривает интернет в качестве пространства, в котором государства и их общество «связаны единой сетью», а значит то, как развивается цифровое пространство, какие правила его регулируют, как обеспечивается безопасность, не может решаться странами в одностороннем порядке. Концепция «Сообщества единой судьбы в киберпространстве» подчеркивает, что взаимосвязанность и взаимозависимость стран создают условия для совместного решения проблем, возникающих в рамках управления цифровым пространством, а также совместного распределения выгод - в противном случае цифровизация усилит неравенство и создаст новые риски и угрозы безопасности стран в Интернете.

Рассматриваемая концепция напрямую связана с более широкой идеей о построении «сообщества единой судьбы человечества», но основной акцент в ней сделан именно на роль киберпространства как особой среды, в которой границы являются проницаемыми, а действия акторов и их последствия могут иметь транснациональный характер. В связи с этим в КНР предлагают рассматривать «сообщество единой судьбы в киберпространстве» как обязательство стран находить общий подход в формулировании правил сосуществования в цифровом пространстве, сотрудничать на основе взаимного уважения, не использовать технологические достижения в качестве инструмента политического давления.

В Белой книге «Совместное построение сообщества единой судьбы в киберпространстве» видение китайских властей о том, каким должна быть

²⁴⁶ Jointly Build a Community with a Shared Future in Cyberspace: White Paper (Белая книга «Совместное формирование сообщества единой судьбы в киберпространстве») [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://english.www.gov.cn/archive/whitepaper/202211/07/content_WS636894aac6d0a757729e2973.html (дата обращения: 02.09.2025).

единая судьба в цифровом пространстве раскрывается через идею о «четырех сообществах»:

1. Сообщество развития. Интернет и технологические достижения являются эффективным инструментом роста и модернизации. Как подчеркивается, рост должен быть совместным: технологии и их использование не должны приводить к увеличению разрыва между государствами, а, наоборот, должны обеспечивать равный доступ к инфраструктуре и знаниям.
2. Сообщество безопасности. В связи с появлением различных угроз нового формата в цифровом пространстве, обеспечение безопасности невозможно отдельными усилиями государств, это должна быть совместная работа. В китайской концепции под «единой судьбой» подразумевается, что уязвимость в вопросе обеспечения информационной безопасности одной страны может стать угрозой для всех участников сети, в связи с чем необходим координированный подход в борьбе с киберпреступностью и кибертерроризмом.
3. Сообщество ответственности. Для эффективного и справедливого управления Интернет-пространством страны должны исходить из единого подхода о том, кто формирует нормы и правила поведения в цифровом пространстве, как предотвращать фрагментацию в сети, как обеспечивать легитимность принимаемых решений. Управление Интернетом должно иметь многосторонний характер и должно быть основано на принципе общей ответственности за принимаемые решения.
4. Сообщество интересов. Цифровое развитие и технологические достижения приносят социально-экономические выгоды, которые не могут принадлежать узкому кругу стран или организаций. Концепция «единой судьбы в цифровом пространстве» подразумевает обязанность стран создавать условия для того, чтобы технологические достижения становились более универсальными и доступными для всех.

В документе отмечается, что двигаться к общему развитию Интернета и его эффективному использованию можно только через диалог и практическое сотрудничество, потому что общий характер сети делает и риски, и возможности по-настоящему общими.

Таким образом, основополагающая концепция киберсуверенитета КНР и концепция построения «сообщества единой судьбы человечества в киберпространстве» формируют идеологическую базу регулирования Интернет-пространства. С одной стороны, в КНР последовательно отстаивают право страны на независимость в вопросе управления национального сегмента сети Интернет, которое основано на принципе суверенного равенства государства и невмешательства во внутренние дела других стран. С другой стороны, подход, основанный на определении «единой судьбы человечества» в цифровом пространстве и на формировании «четырех сообществ», позволяет говорить об отсутствии у КНР желания изолироваться в вопросе регулирования интернета: суверенитет трактуется не как отказ от глобальности, а как необходимое условие равноправного участия в выработке правил и совместного распределения выгод цифровизации.

2.2. Законодательные основания регулирования Интернет-пространства в КНР

Как отмечалось, реализация информационной политики Китайской Народной Республики основывается на обеспечении информационной безопасности страны, создания условий, при которых вмешательство во внутреннюю ситуацию на территории Китая будет невозможным, и превращение Китая в сетевую державу. Угрозы информационной безопасности представляют опасность для всех сфер государственной деятельности: политической, экономической и социальной.

Самыми важными аспектами информационной безопасности являются оригинальность информации, конфиденциальность данных, целостность, проверяемость и управляемость²⁴⁷.

Так, например, Национальный информационный консультативный комитет Китайской Народной Республики рассматривает информационную безопасность, как основное условие обеспечения национальной безопасности и аспект, позволяющий обеспечить рациональное применение цифровых технологий, а также поддерживать социальную стабильность и необходимый уровень идеологического развития²⁴⁸.

Необходимо подчеркнуть, что на территории КНР и за ее пределами важной частью информационной безопасности является защита от киберугроз, таких как хакерство, вывод серверов из строя, хищение и шпионаж данных государственного значения и информационное противоборство. Кроме того, существует проблема информационного воздействия и вмешательства во внутренние дела государства с помощью информационно-коммуникационных технологий. Развитие новейших технологий, таких как искусственный интеллект, блокчейн, 5G, создает новые угрозы безопасности государственной инфраструктуры, частной жизни граждан и социальной стабильности. Среди этих угроз можно выделить высокий риск утечки данных, кибератаки и связанные с ними интеллектуальные преступления.

²⁴⁷ 2017 年中国信息安全行业发展现状及未来发展趋势分析[图] (Анализ состояния развития и будущих тенденций развития индустрии информационной безопасности Китая в 2017 г.) [Электронный ресурс] // Официальный сайт производственной информационной сети КНР. URL: <http://www.chyxx.com/industry/201708/549537.html> (дата обращения: 05.05.2024).

²⁴⁸ 江平:信息化与法治化建设 (Цзян Пин: информатизация и построение верховенства права) [Электронный ресурс] // Официальный сайт Национального информационного консультативного комитета КНР. URL: <http://www.acsi.gov.cn/content.aspx?newsId=1152&TId=171> (дата обращения: 05.05.2024).

Согласно китайским исследованиям²⁴⁹, источники угроз информационной безопасности можно сгруппировать по трем основным направлениям:

1. Риск технической безопасности: слабый уровень защищённости информационных сетей и систем и нарушение конфиденциальности. Плохая защищённость информационных сетей связана с рисками для Интернета и телекоммуникационных систем на территории КНР. Здесь важно отметить, что речь идет не только об информации частного характера, но и о государственных данных и государственной инфраструктуре, которая подвержена влиянию угроз информационного характера. Речь идет об авиационных и железнодорожных узлах, транспортной системе, правительственных ресурсах, банках, электричестве, нефтяной сфере и т.д.
2. Атаки, совершаемые с помощью вредоносного ПО, представляют самую большую угрозу информационной безопасности. Атаки хакеров, которые становятся все более продуманными, опасны как для физических лиц, так и для различных государственных аппаратных систем. Подобные хакерские действия можно разделить на активные (направленные на вмешательство во внутренние дела государства, контроль над информацией и распространение недостоверных данных для создания нестабильности в обществе) и пассивные (направленные на получение и хищение данных).
3. Недостаточно развитая система обеспечения информационной безопасности. Как отмечают некоторые специалисты, во многих странах механизмы по обеспечению информационной безопасности не эффективны в связи с тем, что исследованиям в этой сфере не уделялось достаточного внимания.

Политическое руководство КНР уже на протяжении более 20 лет активно занимается проблемой информационной безопасности. Так, еще в 2003 г.

²⁴⁹ 深度解读:威胁网络安全的源头是什么?如何有效应对复杂的网络环境? (Источники угроз информационной безопасности: как эффективно противостоять сложной интернет-среде?) [Электронный ресурс] // Baidu.com. URL: <https://baijiahao.baidu.com/s?id=1609675674334215917&wfr=spider&for=pc> (дата обращения: 05.05.2024).

Национальная координационная группа по кибербезопасности и информационной безопасности КНР опубликовала первую стратегию, определяющую политику китайских властей в этой сфере²⁵⁰. В соответствии с информацией Госсовета о продвижении развития информатизации и обеспечении информационной безопасности, формирование стратегических концепций в области кибербезопасности началось в 2012 г.²⁵¹. В 2016 г. ЦК КПК опубликовал «План национальной стратегии инновационного развития», в котором отмечалось, что развитие технологической базы для сетевой безопасности поможет обеспечить защиту для экономических трансформаций в КНР, модернизации, а также поддерживать сетевую безопасность страны в целом²⁵².

Для полного понимания истории становления государственной информационной политики КНР была проведен анализ основных документов, определяющих нормативно-законодательную базу действий китайского правительства в информационном поле.

В 1994 г. Государственным советом Китая был опубликован документ под названием «Правила регулирования, направленные на обеспечение безопасности компьютерных и информационных систем»²⁵³. Данный документ дал возможность Министерству государственной безопасности контролировать

²⁵⁰ 2003 年计算机网络与信息安全发展概况 (Обзор развития компьютерных сетей и информационной безопасности в 2003 г.) [Электронный ресурс] // China Radio International (CRI) Online. URL: <http://news.cri.cn/gb/3821/2004/08/26/148@280479.htm> (дата обращения: 05.05.2024).

²⁵¹ 国务院关于大力推进信息化发展和切实保障信息安全的若干意见 (Мнение Государственного совета КНР о форсированном продвижении развития информатизации и реальном обеспечении информационной безопасности) [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: http://www.gov.cn/zwzgk/2012-07/17/content_2184979.htm (дата обращения: 05.05.2024).

²⁵² 中共中央 国务院印发《国家创新驱动发展战略纲要》 (ЦК КПК и Государственный совет КНР опубликовали «План национальной стратегии инновационного развития») [Электронный ресурс] // Официальный сайт Государственного комитета по развитию и реформам КНР. URL: <https://www.ndrc.gov.cn/fggz/fzzlgh/gjfgzh/200709/P020191029595686994247.pdf> (дата обращения: 05.05.2024).

²⁵³ 计算机信息系统安全管理制度 (Правила регулирования, обеспечивающие безопасность компьютерных и информационных систем) [Электронный ресурс] // Baidu Wenku. URL: <https://wenku.baidu.com/view/8814c60716fc700abb68fc31.html> (дата обращения: 05.05.2024).

интернет-трафик: ведомство было наделено такими полномочиями, как контроль и инспекции информационного пространства в целях обеспечения национальной информационной безопасности, а также расследование и предотвращение преступной деятельности в сфере цифровых технологий. В результате, Министерство получило возможность блокировать практически любые ресурсы, распространявшие недостоверную информацию, в особенности материалы, которые могли навредить репутации государства.

Далее в 1997 г. был опубликован «План государственной информатизации в рамках 9-й пятилетки и перспективные цели до 2010 г»²⁵⁴. Данный документ предусматривал цифровизацию основных государственных систем в срок до 2010 года. Как отмечается в документе, в области развития информационных технологий и интегральных схем в Китае будет проводиться стимулирующая политика, включающая льготные условия и специализированные проекты. Это направлено на укрепление потенциала страны в создании информационных систем и оборудования для поддержки экономического и социального развития.

В 2000 г. также был опубликован «Закон о безопасности сетевой инфраструктуры и сети Интернет»²⁵⁵. Согласно основным пунктам данного документа, было запрещено пользоваться ресурсами сети интернет для того, чтобы создавать, распространять, копировать или передавать информацию определенного содержания. К такому типу информации можно отнести призывы к отказу от исполнения государственных законов, совершению террористических актов, нарушению стабильности в обществе. Так, например,

²⁵⁴ 中华人民共和国国民经济和社会发展“九五”计划和2010年远景目标纲要 (План национального экономического и социального развития КНР в рамках 9-й пятилетки и перспективные цели до 2010 г.) [Электронный ресурс] // Официальный сайт Государственного комитета по развитию и реформам КНР. URL: <https://www.ndrc.gov.cn/fggz/fzzlgh/gjfgzh/200709/P020191029595686994247.pdf> (дата обращения: 05.05.2024).

²⁵⁵ 互联网信息服务管理办法 (Порядок управления услугами интернет-информации) [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/gongbao/content/2000/content_60531.htm (дата обращения: 05.05.2024).

согласно Статье 5 данного закона, организации, предоставляющие новостные, издательские, образовательные, медицинские, фармацевтические и другие информационные услуги в интернете, должны проходить проверку и получать одобрение соответствующих государственных органов. Без этого они не могут получить лицензию на свою деятельность или начать учетные процедуры. В статье 15 «Закона о безопасности сетевой инфраструктуры и сети Интернет» уточняется, что поставщики интернет-услуг не должны размещать информацию, которая:

1. Противоречит основным принципам Конституции;
2. Угрожает национальной безопасности, раскрывает государственные секреты, подрывает власть или единство нации;
3. Наносит ущерб чести и интересам страны;
4. Подстрекает к этнической ненависти или дискриминации и подрывает национальное единство;
5. Пропагандирует религиозные культы или феодальные суеверия, нарушая национальную религиозную политику;
6. Распространяет слухи, нарушает социальный порядок или подрывает стабильность общества;
7. Содержит материалы непристойного характера, порнографию, призывы к насилию, убийству, террору или преступлениям;
8. Оскорбляет или содержит клевету на других людей и нарушает их законные права и интересы;
9. Включает в себя другие запрещенные законами и административными правилами материалы.

В 2006 г. была опубликована «Государственная стратегия по развитию информатизации на период с 2006 по 2020 г.»²⁵⁶. Как подчеркивается

²⁵⁶ 2006–2020 年国家信息化发展战略 (Государственная стратегия по развитию информатизации на период с 2006 по 2020 г.) [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL:

в документе, активное продвижение информатизации является стратегическим шагом для современного развития Китая. Уточняется, что сфера информационных технологий продолжает стремительное развитие, и ее влияние на экономический рост постоянно увеличивается. В данном документе перечислены следующие задачи, которые ставились перед государственными ведомствами в рамках стратегического развития информатизации:

1. Содействовать цифровизации национальной экономики;
2. Содействовать постепенному внедрению систем электронного правительства.

Внедрение электронного правительства представляет собой комплексную программу, направленную на улучшение государственного управления и предоставление качественных государственных услуг гражданам и предприятиям. Основные направления этой программы включают в себя совершенствование государственных услуг, укрепление социального управления, комплексный надзор и улучшение макроконтроля экономической деятельности.

Первоочередная задача, которая ставится в данном документе перед государственными ведомствами, заключается в развитии системы электронного правительства, базирующейся на сети Интернет и обеспечивающей координацию между центральными и местными органами власти. Как отмечается, это позволит расширить доступность государственных услуг до уровня улиц, общин и деревень, повысив при этом их содержание и качество.

Также было запланировано усилить социальное управление путем создания эффективной информационной сети, объединяющей ресурсы и обеспечивающей всестороннее социальное управление. Важными аспектами этого процесса станут механизмы реагирования на чрезвычайные ситуации и обеспечение национальной безопасности и стабильности.

https://www.gov.cn/gongbao/content/2006/content_315999.htm (дата обращения: 05.05.2024).

Кроме того, «Государственная стратегия по развитию информатизации на период с 2006 по 2020 г.» предусматривала усиление комплексного надзора в ключевых отраслях экономики, включая финансы, налогообложение, торговлю и другие.

3. Создать передовую сетевую культуру в китайском сегменте Интернета.

В документе подчеркивается, что для успешного развития сетевой культуры необходимо усилить присутствие передовой социалистической культуры в интернете. Это включает в себя поддержку здоровых и благотворных культурных инициатив, стандартизацию сетевого общения и создание позитивной сетевой атмосферы.

Также одной из важнейших задач обозначается необходимость построить позитивную и здоровую сетевую культуру, устанавливая нормы сетевого поведения и активно противостоять негативным явлениям в сети.

4. Построить национальную систему информационной безопасности. Данная задача, указанная в тексте «Государственной стратегии по развитию информатизации на период с 2006 по 2020 г.», является самой важной и одним из первых подтверждений тому, что внутренняя и внешняя политика властей КНР будут направлены на обеспечение информационной безопасности страны. Подчеркивается важность активного повышения потенциала национальной информационной безопасности КНР, включая освоение передовых технологий и теорий, обучение талантов в области информационной безопасности и улучшение юридической базы, регулирующей действия субъектов в информационной сфере.

Впоследствии в 2012 году было опубликовано Постановление Госсовета КНР «По продвижению информатизации и улучшению механизмов обеспечения информационной безопасности»²⁵⁷. Данный документ затрагивал

²⁵⁷ 国务院关于大力推进信息化发展和切实保障信息安全的若干意见（国发〔2012〕23号）（Некоторые мнения Государственного совета КНР о форсированном продвижении развития информатизации и реальном

такие сферы регулирования информационного пространства, как: контроль интернет-приложений и оказание информационных услуг. Также в рамках указанного Постановления был утвержден список ответственных за обеспечение информационной безопасности в регионах. Кроме того региональные власти получили возможность ограничивать интернет-трафик и доступ к переписке при потенциальной угрозе информационной безопасности государства.

Развитие законодательства, связанного с регулированием информационного пространства, продолжалось непрерывно и адаптировалось под новые реалии. Так, в 2015 году был принят «Антитеррористический закон КНР»²⁵⁸, согласно которому КНР будет противодействовать любым проявлениям терроризма, будет подвергать преследованию организации, которые занимаются террористической деятельностью, подстрекательством к совершению противоправных действий. В законе объясняется, что под терроризмом понимаются убеждения и действия, которые вызывают паническое состояние в обществе и угрожают общественной безопасности. Такие действия могут направляться на причинение вреда частной собственности или угрожать государственным органам и международным организациям. Целью терроризма является достижение политических и идеологических целей через применение насилия и угроз.

В пункте 19 данного закона подчеркивается, что операторы телекоммуникационного бизнеса и провайдеры интернет-услуг обязаны внедрить системы безопасности для контроля за информационным содержанием и предотвращения распространения материалов с

обеспечении информационной безопасности, № 23, 2012 г.) [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/gongbao/content/2012/content_2192395.htm (дата обращения: 05.05.2024).

²⁵⁸ 中华人民共和国反恐怖主义法 (Закон КНР «О противодействии терроризму») [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/zhengce/2015-12/28/content_5029899.htm (дата обращения: 05.05.2024).

террористическим или экстремистским содержанием. В случае обнаружения подобной информации, они должны прекратить ее передачу, сохранить соответствующие записи, удалить контент и сообщить об этом органам общественной безопасности. Это позволяет государству эффективнее бороться с терроризмом и экстремизмом в сети, обеспечивая безопасность информационного пространства.

В октябре 2016 года постоянный комитет ВСНП принял «Закон о кибербезопасности КНР»²⁵⁹, который вступил в силу 1 июня 2017 года. Данный нормативный акт состоит из шести основных глав и приложения и определяет права и обязанности пользователей и компаний-провайдеров:

- Глава 1. Общие положения;
- Глава 2. Поддержка и продвижение кибербезопасности;
- Глава 3. Операционная безопасность сетей;
- Глава 4. Информационная безопасность сетей;
- Глава 5. Мониторинг, раннее предупреждение и реагирование в чрезвычайных ситуациях;
- Глава 6. Юридическая ответственность;
- Глава 7. Уставные документы.

В рамках данного документа сформулированы основные принципы и механизмы поддержки и развития безопасности китайского сегмента Интернета, в том числе надзора и превентивных мер, а также реагирования на различные экстренные ситуации.

Как отмечается в первой статье «Закона о кибербезопасности КНР», государство проводит различные меры по контролю, обеспечению безопасности и устранению угроз в цифровой сфере, возникающих как на территории КНР,

²⁵⁹ 中华人民共和国网络安全法 (Закон КНР «О кибербезопасности») [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm (дата обращения: 05.05.2024).

так и исходящих извне. Соответствующие меры направлены на защиту критически важной информационной инфраструктуры от атак, а также на вынесение наказания для киберпреступников, нарушивших закон. Важно подчеркнуть, что данный нормативный документ включил в себя основные нормы и правила пользования Интернетом на территории КНР, действовавшие до момента вступления в силу этого закона.

«Закон о кибербезопасности КНР» направлен на обслуживание и использование ресурсов интернета, а также эксплуатацию различных социальных платформ. В законе подчеркивается, что государство предпринимает различные меры для укрепления сетевой безопасности. Так, например, уточняется, что операторы связи должны самостоятельно регулировать системы, обеспечивающие безопасность, и создавать условия для предотвращения распространения компьютерных вирусов или хакерских атак. Согласно нормативному акту, операторам предписано заниматься обеспечением мониторинга состояния сетей, решать возникающие проблемы безопасности, а также создать условия для хранения подготовленных отчетов сроком не менее полугода с момента создания. Важно подчеркнуть, что рассматриваемый закон стал прецедентным в рамках китайского законодательства: власти получили возможность контролировать все, что происходит в китайском сегменте Интернета. В законе отдельно отмечается важность идентификации пользователей: для того, чтобы зарегистрироваться в социальной сети и проводить какие-то действия в цифровом пространстве гражданам необходимо указывать свои настоящие данные.

В соответствии со статьей 31 рассматриваемого Закона государство рассматривает в качестве необходимой меры защиту ключевой информационной инфраструктуры, которая используется для обеспечения бесперебойной работы в сферах энергетики, государственных и финансовых услуг и других сфер. Как подчеркивается, в случае повреждения объектов

данной инфраструктуры, утечки информации и кибератак национальной безопасности всего государства может оказаться под угрозой.

Законом о кибербезопасности КНР было введено понятие «ключевой информационной инфраструктуры», что привело к наложению дополнительных обязательств на операторов, обеспечивающих работу ключевой информационной инфраструктуры. Важно отметить, что в законе не дается четкого определения КИИ и конкретной сферы применения.

Как указано в статье 37 Закона о кибербезопасности, вся личная информация пользователей, а также данные, которые были собраны в результате операционных действий, должны храниться на серверах, расположенных на территории КНР. В случае предоставления подобной информации иностранным компаниям проводится оценка безопасности, которая основана на предписаниях, сформулированных национальным органом управления киберпространством и соответствующим департаментом Госсовета КНР. Данная статья определяет обязанность иностранных юридических лиц хранить серверы для китайских пользователей на территории Китайской Народной Республики.

Закон о кибербезопасности КНР включает в себя понятие «многоуровневой системы информационной безопасности», которое было сформулировано еще в Правилах безопасности защиты компьютерных информационных систем от 1994 года. Так, стоит подчеркнуть, что правила, регламентирующие такие вопросы, как доступ в интернет, регистрацию доменов, распространение информации, обмена сообщениями, и требующие от пользователей предоставления своих персональных данных, уже являлись частью государственной политики по регулированию деятельности граждан в Интернете.

В статье 65 рассматриваемого Закона сказано, что в случае, если продукция или услуги не соответствуют стандартам безопасности и не прошли проверку, то деятельность операторов является незаконной.

Особое внимание в нормативном акте уделили сбору, обработке и защите персональных данных граждан. Глава 4 Закона о кибербезопасности полностью посвящена вопросу безопасности данных в сети Интернет.

В статье 40 отмечается, что операторы сетей обязаны создать надёжную систему хранения и обработки персональной информации для обеспечения конфиденциальности. Деятельность операторов сетей должна основываться на принципах «законности, правомерности и необходимости». Кроме того, информация о правилах сбора и использования полученной информации должна быть транспарентной, а операторы сетей в обязательном порядке должны получать согласие лица, чья персональная информация подлежит сбору и дальнейшей обработке.

В случае утечки личных данных, оператор обязан в кратчайшие сроки уведомить об этом пользователей и сообщить всю необходимую информацию компетентным органам. Если пользователем будет обнаружена ситуация, когда оператор сети использует его личные данные в нарушение положений Закона, он может потребовать от оператора удалить информацию, которая нарушает конфиденциальность переданных оператору данных.

Система реализации государственной информационной политики в КНР определяется строгой иерархией на уровне партийных органов и различных государственных ведомств.

Среди государственных структур в рамках обеспечения кибербезопасности можно выделить Министерство общественной безопасности Китайской Народной Республики.

Деятельность данного ведомства направлена на разработку необходимых стандартов и нормативно-правовых документов, осуществление надзора за

соблюдением правил сетевой безопасности, мониторинг потенциальных угроз и изо своевременное предотвращение, контроль производства товаров и услуг в цифровом пространстве, а также на проведение расследований деятельности киберпреступников.

В 2015 году на базе Министерства общественной безопасности КНР была сформирована так называемая Сетевая полиция²⁶⁰ (网络警察). Учреждение подобного рода структуры являлось прямым сигналом к тому, что государство уделяет особое внимание борьбе с киберпреступностью.

В рамках деятельности государства в цифровом пространстве важную роль играет Министерство государственной безопасности КНР²⁶¹. В состав данного ведомства входит Центр оценок информационной безопасности КНР (中国信息安全测评中心), который отвечает за обеспечение информационной безопасности различных государственных органов. Единственным исключением является НОАК, в которой существует свой собственный ресурс по обеспечению безопасности, в том числе информационной.

Одним из основных органов в рамках имплементации информационной политики на территории КНР является Управление по делам киберпространства КНР (国家互联网信息办公室). Данное ведомство регулирует взаимодействие между партийными и государственными структурами и относится сразу и к КПК, и к Госсовету КНР.

В рамках регулирования информационного пространства китайского сегмента сети Интернет основным государственным органом, который занимается вопросами медиарегулирования, является Канцелярия центральной

²⁶⁰ Официальный сайт Сетевой полиции КНР [Электронный ресурс]. URL: <https://cyberpolice.mps.gov.cn/#/> (дата обращения: 18.02.2022).

²⁶¹ Официальный сайт Министерства государственной безопасности КНР [Электронный ресурс]. URL: <http://www.itsec.gov.cn> (дата обращения: 18.02.2022).

комиссии по кибербезопасности и информационным технологиям КНР (中央网络安全和信息化委员会办公室 или ССАС).

Кроме того, важным ведомством в рамках реализации государственной информационной политики КНР является Центральная комиссия по сетевой безопасности и информатизации КПК (中央网络安全和信息化委员会), которая курирует вопросы борьбы с киберпреступностью и противоправной деятельностью в сети Интернет. Важно подчеркнуть, что председателем данного ведомства является лично Председатель КНР, генеральный секретарь КПК, Председатель Центрального военного совета КНР Си Цзиньпин.

В соответствии с открытыми данными можно сделать вывод о том, что Центральная комиссия по сетевой безопасности и информатизации отвечает за вопросы, связанные с оборонительными и наступательными действиями в цифровой среде, а также за вопросы контентной политики в китайском сегменте сети Интернет.

Управление по делам киберпространства КНР было создано в 2011 году по решению Госсовета Китайской Народной Республики²⁶². Ведомству были переданы функции, связанные с координацией обеспечения информационной безопасности и реализуемые ранее Министерством промышленности и информационных технологий (中华人民共和国工业和信息化部). В 2014 году был начат процесс реорганизации работы органов, регулирующих информационное пространство, в результате чего Управлению были переданы новые полномочия, включающие регулирование и контроль Интернет-контента,

²⁶² «Создано Управление по делам киберпространства» [Электронный ресурс] // Официальный сайт газеты Guangming Daily. URL: http://epaper.gmw.cn/gmrb/html/2011-12/22/nw.D110000gmrb_20111222_7-04.htm?div=-1 (дата обращения: 05.05.2024).

а также координацию правоохранительных органов²⁶³. В 2018 полномочия Управления по делам киберпространства КНР были вновь расширены: под управление ведомства был переведён Центр кризисного управления в сфере информационной безопасности (国家计算机网络与信息安全管理中心), который ранее находившийся в подчинении Министерства промышленности и информационных технологий. Важно подчеркнуть, что Центр кризисного управления в сфере информационной безопасности является негосударственным и некоммерческим²⁶⁴.

Функционал Управления по делам киберпространства КНР может быть определен следующими задачами:

1. Создание правовой системы по распространению информации в сети Интернет;
2. Осуществление координации работы государственных институтов, ответственных за управление информационными потоками в сети Интернет;
3. Контроль за деятельностью органов, ответственных за построение сетевого культурного фронта;
4. Отслеживание и борьба с вредоносными ресурсами, появляющимися в сети Интернет;
5. Координация деятельности структур, которые занимаются регистрацией доменных имен, IP-адресов, а также мобильных операторов и провайдеров;

Управление по делам киберпространства КНР (САС) принимает активное участие в процессах разработки и имплементации политических решений, направленных на регулирование деятельности граждан и компаний в сети

²⁶³ «Реорганизация Управления по делам киберпространства: Госсовет уполномочивает его нести ответственность за регулирование Интернет-контента и координацию правоохранительных органов» [Электронный ресурс] // Guancha.cn. URL: http://www.guancha.cn/politics/2014_08_28_261572.shtml (дата обращения: 22.02.2024).

²⁶⁴ «Центр кризисного управления в сфере информационной безопасности» [Электронный ресурс] // Национальный центр реагирования на компьютерные инциденты КНР. URL: <https://www.cert.org.cn/publish/main/34/index.html> (дата обращения: 22.02.24).

Интернет. Данное ведомство напрямую подчиняется Руководящей группе ЦК КПК по вопросам информатизации и безопасности в Интернете, которая, в свою очередь, подчиняется Центральному комитету КПК. Руководитель САС является заместителем председателя данной Руководящей группы.

Согласно доступным источникам, в Управлении по делам киберпространства КНР есть следующие отделы: Центр решения чрезвычайных ситуаций в сфере интернет-безопасности, Центр обслуживания нужд агенства, а также Центр докладов о незаконной информации, распространяемой в сети Интернет²⁶⁵.

В отличие от других государственных ведомств КНР, на сайте Управления по делам киберпространства не представлена информация о его структуре, функционале, бюджете.

Как отмечают Кокошин А. Ю., Кашин В.Б., Главный центр кризисного управления в сфере кибербезопасности считается «самым крупным департаментом Управления по делам киберпространства КНР»²⁶⁶.

САС курирует такие сферы, как отслеживание IP-адресов пользователей, комментарии, оставленные пользователями в социальных сетях, блокировка сервисов VPN, цензура контента, публикуемого в Интернете и т.д.

В соответствии с текстом «Закона о кибербезопасности КНР»²⁶⁷, который вступил в силу в 2017 году, САС также занимается сертификацией оборудования, используемого в рамках обеспечения информационной

²⁶⁵ 中央网信办所属事业单位面向社会公开招聘 (Подведомственные учреждения Центрального управления по делам киберпространства проводят открытый набор сотрудников) [Электронный ресурс] // Официальный сайт информационного агенства «Синьхуа». URL: http://www.xinhuanet.com/politics/2015-10/19/c_128335178.htm (дата обращения: 17.07.2024).

²⁶⁶ Кокошин А.А., Кашин В.Б. О подходах руководства КНР и китайских силовых структур к противоборству в киберпространстве [Электронный ресурс] // Российский совет по международным делам. URL: <https://russiancouncil.ru/analytics-and-comments/comments/o-podkhodakh-rukovodstva-knr-i-kitayskikh-silovykh-struktur-k-protivoborstvu-v-kiberprostranstve/> (дата обращения: 2.08.2025).

²⁶⁷ 中华人民共和国网络安全法 (Закон КНР «О кибербезопасности») [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm (дата обращения: 13/11/2024).

безопасности КНР. Управление также проводит проверки данных китайских компаний, которые хранятся не на территории Китайской Народной Республики.

В рамках своей деятельности САС уделяет особое внимание борьбе с дезинформацией и информацией, распространение которой может привести к дестабилизации ситуации внутри страны. Так, по сообщению государственного информационного агентства «Синьхуа», Управление распространило среди китайских Интернет-компаний, владеющих различными социальными сетями, платформами и Интернет-порталами, перечень правил, определяющих, какие комментарии могут быть допущены в публикации, а какие комментарии должны быть заблокированы. Блокировке должны быть подвергнуты комментарии, наносящие ущерб национальной безопасности КНР, интересам граждан КНР, религиозной политике, а также комментарии, распространяющие дезинформацию в целях нарушения общественного порядка²⁶⁸.

В рамках реализации государственной информационной политики КНР одним из важнейших партийных органов является Отдел пропаганды ЦК КПК.

Основными задачами данного Отдела являются: содействие распространению марксистской теории на территории все страны; контроль и координационные мероприятия по налаживанию работы СМИ; создание продуктов духовной культуры; определение вектора идеологической работы ответственных органов и ведомств; модерирование работы органов государственной пропаганды²⁶⁹.

Отдел пропаганды ЦК КПК управляет идеологической работой, средствами массовой информации, образовательной политикой, а также

²⁶⁸ 29家网站签署《跟帖评论自律管理承诺书》(29 сайтов подписали «Обязательство о саморегулировании управления комментариями к публикациям») [Электронный ресурс] // Sina News. URL: <http://news.sina.com.cn/c/2014-11-06/223631106669.shtml> (дата обращения: 14.02.2023).

²⁶⁹ 中国共产党中央委员会宣传部 (Отдел пропаганды Центрального комитета Коммунистической партии Китая) [Электронный ресурс] // Baidu Baike. URL: https://baike.baidu.com/item/中国共产党中央委员会宣传部?fromtitle=中共中央宣传部&fromid=10317351&fromModule=lemma_search-box (дата обращения: 17/06/2023).

деятельностью различных органов Госсовета КНР, региональных властей и культурных учреждений, осуществляя цензуру всех источников информации в Китае. В рамках достижения целей, стоящих перед Отделом пропаганды ЦК КПК, активное участие принимают также департаменты пропаганды партийных комитетов и бюрократические ведомства всех уровней, профсоюзы, ассоциации работников сферы культуры, а также представители отделов пропаганды китайских и иностранных компаний, в которых есть партийные комитеты.

Важно подчеркнуть, что Отдел пропаганды ЦК КПК, несмотря на свою значимую роль в системе цензуры и пропаганды, не обладает практическим функционалом. Данный Отдел занимается преимущественно формулированием и распространением письменных или устных инструкций среди соответствующих ведомств.

Кроме того, важную роль в рамках функционирования системы пропаганды на территории китайской Народной Республики играет государственное информационное агентство «Синьхуа», которое функционирует не только на территории КНР, но и за ее пределами, во многих странах. Основными функциями данного информационного агентства являются освещение новостей и содействие распространению официальной государственной пропаганды.

Функционирование системы пропаганды в КНР направлено на обеспечение общественной стабильности. Работа органов пропаганды основывается на принципе позитивности пропаганды, в соответствии с которым необходимо поддерживать в обществе стабильность и уверенность. Кроме того, в китайских средствах массовой информации намеренно ограничивается объем распространяемого негативного контента, чтобы не создавать негативный образ партии, ее руководству и государству в целом²⁷⁰.

²⁷⁰ Brady A.-M. Guiding Hand: The Role of CCP Central Propaganda Department in the Current Era // Westminster Papers in Communication and Culture. 2006. Vol. 3, no. 1. P. 58–77.

В вопросе реализации государственной информационной политики, а также обеспечения контроля над распространяемой в цифровой среде информацией следует отметить работу Министерства промышленности и информационных технологий (*中华人民共和国工业和信息化部*)²⁷¹.

Данное Министерство было создано в 2008 году и изначально отвечало за вопросы регулирования и развития на территории КНР почтовой системы, распространения доступа к Интернету, мобильной связи, обеспечение доступа населения к телевизионным услугам, производства электронных товаров и информационных услуг, а также за устойчивое информационное развитие общества.

Среди функций Министерства промышленности и информационных технологий, необходимых к рассмотрению в рамках данного исследования, можно выделить:

1. Способствовать развитию производства национального программного обеспечения для компьютерных систем;
2. Координировать деятельность ответственных государственных органов по разработке политики по информатизации общества и внедрению технологий, в том числе в рамках формирования электронного правительства;
3. Обеспечивать устойчивость систем национальной информационной безопасности.

Так, например, 5 июня 2023 года в рамках 31-ой Международной выставке информации и телекоммуникаций Цзинь Чжуанлун заявил о планах Министерства по активизации работы по разработке и дальнейшему внедрению Интернету нового шестого поколения - сети 6G²⁷².

²⁷¹ Официальный сайт Министерства промышленности и информатизации КНР [Электронный ресурс]. URL: <https://www.miit.gov.cn> (дата обращения: 13.08.2023).

²⁷² Министерство промышленности и информатизации КНР объявило о начале разработки сети 6G [Электронный ресурс] // Официальный сайт газеты «Жэньминь жибао». URL: <http://russian.people.com.cn/n3/2023/0605/c31518-20027943.html> (дата обращения: 14.03.2023).

Таким образом, государственная информационная политика Китая представляет собой целостную и динамично развивающуюся систему, в которой меры по технологическому развитию и цифровой трансформации неразрывно связаны с комплексным обеспечением национальной безопасности в киберпространстве. Стратегической целью является построение «сетевой державы», что подразумевает достижение технологического суверенитета, укрепление информационного суверенитета и защиту от внешних угроз. Ключевым инструментом для этого служит создание мощной нормативно-правовой базы, централизованная система управления под руководством Коммунистической партии Китая и чёткое распределение функций между профильными ведомствами. Приоритет отдаётся защите критической информационной инфраструктуры, контролю над данными и интернет-контентом, а также формированию «здоровой» и управляемой сетевой среды. Все эти меры направлены на обеспечение стабильности политической системы, устойчивого социально-экономического развития и защиты идеологических основ государства в цифровую эпоху.

2.3. Адаптация государственной власти к развитию социальных сетей в Китае

Одним из важнейших направлений информационной политики КНР является содействие расширению доступа к сети Интернет на территории всей страны, а также контроль публикуемой пользователями информации. В первую очередь это обусловлено тем, что контроль над информационными потоками, появляющимися в свободном доступе, играет ключевую роль в вопросе обеспечения социальной стабильности. Интернет также используется государственными ведомствами для донесения официальной позиции государства по вопросам первостепенной важности и для формирования общественного мнения по этим вопросам. В целях обеспечения национальной

безопасности китайские власти также ограничивают доступ к информации, распространяющей отличающиеся от идей КПК ценности, которые могут сыграть деструктивную роль в вопросе отстаивания национальных интересов. Кроме того, развитие суверенной сети Интернет позволяет Китаю отказаться от зависимости от Запада в вопросе Интернет-технологий, социальных сетей, поисковых систем и другое.

В настоящее время развитие Интернета в Китае характеризуется высокими темпами: как с точки зрения строительства инфраструктуры, так и с точки зрения активной цифровизации всех сфер жизнедеятельности в КНР. Так, согласно 57-му «Статистическому отчету о состоянии развития интернета в Китае (第 57 次《中国互联网络发展状况统计报告》)²⁷³, публикуемому Китайским информационным центром в сфере Интернет (CNNIC), по состоянию на февраль 2026 года, совокупное количество интернет-пользователей на территории КНР составило 1,125 млрд человек. По сравнению с июлем 2025 года, данный показатель увеличился на 2 млн человек. Среди всех пользователей Интернета на территории Китайской Народной Республики доля городского населения составляет 72% от общего число (около 795 млн человек, а сельского населения - почти 28: (около 304 млн человек). Согласно отчету, число пользователей мобильного интернета достигло 1,096 млрд человек, а более 99% граждан, пользующихся Интернетом, подключаются к нему с помощью мобильных устройств. Как уточняется в документе, среди самых популярных способов доступа пользователей в Интернет можно выделить: мобильные устройства (99,7%), настольные компьютеры (34%), ноутбук (32,5%).

²⁷³ 新华社权威快报 | 我国网民规模达 11.25 亿人 (Количество интернет-пользователей в Китае достигло 1,125 млрд человек) [Электронный ресурс] // Официальный сайт агентства «Синьхуа». URL: <https://www.news.cn/politics/20260205/2b0859a2bc4a498ebf0bbaeb07557820/c.html> (дата обращения: 08.02.2026).

На территории Китайской Народной Республики Интернет был запущен в 1987 году, когда в Пекинском институте физики и высоких технологий было впервые сформировано и отправлено электронное сообщение²⁷⁴. А уже в 1990 году была проведена регистрация домена «.cn», которая в настоящее время принадлежит КНР и используется для ресурсов, зарегистрированных на территории Китая.

Государственная политика китайских властей в отношении контроля информации, а также развития Интернета и расширения доступа граждан к нему может быть разделена на следующие этапы²⁷⁵:

1. Первый этап (1994 - 1999 гг) - постепенное формирование институциональной базы для строительства инфраструктуры и дальнейшего распространения доступа к сети Интернет на территории всей страны. В 1994 году Министерством государственной безопасности КНР был подписан документ «Правила безопасности и защиты компьютерных и информационных систем», что позволило ведомству официально регулировать действия пользователей в сети Интернет, а также проверять их на предмет нарушений.
2. Второй этап (2000 - 2003 гг) - совершенствование механизмов контроля Интернета.
3. Третий этап (с 2003 года) - начинается с приходом к власти Ху Цзиньтао и характеризуется ужесточением правил пользования Интернетом для граждан КНР, ускорением процесса создания механизма цензуры и фильтрации публикуемой информации, а также формированием предпосылок и дальнейших технологических решений для того, чтобы заблокировать на

²⁷⁴ Люлина А.Г., Ефименко Е.С. Интернет-цензура в современном Китае: жесткий контроль и гибкая система урегулирования // Вестник Российского университета дружбы народов. Серия: Всеобщая история. 2022. Т. 14, № 2. С. 177.

²⁷⁵ Там же.

территории Китайской Народной Республики доступ к западным социальным сетям, сайтам и платформам²⁷⁶.

Основной задачей реализации цензуры в Китае является не ограничение пользователям доступа на получение запрашиваемой информации, а контроль над публикацией материалов по некоторым темам, обсуждение которых могут стать причиной нарушения стабильности и общественного порядка²⁷⁷.

В период с 2009 года власти КНР начали реализовывать план по активной цензуре, а затем и дальнейшей блокировке доступа к западным социальным сетям, сайтам и платформам²⁷⁸. Так, в настоящее время на территории Китая заблокирован доступ к следующим сайтам: Google, Twitter, Facebook, WhatsApp, Instagram, Yahoo, Viber и другим. Одновременно с этим соответствующие ведомства, отвечающие за развитие Интернета в КНР, начали активно реализовывать планы по созданию собственных национальных платформ, которые позиционировались в качестве альтернативы западным приложениям, которые применялись для того, что отправлять электронные сообщения, смотреть видео, искать различную информацию в сети Интернет и другие.

На сегодняшний день в Китайской Народной Республике созданы и активно функционируют такие платформы, как: Weibo, Wechat, Douyin, Bilibili, Tencent QQ, Kuaishou, Youku, Xiaohongshu, Toutiao, а также национальная поисковая система Baidu.

Самым популярным по количеству пользователей и их активности на территории Китая является социальная сеть WeChat (微信).

²⁷⁶ Габриелян Г.Р. Развитие национальных интернет-платформ как фактор обеспечения информационной безопасности КНР // Вопросы национальных и федеративных отношений. 2024. Т. 14, № 6(111). С. 1878.

²⁷⁷ Зверев А.Л., Федоров А.П. Социальные сети как инструмент политического манипулирования (на примере организации массовых протестов в Гонконге 2014 г.) // Вестник Бурятского государственного университета. 2015. № 7. С. 152.

²⁷⁸ Хегай А.Д. Проект «Золотой щит» // Запад и Восток: диалог культур: материалы Первой Международной молодежной научно-практической конференции, 28–29 апреля 2014 г. Томск: Издательство Томского университета, 2014. С. 58.

По состоянию на конец 2024 года общее число уникальных пользователей, зарегистрированных в WeChat, составляет порядка 1,385 млрд человек. Несмотря на большую распространенность данного приложения среди населения Китайской Народной Республики, ежегодный прирост новых пользователей составляет в среднем 2-3% в год²⁷⁹.

Создание WeChat началось в 2010 году компанией Tencent, которая к тому моменту уже запустила мессенджер QQ. Данный мессенджер был популярен, но им можно было пользоваться только с компьютера, в связи с чем компания Tencent начала искать возможности для создания мобильного приложения. Над созданием WeChat работала команда разработчиков во главе с Чжан Сяолуном. В январе 2011 года была представлена и запущена первая версия мессенджера, которая предлагала такие базовые услуги, как отправка текстовых сообщений и фото. На тот момент одним из основных конкурентов WeChat был мессенджер WhatsApp, но китайская платформа отличалась тем, что сразу была ориентирована на китайский рынок и особенности китайских пользователей. В 2012 году функционал мессенджера был расширен: появилась возможность отправлять голосовые сообщения (Push-to-Talk), позднее была добавлена функция сканирования QR-кодов. Уже в 2013 году в мессенджер была интегрирована важная функция, которая фактически превращала WeChat приложение онлайн-банкинга - WeChat Pay. С помощью данной функции стало возможным оплачивать онлайн-покупки, отправлять и принимать денежные переводы. Это стало одной из отправных точек для активного развития мобильных платежей на территории КНР. В 2017 году функционал мессенджера был дополнен мини-приложениями (WeChat Mini-apps), которые встроены прямо в WeChat и не требуют установки дополнительных приложений. К такими

²⁷⁹ Tencent Annual Report 2024 (Годовой отчет компании Tencent за 2024 год) [Электронный ресурс] // Официальный сайт компании Tencent. URL: <https://static.www.tencent.com/uploads/2025/04/08/1132b72b565389d1b913aea60a648d73.pdf> (дата обращения: 27.10.2024).

мини-приложениям можно отнести программы для бронирования гостиниц, покупки авиабилетов, заказа такси, онлайн-шоппинга и другое.

Кроме того, в WeChat есть возможность регистрировать как обычные пользовательские аккаунты, так и публичные верифицированные аккаунты, которые имеют более широкий функционал и возможности.

Публичный аккаунт в WeChat - это официальный верифицированный аккаунт, который может быть использован как авторизованный источник распространения информации. Подобные типы аккаунтов используются компаниями, государственными ведомствами, СМИ. Как уточняют в самом WeChat, если пользователь хочет заниматься распространением новостного или развлекательного контента, то ему стоит зарегистрировать публичный аккаунт²⁸⁰.

Компания Tencent прикладывает большие усилия для защиты прав производителей и на постоянной основе проводит проверки публичных аккаунтов в WeChat, которые занимаются продажей товаров. Так, в 2024 году в WeChat было обнаружено и заблокировано около 50 тысяч аккаунтов, которые занимались продажей поддельных товаров²⁸¹. Кроме того, в течение года было изучено около 76 тысяч прямых трансляций, которые проводились публичными аккаунтами, продающими поддельные товары, а 25 тысяч подобных аккаунтов было заблокировано.

Важно подчеркнуть, что WeChat является уникальной платформой, которая не имеет аналогов ни на территории Китая, ни в мире: данная социальная сеть трансформировалась в единую экосистему, предоставляющую

²⁸⁰ 什么是公众号 (Что такое официальный аккаунт WeChat) [Электронный ресурс] // Tencent Customer Service. URL: https://kf.qq.com/faq/120911VrYVrA15091832Qzqq.html?scene_id=kf33847 (дата обращения: 27.10.2024).

²⁸¹ Tencent 2024 Environmental, Social and Governance Report (Отчет Tencent в области экологии, социальной ответственности и корпоративного управления за 2024 год) [Электронный ресурс] // Официальный сайт компании Tencent. URL: <https://static.www.tencent.com/uploads/2025/04/08/00ef711d9596ce09344c0260b14cda7e.pdf> (дата обращения: 27.04.2025).

возможности для общения с помощью текстовых и голосовых сообщений, для совершения аудио- и видеозвонков, прослушивания музыки и видео, совершения покупок, оплаты налогов, перевода и получения денег через WeChat Pay и многое другое. С появлением WeChat Pay на территории КНР фактически потеряли свою актуальность приложения для онлайн-банкинга, так как в мессенджеры собраны все функции, позволяющие отправлять и принимать денежные переводы, оплачивать счета и т.д.

Учитывая роль мессенджера WeChat в информационном пространстве Китая, компания Tencent реализовывает ряд программ, направленных на борьбу с распространением слухов и недостоверной информации через аккаунты в WeChat. Так, например компанией была создана платформа «Fact Check», которая в автоматизированном режиме помогает найти недостоверную информацию и опубликовать материал, который содержит проверенные данные по соответствующей тематике. В среднем данная платформа публикует до семи образовательных материалов, которые направлены на борьбу с дезинформацией через аккаунты в Tencent News и WeChat, на тему медицины, науки, технологий и другое²⁸².

Также в WeChat активно борются с мошенническими аккаунтами: в платформу интегрированы комплексные инструменты для того, чтобы проводить мониторинг, предотвращать, а также соответствующим образом реагировать на мошеннические действия со стороны пользователей. Данные инструменты позволяют выявлять аккаунты, которые потенциально занимаются мошеннической деятельностью, оповещать пользователей и заблаговременно блокировать подобные аккаунты.

²⁸² Tencent 2023 Environmental, Social and Governance Report (Отчет Tencent в области экологии, социальной ответственности и корпоративного управления за 2023 год) [Электронный ресурс] // Официальный сайт компании Tencent. URL: <https://static.www.tencent.com/uploads/2024/04/08/a041eba55b96c7952e26180a2c7cdd28.pdf> (дата обращения: 27.10.2024).

Еще одной популярной на территории КНР платформой является Weibo - социальная сеть, общее количество активных пользователей которой, по данным на 2024 год, составляет около 583 млн человек²⁸³. Данная платформа используется для того, чтобы создавать и публиковать текстовые посты, изображения, видео, статьи, опросы и т.д. Weibo является платформой для того, чтобы обмениваться информацией, поэтому уделяет большое внимание оперативности публикаций, событиям, происходящим в Китае и мире, а также реакциям на подобные события.

Данный сервис был запущен в 2009 году компанией Sina Corp. Название Weibo (微博) переводится с китайского языка как «микроблог». Но в сравнении с западными платформами, такими как X или Facebook, китайская социальная сеть обладает более широким спектром опций.

Основные правила пользования платформой Weibo изложены в документе под названием «Конвенция сообщества Вэйбо»²⁸⁴.

Как отмечается в тексте данного документа, основной целью регулирования деятельности пользователей платформы является создание гармоничной и основанной на нормах права и законах КНР среды.

Для регистрации в Weibo пользователю нужно пройти верификацию личности через номер телефона. Для регистрации на других платформах, например Douyin, пользователям понадобится китайский номер телефона, а также удостоверение личности гражданина КНР. Это означает, что каждый аккаунт подтвержден с помощью ID-карты гражданина и закреплен конкретно за этим человеком. Таким образом платформа снижает вероятность незаконной

²⁸³ Number of monthly active users of Weibo Corporation from 2nd quarter of 2018 to 2nd quarter of 2024 (Количество ежемесячно активных пользователей Weibo Corporation со II квартала 2018 г. по II квартал 2024 г.) [Электронный ресурс] // Официальный сайт Statista. URL: <https://www.statista.com/statistics/795303/china-mau-of-sina-weibo/> (дата обращения: 29.10.2024).

²⁸⁴ Weibo Community Convention (Правила сообщества Weibo) [Электронный ресурс] // Официальный сайт Weibo. URL: <https://service.account.weibo.com/roles/gongyue> (дата обращения: 30.10.2024).

деятельности граждан, так как личности владельцев аккаунтов становятся известны еще на этапе регистрации.

В «Правилах для пользователей Weibo» уточняется, что платформа продвигает социалистические ценности, разработав правила управления контентом совместно с государственными ведомствами. Как подчеркивается, для борьбы с дезинформацией и управления безопасностью публикуемой информации были разработаны особые нормы, а также каналы для подачи жалоб на аккаунты, которые занимаются распространением недостоверной информации или незаконной деятельностью.

Согласно нормативным документам платформы, в Weibo запрещено публиковать информацию, которая нарушает общественный порядок или создает угрозу для безопасности граждан. Кроме того, публикации, содержащие кадры насилия, порнографии или запрещенных веществ, также не допускаются к публикации.

Для борьбы с публикацией недостоверной информации, неподтвержденных новостей или слухов Weibo использует следующие методы:

1. Официальные аккаунты, которые публикуют сообщения с опровержением появившейся на платформе недостоверной информации. Примером такого аккаунта может послужить официальный верифицированный аккаунт 微博辟谣 («Weibo опровергает слухи»)²⁸⁵. На данный аккаунт подписано более 2 млн человек, а частота публикации сообщения с опровержением составляет от 5 до 8 постов в день. Данный аккаунт активно взаимодействует с различными государственными ведомствами, а также с экспертами для того, чтобы раскрыть и опровергнуть дезинформацию в различных сферах.

²⁸⁵ Аккаунт «Weibo опровергает слухи» [Электронный ресурс] // Официальный сайт Weibo. URL: <https://m.weibo.cn/u/1866405545> (дата обращения: 30.10.2024).

За 2023 год через аккаунт 微博辟谣 было обработано более 87 тысяч постов с подозрением на недостоверность опубликованной информации, а также было опубликовано 3617 постов с опровержением слухов, которые публиковались в течение года в Weibo²⁸⁶.

2. Алгоритмы фильтрации информации. Для блокировки или удаления нежелательного контента, в том числе недостоверных новостей, сообщений, содержащих агрессию или нарушающих законы КНР, используются специальные механизмы работы с публикуемой информацией. Работа данных алгоритмов основана на машинном обучении и технологиях искусственного интеллекта, что позволяет в кратчайшие сроки анализировать и обрабатывать тексты, изображения и видео на предмет наличия запрещенного контента.
3. Метки достоверности. Все сообщения и публикации, которые прошли проверку на достоверность, получают соответствующую метку о том, что информация, изложенная в данном посте, соответствует действительности. Таким образом, пользователи могут сразу определить, что информация, которую они нашли в Weibo, достоверна. Это включает в себя такие метки, как "官方" (официальный), "认证" (верифицированный), а также "辟谣" (опровержение слухов). Подобные метки присваиваются аккаунтам, публикующим информацию, проверенную государственными или официальными источниками.
4. Система жалоб для пользователей. В Weibo пользователи могут сообщить о несоответствии правилам платформы опубликованной другими пользователями информации через систему жалоб. Для этого необходимо перейти в раздел «Жалобы» посредством нажатия кнопки «Оставить жалобу», которая доступна в каждой публикации. Затем пользователи могут выбрать

²⁸⁶ Weibo об удалении публикаций с недостоверной информацией [Электронный ресурс] // Baijiahao. URL: <https://baijiahao.baidu.com/s?id=1788306937048181558&wfr=spider&for=pc> (дата обращения: 30.10.2024).

категорию нарушения, например, дезинформация или нарушение авторских прав, и направить запрос на проверку конкретной публикации.

В правилах платформы уточняется, что отправлять заявление на рассмотрение жалобы могут только те пользователи, которые прошли проверку и верифицировали свою личность²⁸⁷. Обработка публикации после того, как будет направлено заявление с жалобой, включает в себя как изучение конкретного сообщения, так и деятельности аккаунта в целом. Действия платформы в отношении конкретного сообщения, на которое поступила жалоба могут включать: блокировку данного сообщения или его удаление, запрет на пересылку и комментарии, невозможность увидеть данное сообщение среди других сообщений и т.д. Действия платформы в отношении аккаунта, в адрес которого поступила жалоба, могут включать: блокировку функции публикации сообщений, а также написания комментариев, запрет на внесение изменений в информацию об учетной записи, удаление учетной записи.

5. Образовательные инициативы Weibo, направленные на развитие способности пользователей отличать недостоверную информацию от фактов. В разделе 创作者中心 («Центр для создателей контента») есть подраздел «Обучение», где ежедневно публикуются обучающие видео от самой платформы на различную тематику, в том числе и о том, как работать с источниками информации²⁸⁸.

В Weibo уделяют особое внимание борьбе с распространением слухов в социальной сети. Для того, чтобы вовремя обнаружить и отреагировать на подобные сообщения с недостоверной информацией, внутренние алгоритмы платформы анализирует три основных показателя: содержание публикаций,

²⁸⁷ Weibo Community Convention (Правила сообщества Weibo) [Электронный ресурс] // Официальный сайт Weibo. URL: <https://service.account.weibo.com/roles/gongyue> (дата обращения: 30.10.2024).

²⁸⁸ Центр обучения для пользователей Weibo [Электронный ресурс] // Официальный сайт Weibo. URL: <https://me.weibo.com/study> (дата обращения: 30.10.2024).

охваты публикаций и информация об аккаунт²⁸⁹. Так, информация по содержанию публикации включает в себя длину текста, наличие изображений или видео в конкретной публикации, эмоциональную окраску сообщения. Охваты оцениваются посредством анализа активности пользователей, количества репостов, а также количества лайков. При оценке аккаунта изучается степень авторитетности данного пользователя, количество подписчиков, история публикаций. Кроме того, в качестве дополнительного параметра учитывается такая метрика, как «аномалия комментариев», которая позволяет оценить количество комментариев под рассматриваемым сообщением, тональность и их содержание, что позволяет повысить вероятность обнаружения недостоверной информации²⁹⁰.

Еще одной популярной на территории КНР социальной сетью является Douyin - платформа для создания и просмотра коротких видео вертикального формата. Данная платформа была создана компанией ByteDance в сентябре 2016 года, а спустя год в рамках глобализации деятельности компании и ее продуктов была запущена международная версия Douyin - TikTok²⁹¹. На сегодняшний день платформа TikTok является одной из наиболее популярных платформ для создания и просмотра вертикальных видеороликов во всем мире.

Платформа Douyin активно использует государственные нормативные акты, которые находятся в публичном доступе, для того, чтобы адаптироваться

²⁸⁹ Лю Яхуэй, Цзинь Сяолун, Шэнь Хуавэй, Бао Пэн, Чэн Сюэци (Liu Ya-Hui, Jin Xiao-Long, Shen Hua-Wei, Bao Peng, Cheng Xue-Qi). 社交媒体中的谣言识别研究综述 (Обзор исследований по выявлению слухов в социальных медиа / A Survey on Rumor Identification over Social Media) // 计算机学报 (Китайский журнал компьютеров / Chinese Journal of Computers). 2018. Т. 41, № 7. С. 1547.

²⁹⁰Чжан Янсэнь, Пэн Юаньюань, Дуань Юйсян, Чжэн Цзя, Ю Цзяньцин (Zhang Yang-Sen, Peng Yuan-Yuan, Duan Yu-Xiang, Zheng Jia, You Jian-Qing). 基于评论异常度的新浪微博谣言识别方法 (Метод выявления слухов в Sina Weibo на основе аномальности комментариев / The Method of Sina Weibo Rumor Detecting Based on Comment Abnormality) // 自动化学报 (Acta Automatica Sinica). 2020. Т. 46, № 8. С. 1693.

²⁹¹ История создания компании ByteDance [Электронный ресурс] // Официальный сайт компании ByteDance. URL: <https://www.bytedance.com/en/> (дата обращения: 30.10.2024).

к требованиям регуляторов и формировать нормы поведения пользователей²⁹². Для того, чтобы зарегистрировать аккаунт в Douyin, пользователю необходимо предоставить китайский номер телефона, настоящее ФИО, а также национальную идентификационную карту КНР (ID-карта) для того, чтобы подтвердить свою личность²⁹³. Данная мера демонстрирует приверженность данной платформы соблюдению законов о деятельности пользователей в сети Интернет на территории КНР. Кроме того, в условиях пользования социальной сетью Douyin отмечается, что в случае, если из-за незаконной деятельности пользователя в отношении платформы будут применены какие-то санкции, то данный пользователь будет обязан компенсировать все издержки. Также в правилах пользования платформой подчеркивается, что пользователям не допускается использовать данные, изображения в профиле или описание данного аккаунта, которые выдают данного пользователя за другого человека, а также не допускается передача доступа к аккаунту другим лицам. Таким образом в Bytedance и Douyin придерживаются принципа прозрачности в деятельности пользователей, который отражает тесную связь между конкретным гражданином и аккаунтом, который зарегистрирован на имя данного человека.

В апреле 2022 года многие китайские социальные сети и платформы, в частности Douyin, Zhihu, Kuaishou, Jinri Toutiao и другие, начали отображать местоположение пользователей на основе их IP-адресов²⁹⁴. Данная мера направлена на борьбу с распространением слухов и информации, не соответствующей действительности. Если пользователь пользуется платформой

²⁹² Scharlach R., Hallinan B., Shifman L. Governing Principles: Articulating Values in Social Media Platform Policies // *New Media & Society*. 2023.P.134.

²⁹³Jiang M. Managing the Micro-Self: The Governmentality of Real Name Registration Policy in Chinese Microblogosphere // *Information, Communication & Society*. 2016. Vol. 19, no. 2. P. 211.

²⁹⁴ Chinese Social Media to Display User Locations Based on IP Address, Including Platforms from ByteDance and Zhihu [Электронный ресурс] // Официальный сайт газеты South China Morning Post. URL: <https://www.scmp.com/tech/big-tech/article/3174487/chinese-social-media-display-user-locations-based-ip-address> (дата обращения: 02.11.2024).

с территории Китая, то под каждым из опубликованных им видео будет отображаться конкретная провинция, которой принадлежит данный IP-адрес. В том случае, если пользователь находится за пределами территории КНР, то на его странице в Douyin будет демонстрироваться страна пребывания. Ни в одном из случаев точный IP-адрес пользователей не раскрывается.

Платформа Douyin активно борется с распространением не соответствующей действительности информации, особенно в тех случаях, когда это касается новостной повестки. Основные положения в рамках политики платформы по борьбе с дезинформацией раскрыты в пункте 5 «Правил по регулированию сообщества Douyin»²⁹⁵.

Так, в соответствии с правилами платформы запрещается:

1. Публикация неподтвержденных данных во время актуальных событий государственного или мирового масштаба или в отношении представителей политической элиты КНР с целью привлечения внимания;
2. Публикация информации, не соответствующей действительности и подрывающей имидж партии и правительства;
3. Публикация ложной информации, которая может привести к нарушению общественного порядка (например, информация о террористическом акте);
4. Публикации информации, которая может привести к насильственным действиям граждан в отношении друг друга;
5. Публикация видео или фото, которые были созданы с помощью технологий искусственного интеллекта или виртуальной реальности для введения пользователей в заблуждение.

В рамках борьбы платформы с распространением слухов и дезинформации были созданы инструменты, которые позволяют отслеживать и вовремя блокировать сообщения, в которых содержится ложная информация. В Douyin

²⁹⁵ Правила по регулированию сообщества Douyin [Электронный ресурс] // Официальный сайт Douyin. URL: https://www.douyin.com/rule/policy?activeId=self_decipline#heading-7 (дата обращения: 01.11.2024).

есть раздел « 抖音辟谣专区 » («Антифейковый раздел»), в котором на ежедневной основе публикуются материалы от экспертов, разоблачающих ложные сведения, появляющиеся в Douyin. Данные материалы представляют собой разъяснения от специалистов в сфере политики, экономики, истории, военного дела, медицины и других. Кроме того, создана группа « 抖音媒体辟谣团 » («Группа по разоблачению слухов СМИ»), основная деятельность которой заключается в анализе подозрительной информации на основе публикаций официальных СМИ, а также продвижении проверенных данных для очистки интернет-пространства. Вышеуказанные механизмы борьбы с дезинформацией были созданы и продвигаются в рамках инициативы « 谣零零计划 » («Равнение на ноль»). Данная инициатива направлена на поддержку пользователей, которые создают качественный антифейковый контент для борьбы с дезинформацией. Кроме того, платформа активно привлекает специалистов, создателей контента, а также простых пользователей в качестве общественных наблюдателей для отслеживания случаев появления в Douyin неподтвержденной информации. Таким образом платформа создает условия для эффективной борьбы со слухами, контроля публикуемой информации и предотвращения случаев незаконной деятельности пользователей.

Учитывая высокую скорость появления и развития социальных сетей на территориях КНР, представляется важным регулирование информации, которая появляется на данных платформах. Контроль за контентом, который публикуется в китайских социальных сетях обоснован необходимостью обеспечения общественного порядка, защиту национальных интересов, а также создания безопасных условий пользования Интернетом для пользователей.

В последние год популярностью пользуются платформы для создания и публикации коротких вертикальных роликов, такие как Douyin, Kuaishou и

другие. Данные платформы актуальны за счет своей инновационности, скорости создания и публикации контента, простоты понимания и адаптации к уникальным потребностям китайской аудитории. Важным следствием большой популярности платформ для создания вертикальных видео является то, что через подобные короткие ролики создаются и продвигаются новые тренды в таких сферах как мода, музыка, повседневная жизнь, а также популяризируются различные модели поведения. Так, молодежь активно использует данные платформы для самовыражения, также интегрирует так называемые «тренды» из данных социальных сетей в жизнь. Таким образом, пользователи с большим количеством подписчиков в данных социальных сетях, становятся лидерами общественного мнения и могут оказывать влияние на поведение граждан. Это создает угрозы для обеспечения стабильности в обществе, на которые государственные ведомства должны реагировать определенным образом и формировать механизмы, которые позволят контролировать деятельность пользователей подобных платформ. Так, в декабре 2021 года Государственное управление по делам телевидения и радиовещания КНР опубликовало «Подробные правила по проверке стандартов коротких видео в Интернете»²⁹⁶. Данный документ, как уточняется в пункте 1, продолжает создавать базу для регулирования деятельности пользователей в Интернете, как и ранее опубликованные нормативные акты. Всего данные правила включают в себя 100 пунктов, устанавливающих стандарты для проверки содержания публикуемых в китайских социальных сетях коротких роликов и направленных на повышение качества публикуемых материалов и предотвращения распространения недостоверной информации.

Так в документе уточняется, что для публикации запрещен контент,

²⁹⁶ «Подробные правила по проверке стандартов коротких видео в Интернете». Официальный сайт Государственного управления по делам телевидения и радиовещания КНР. Электронный ресурс. URL: https://www.nrta.gov.cn/art/2021/12/15/art_113_58926.html?fbclid=IwAR0wQvCBXoK2-O91vLP6PH-qUzUdVsgzMGNekLEz_Vnc_hxzz6E4fji_AJE. Дата обращения: 29.10.24

который создает угрозу для социалистической системы, включает призывы к разделению страны, наносит ущерб национальному имиджу, содержит оскорбления в отношении лидеров и героев революции, разглашает государственную тайну, не соответствует государственной политике в отношении религии, распространяет идеи терроризма и сепаратизма, оскорбляет традиционную культуру КНР, порочит образ государственных деятелей, содержит жестокие кадры или порнографию, оскорбляет чувства других граждан.

Кроме того, в октябре 2023 года шестью основными китайскими платформами, в том числе Douyin, Weibo, WeChat, Bilibili, было опубликовано заявление, согласно которому блогеры, чья аудитория насчитывает более 500 тысяч подписчиков, должны указывать свои реальные имена²⁹⁷. Данная инициатива в большей степени направлена в отношении акаунтов, на которых размещается новостной контент. В Китае такие аккаунты называют 自媒体 («Мы-медиа») и обозначают народную или любительскую журналистику, которая не имеет связи с профессиональными СМИ. Такие меры были приняты для того, чтобы контролировать и выявлять источники появления информации, которая не согласована с официальной цензурой руководства КНР. Как уточнили в компании ByteDance, являющейся владельцем Douyin, платформа не будет запрашивать никакой другой информации, кроме реальных имен и фамилий, и данные не будут передаваться третьим лицам. Как уточняли в СМИ, данные меры затронут деятельность тысяч блогеров, лишив их анонимности²⁹⁸.

Несоблюдение необходимых мер и правил может привести ко временным ограничениям деятельности соответствующих акаунтов или к полной

²⁹⁷ «Заявление восьми основных платформ о необходимости предоставлять настоящие данные владельцам аккаунтов с более чем 500 тыс. подписчиков» [Электронный ресурс] // Guancha.cn. URL: https://www.guancha.cn/politics/2023_10_31_714041.shtml (дата обращения: 28.10.2024).

²⁹⁸ China Removes Anonymity of Bloggers' Accounts with More than 500,000 Followers [Электронный ресурс] // Официальный сайт агентства Reuters. URL: <https://www.reuters.com/world/china/china-removes-anonymity-bloggers-accounts-with-more-than-500000-followers-2023-10-31/> (дата обращения: 28.10.2024).

блокировке и удалению страницы. Подобная инициатива демонстрирует заинтересованность властей КНР в контроле информации, которая публикуется в сети Интернет, и в прозрачности источников, которые распространяют информационные сообщения, особенно новостные.

В мае 2024 года появилась информация о том, что в Douyin выпустили новые правила, согласно которым деятельность пользователей по публикации политического, экономического, медицинского и социального контента в коммерческих целях будет ограничена²⁹⁹. Новые меры затронули аккаунты с большим числом подписчиков и широкой узнаваемостью среди пользователей, ограничив для них возможность использовать чувствительный контент для проведения коммерческих промоакций. Таким образом в Douyin была усилена проверка информации, связанной с политической, экономической или социальной тематикой, и фактически ограничена возможность публиковать подобный контент индивидуальным пользователям, чьи аккаунты не связаны с организациями.

Особое внимание платформа Douyin уделяет пользователям, публикующим новостной контент. Так, необходимо подчеркнуть, что только верифицированные аккаунты СМИ имеют право официально и легально публиковать новости. Среди китайских СМИ, которые официально зарегистрированы в Douyin, можно выделить Xinhua, Huanqiu Shibao, Guancha, Renmin Ribao и многие другие. Иностранные СМИ не присутствуют в Douyin по причине отсутствия возможности официальной верификации иностранного средства массовой информации на данной платформе. В Douyin действует наиболее жесткая форма контроля за публикуемой информацией и верификацией пользователей. В таких социальных сетях как Weibo или Bilibili иностранные СМИ могут зарегистрировать официальный аккаунт, пройти

²⁹⁹ Douyin Restricts Users from Publishing Political, Social Affairs, Legal and Other Content for Commercial Purposes [Электронный ресурс] // Официальный сайт газеты Global Times. URL: <https://www.globaltimes.cn/page/202405/1312220.shtml> (дата обращения: 01.11.2024).

процедуру верификации и далее в легальном порядке публиковать новостной контент. Так, например, новостное агентство Sputnik³⁰⁰ и международный телеканал RT³⁰¹ имеют официальные верифицированные аккаунты в Weibo, которые насчитывают около 11,775 млн и 2,1 млн подписчиков соответственно. В том случае, если в Douyin публикуется новостной контент с аккаунта, который не является официальным аккаунтом СМИ или не связан с таковым, то платформа после проверки данного видео не позволяет его опубликовать и направляет пользователю сообщение с предупреждением о том, что с аккаунтом, которые не верифицированы как СМИ, новостные сообщения публиковать нельзя. Меры, предпринятые платформой в отношении подобных пользователей, могут варьироваться от блокировки комментариев под конкретным видео до удаления аккаунта без права восстановления доступа к нему.

Кроме того, в Douyin немаловажным является вопрос соблюдения авторских прав, в связи с чем платформа разработала необычный механизм борьбы со случаями нарушения авторских прав. В Douyin, в отличие от других платформ, где применяется автоматизированная система отслеживания нарушений, применяется механизм под названием «жюри сообщества». Это группа зарегистрированных на платформе и обладающих высоким рейтингом пользователей, которые в рамках голосования выносят решения по спорным ситуациям. Так, если большинство из 31 члена жюри определяют деятельность пользователя как нарушение авторских прав, то в отношении данного аккаунта применяются меры - от временной блокировки аккаунта до его удаления. Для создателей контента, который нарушает правила платформы, разработана система, включающая в себя образовательные ролики и тесты для пользователей и позволяющая «переобучить пользователей и вновь сделать их

³⁰⁰ Официальный аккаунт новостного агентства Sputnik в Weibo [Электронный ресурс]. URL: <https://weibo.com/2181597154> (дата обращения: 01.11.2024).

³⁰¹ Официальный аккаунт международного телеканала RT (Russia Today) в Weibo [Электронный ресурс]. URL: <https://weibo.com/u/6244553417> (дата обращения: 18.12.2024).

частью сообщества»³⁰². Данные материалы и другие нормы по пользованию Douyin опубликованы в разделе «Объяснение правил» на сайте Douyin³⁰³.

Все обучающие материалы сопровождаются следующим сообщением: «Если вы впервые нарушаете правила Douyin, следуйте инструкциям на экране, чтобы получить информацию о правилах. Вы можете разблокировать свой аккаунт, приняв участие в викторине по правилам. Если ваш аккаунт заблокирован навсегда, вы можете только подать апелляцию и дождаться оценки платформы».

Таким образом, Douyin рассматривает пользователей, которые публикуют контент, не соответствующий правилам платформы, в качестве пользователей, которые не знакомы с ценностями сообщества. Если платформа приостанавливает действие аккаунта, единственный способ получить доступ к своему аккаунту и продолжить публиковать материалы на платформе - продемонстрировать свое понимание и согласие с теми нормами и правилами, которые являются для Douyin правильными.

Douyin уделяет большое внимание защите несовершеннолетних пользователей от нежелательного контента, так как это создает риски общественного порицания и возникновения спорных ситуаций. Так, в 2022 году руководством платформы были приняты новые правила по публикации и просмотру контента, которые были направлены на ограничение доступа несовершеннолетних пользователей к вредному контенту³⁰⁴. В соответствии с новыми правилами платформа будет блокировать все видеоматериалы, в которых будут содержаться призыв к совершению покупок в приложениях, вульгарные

³⁰² Petre C., Duffy B.E., Hund E. Gaming the System: Platform Paternalism and the Politics of Algorithmic Visibility // *Social Media + Society*. 2019. Vol. 5, no. 4. P. 7.

³⁰³ Правила по регулированию сообщества Douyin [Электронный ресурс] // Официальный сайт Douyin. URL: https://www.douyin.com/rule/policy?activeId=self_decipline (дата обращения: 01.11.2024).

³⁰⁴ Douyin Unveils New Content Rules to Safeguard Minors [Электронный ресурс] // Официальный сайт портала The China Project. URL: <https://thechinaproject.com/2022/03/24/douyin-unveils-new-content-rules-to-safeguard-minors/> (дата обращения: 02.11.2024).

кадры, пропаганда членства в незаконных формированиях и информация, не соответствующая традиционным ценностям.

Кроме того, в приложении Douyin добавили «Режим для молодежи», который подразумевает, что пользование платформой для пользователей младше 14 лет будет ограничено и составляет 40 минут в день, а также доступ к Douyin для данной категории пользователей будет недоступен после 22:00³⁰⁵. Данный режим просмотра видео на платформе Douyin предполагает доступ только к образовательным материалам, в том числе научные эксперименты, лекции по истории и культуре и т.д.

За последние несколько лет власти Китайской Народной Республики реализовали целый ряд решений, способствующих укреплению кибербезопасности страны, регулированию Интернета, а также ужесточению контроля на средствами массовой информации.

В рамках ужесточения наказаний и более строгого контроля за публикациями информации, имеющей стратегически важное значение для государства, 28 февраля 2024 года было объявлено о пересмотре некоторых пунктов "Закона о защите государственной тайны" и публикации новой редакции данного закона, которая вступила в силу с 1 мая 2024 года³⁰⁶. Пересмотренный закон предусматривает ужесточение наказания за нарушения нормативных актов о государственной тайне, а также расширение самого определения «государственная тайна». Так, в соответствии с новой редакцией "Закона о защите государственной тайны», к государственной тайне теперь относится и информация, имеющая отношение к экономике, политике, науке, технологиям, а также внешнеполитической деятельности КНР. Кроме того,

³⁰⁵ Заявление Douyin о введении новых правил пользования платформой для пользователей младше 14 лет [Электронный ресурс] // Официальный сайт газеты Shanghai Observer. URL: <https://sghexport.shobserver.com/html/baijiahao/2021/09/19/542299.html> (дата обращения: 02.11.2024).

³⁰⁶ 新修订的保守国家秘密法今年5月1日起施行 (В Китае с 1 мая 2024 года вступает в силу пересмотренный закон о защите государственной тайны) [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/yaowen/liebiao/202402/content_6934629.htm (дата обращения: 28.10.2024).

ужесточаются требования к гражданам, имеющим доступ к государственной тайне, и меры наказания за раскрытие или неправомерное применение информации государственной важности: штрафы до 1 миллиона юаней или тюремное заключение сроком до 10 лет.

Как подчеркивается, данный закон может способствовать дальнейшему укреплению национальной безопасности КНР и предотвращению раскрытия секретной информации. Власти КНР уточняет, что пересмотренный "Закон о защите государственной тайны» не предусматривает ограничение прав граждан или их свободы слова, а лишь способствует обеспечению стабильной ситуации в стране, а также защите национальных интересов³⁰⁷.

Принятие новой редакции данного закона также является показателем тенденции по усилению контроля над публикуемой на территории Китая и в китайском сегменте Интернета информации.

В апреле 2024 года Министерство общественной безопасности КНР выпустило заявление о начавшейся в декабре 2023 года масштабной операции по борьбе с распространением слухов и не соответствующей действительности информации в Интернете³⁰⁸. Как уточняется, за этот период полицейскими было проведено более 1500 арестов и заведено около 10 тысяч дел. Кроме того, надзорные органы наложили более 10 тысяч штрафов, а более 4200 различных информационных сообщений, распространяющих ложные сведения, были опровергнуты. В рамках данной кампании особое внимание было уделено социальным сетям и платформам, которые позволяют публиковать короткие видео и проводить прямые трансляции. Как отмечается, в результате деятельности соответствующих органов было заблокировано около 60 тысяч

³⁰⁷ 新修订的保守国家秘密法今年5月1日起施行 (В Китае с 1 мая 2024 года вступает в силу пересмотренный закон о защите государственной тайны) [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/yaowen/liebiao/202402/content_6934629.htm (дата обращения: 28.10.2024).

³⁰⁸ China Arrests over 1,500 for Illegal Acts Related to Cyberspace Rumors [Электронный ресурс] // Официальный сайт газеты China Daily. URL: <https://www.chinadaily.com.cn/a/202404/13/WS6619d500a31082fc043c1c01.html> (дата обращения: 29.10.2024).

аккаунтов, а также удалено более 700 тысяч публикаций, которые распространяли недостоверную информацию среди граждан.

Некоторые СМИ, освещая деятельность Министерства общественной безопасности КНР по борьбе с дезинформацией привели примеры дел против популярных блогеров, в том числе историю Турман Маоибэй³⁰⁹. Как уточняется, в феврале 2024 года ею было опубликовано видео, в котором она сообщила, что в одном из ресторанов Парижа ей дали учебники, которые якобы были забыты мальчиком из КНР по имени Цинь Лан. Блогер добавила, что вернет учебники данному мальчику. Данная публикация стала активно распространяться в социальных сетях и набрала большое количество просмотров в Douyin и Weibo. Спустя некоторое время девушка сообщила своим подписчикам, что ей удалось найти этого мальчика и вернуть ему учебники. Однако некоторые пользователи засомневались в том, что ситуация обстояла именно таким образом, и обратились в полицию. Полиции удалось выяснить, что данная история оказалось выдуманной и не имела ничего общего с реальностью. В результате на блогера наложили административный штраф, а в связи с резонансом и активными осуждениями подобных действий, девушка записала видеообращение с извинениями.

Еще одним примером эффективности мер, принятых китайскими властями в рамках борьбы с распространением дезинформации в Интернете, может послужить ситуация с одним из граждан, о которой в своем аккаунте в WeChat сообщил Отдел общественной безопасности городского округа Хэньян провинции Хунань³¹⁰. Так, некий гражданин Чжоу для того, чтобы повысить

³⁰⁹ Chinese Police Arrest over 1,500 for Online Rumours in Campaign Targeting Influencers, Bloggers and Live-Streamers [Электронный ресурс] // Официальный сайт газеты South China Morning Post. URL: <https://www.scmp.com/news/china/politics/article/3259183/chinese-police-arrest-over-1500-online-rumours-campaign-targeting-influencers-bloggers-and-live> (дата обращения: 28.10.2024).

³¹⁰ Официальный WeChat-аккаунт Отдела общественной безопасности городского округа Хэньян провинции Хунань [Электронный ресурс]. URL: https://mp.weixin.qq.com/s?__biz=MzI0NzA4NzAxNw==&mid=2651659646&idx=2&sn=7e1238f9146ef7398198141e

охваты публикаций в социальных сетях, разместил несколько фотографий с сообщением о том, что ему якобы одним из первых удалось посетить новое колесо обозрения в городе Хэньян. Это стало причиной активных обсуждений в Интернете и негативных комментариев со стороны жителей города. Гражданин Чжоу был оперативно обнаружен и получил наказание в соответствии с законом.

В октябре 2024 года Канцелярия центральной комиссии по делам киберпространства КНР объявила о проведении кампании по улучшению механизмов по регулированию деятельности сервисов, публикующих новостные сообщения, а также по противодействию незаконным действиям в этой области, в том числе распространению ложных сведений³¹¹. Данная кампания продлилась три месяца.

К основным целям данной кампании можно отнести усиление контроля над публикацией ложных новостей в Интернете и попыток манипулировать общественным мнением при помощи новостей, запрет на использование поддельных документов для регистрации новостных аккаунтов в социальных сетях, пресечение неправомерной деятельности сайтов, которые выдают себя за официальные средства массовой информации, необходимость лицензирования и соответствующей маркировки для аккаунтов, которые занимаются освещением новостей. Кроме того, как отмечается, для того, чтобы публикуемый контент был основан на новостных первоисточниках и имел доказательную базу, были ужесточены алгоритмы модерации публикаций в социальных сетях. Также будут увеличены способы и механизмы для отправки жалобы на сообщение, содержащее информацию, которая не соответствует действительности и создает ложное представление о происходящем.

ba84f33a&chksm=f384faeb25a036e350763eda15066fa0a7c6d050ce82f2935684b60557b39d9c32e9968f840d&scene=27 (дата обращения: 30.10.2024).

³¹¹ Канцелярия центральной комиссии по делам киберпространства КНР запустила кампанию по устранению нарушений в работе новостных и информационных служб в интернете [Электронный ресурс] // Официальный сайт Центрального телевидения Китая. URL: <https://news.cctv.com/2024/10/03/ARTIcB0WNYVSPRnVkmkVOpNq241003.shtml> (дата обращения: 29.10.2024).

Как отмечало агентство «Синьхуа», с января по сентябрь 2024 года ведомствами, ответственными за защиту киберпространства Китая, было рассмотрено около 27 тысяч дел, которые были связаны с ложными обвинениями и клеветой, и удалено порядка 1,5 млн опубликованных в социальных сетях сообщений³¹². Основной целью действий ответственных ведомств стала борьба с клеветой и публикацией дезинформации для того, целью которой являлось увеличение количества подписчиков, расширение охватов публикуемых постов, увеличение графика, а также незаконный действия по обогащению за счет увеличившегося числа подписчиков или выросших просмотров на публикуемых постах.

Таким образом, адаптация власти к соцсетям в Китае носит стратегический характер: от блокировки и замены западных платформ на национальные аналоги до внедрения идеологических установок через правила сообществ. Власть делегирует техническое регулирование компаниям, но сохраняет за собой роль законодателя. В свою очередь, социальные платформы адаптировались к законам, интегрировав требования государственных ведомств в модель развития социальных сетей. Они внедрили жёсткую систему верификации пользователей, сложные алгоритмы модерации и «воспитательные» меры для граждан, публикующих недостоверный контент. Эта адаптация сделала их не просто платформами, а инструментами управляемой цифровизации и реализации политики регулирования Интернета в КНР.

* * *

Таким образом, по итогам анализа теоретико-идеологических основ информационной политики КНР, законодательных механизмов регулирования

³¹² China Launches Crackdown on Illegal Online News Services [Электронный ресурс] // Официальный сайт агентства «Синьхуа». URL: <https://english.news.cn/20241003/d7004b4c772d4dbbb7fb44bcf3a1de37/c.html> (дата обращения: 28.10.2024).

интернет-пространства и практики адаптации государственной власти к развитию социальных сетей выявлены ключевые особенности китайской модели управления цифровой средой.

Установлено, что интернет-пространство в КНР рассматривается как сфера государственного суверенитета, национальной безопасности и идеологического воздействия, что закреплено в концепции киберсуверенитета.

Показано, что законодательная база регулирования носит системный характер и направлена на обеспечение контроля над данными, контентом и цифровой инфраструктурой, ключевую роль в чем играет Закон о кибербезопасности КНР.

Выявлено, что институциональная модель управления отличается высокой степенью централизации при ведущей роли партийных органов, обеспечивающих координацию регулирования и контроль информационных потоков.

Установлено, что адаптация к развитию социальных сетей реализуется через сочетание расширения доступа к Интернету и развития национальных платформ с усилением контроля над информационной средой.

Таким образом, китайская модель регулирования интернет-пространства представляет собой централизованную систему, направленную на обеспечение информационного суверенитета и социальной стабильности в условиях цифровизации.

Глава III. Управление Интернет-пространством в КНР: акторы, технологии и перспективы

3.1. Государство и цифровые корпорации в КНР: интересы и сферы взаимоотношений

В рамках изучения процессов повсеместной цифровизации и политики регулирования информационного пространства необходимо рассмотреть крупнейших игроков ИТ-сферы, большой тройки ВАТ: Baidu, Alibaba и Tencent. Данные компании являются прямыми конкурентами таким американским корпорациям, как Facebook, Amazon, Netflix, Google и другим. Так, основной специализацией Baidu являются поисковые системы, Tencent - социальные сети и мессенджеры, Alibaba - рынок электронной коммерции.

Анализ активности данных китайских компаний на рынке позволяет сделать вывод, что ВАТ проявляют большой интерес к различным стартапам и небольшим ИТ-компаниям и заключают сделки по их приобретению. Стратегия китайских технологических гигантов основана на приобретении небольших перспективных компаний, вложении средств в их развитие и дальнейшее обогащение за счет роста акций этих компаний или их перепродаже. Так, за период 2000-2020 гг. Baidu, Alibaba и Tencent приобрели 14 компаний, а общая стоимость заключенных сделок составила примерно 63 млрд долларов США³¹³. Лидирующую позицию в рамках приобретения стартапов занимает Alibaba, инвестировавшая порядка 49 млрд долларов США в покупку 11 компаний. При этом, важно подчеркнуть, что 12 из 14 приобретенных компаний являются китайскими, что демонстрирует сфокусированность ИТ-гигантов именно на развитии внутреннего китайского рынка и на получении доминирующего положения в сфере информационных и цифровых технологий КНР.

³¹³ China Digital Consumer Trends in 2019 [Электронный ресурс] // McKinsey & Company. URL: <https://www.mckinsey.com/~media/mckinsey/featured%20insights/china/china%20digital%20consumer%20trends%20in%202019/china-digital-consumer-trends-in-2019.pdf> (дата обращения: 30.10.2023).

Благодаря тому, что со стороны государственных органов власти Baidu, Alibaba и Tencent получали косвенную поддержку - блокировка западных социальных сетей и платформ - эти компании, начиная с 2009 года начали набирать экономическую мощь, а также начали играть важную роль и в политической сфере, углубив взаимодействие с государством. Основной стратегией компаний ВАТ является охват всей активности китайских пользователей сети Интернет за счет расширения спектра предлагаемых услуг. Некоторые исследователи называют подход, основывающийся на оказании широкого спектра услуг в рамках одной компании, «стратегией формирования бизнес-петли»³¹⁴. Китайские интернет-компании в рамках принятия этой стратегии основывались на бизнес-моделях Google, Facebook и Amazon. В соответствии с этим подходом компания увеличивает число клиентов за счет расширения спектра оказываемых услуг, пытаясь удовлетворить потребность каждого пользователя.

Baidu является крупнейшей компанией, функционирующей на территории КНР, по предоставлению комплексных интернет-услуг. Компания Baidu была основана в январе 2000 года предпринимателем Ли Яньхунем (李彦宏) в городе Чжунгуаньцунь. В настоящее время Baidu является одной из ведущих мировых технологических Интернет-компаний, которая создала китайскую национальную поисковую систему.

Так, в 2000 году основной целью Baidu являлось предоставление услуг по поиску информации в Интернете, так как на тот момент на уже наблюдался высокий спрос со стороны пользователей, а национальных компаний, способных предоставить соответствующий уровень услуг не было. Кроме того, иностранные поисковые системы ограничивали доступ китайским

³¹⁴ Срничек Н. Капитализм платформ / пер. с англ.; под науч. ред. М. Добряковой. М.: Изд. дом ВШЭ, 2019. С. 76.

пользователям к различным источникам информации. Так, согласно отчету компании за 2024 год, Baidu предоставляет услуги около 1 млрд пользователей и отвечает на поисковые запросы из более чем 100 стран и регионов мира³¹⁵. Как уточняется в отчетных документах компании, сервисы Baidu привлекают около 670 млн активных пользователей. За годы операционной деятельности компания Baidu создала экосистему, состоящую из различных приложений, сервисов и платформ, которые предоставляют пользователям разнообразные услуги. В экосистему Baidu входят следующие направления:

1. Baidu App - флагманское приложение, которое является основным ресурсом для получения поисковых и других услуг. Приложение позволяет получить доступ к поисковой системе, ленте новостей, музыкальным сервисам, видео- и аудио-материалам, картам, играм и т.д. Данное приложение можно использовать для получения доступа к большинству сервисов Baidu по системе «одного окна». Кроме того, в приложение интегрированы системы перевода, поиска информации по визуальному контенту, а также распознавание голоса. Поиск с помощью Baidu App характеризуется скоростью и точностью, так как приложение работает и на основе искусственного интеллекта.
2. Baidu Baike (百度百科) - онлайн-энциклопедия, созданная компанией Baidu и находящаяся в свободном доступе. Данный ресурс является аналогом Wikipedia. Бета-версия сайта Baidu Baike была запущена в 2006 году, а уже в в апреле 2008 года сайт был официально запущен.
3. Baidu Zhidao (百度知道) - платформа для обмена мнениями по различным аспектам политики, экономики, культуры и других. Так, пользователи могут

³¹⁵ Baidu 2024 Environmental, Social and Governance Report (Отчет Baidu в области экологии, социальной ответственности и корпоративного управления за 2024 год) [Электронный ресурс] // Официальный сайт компании Baidu. URL: <https://esgs.cdn.bcebos.com/2025/04/28/a2/39a2aaa4f728f4e2d0aebaff346c045e.pdf> (дата обращения: 10.06.2025).

задавать интересующие их вопросы и получить ответы от других пользователей (частных лиц и предприятий).

4. Baidu Jingyan (百度 经验) - блог-платформа, на которой пользователи могут вести свой личный блог, делиться различными историями, знаниями и наблюдениями в таких областях, как программирование, игры, кулинария и других.

Так, поисковая система Baidu, Baidu Baike, Baidu Zhidao и Baidu Jingyan работают в рамках единой системы, что позволяет пользователям оперативно получить необходимую им информацию.

5. Baidu Ditu (百度 地图) - приложение, с помощью которого можно построить различные маршруты, получить информацию по точному местонахождению и найти информацию по интересующим объектам. Кроме того, в приложение интегрирован голосовой ассистент, который позволяет полноценно управлять приложением с помощью голоса.

6. Baidu Health (百度 健康) - сервис, на котором публикуются различные материалы по теме медицинской тематике, лекции от более чем 300 тыс врачей и экспертов в сфере здравоохранения, дискуссионные форумы, а также предоставляются услуги телемедицины. С помощью данного приложения пользователи получают медицинские услуги, поддерживают связь с больницей и лечащим врачом, получают назначения и рекомендации по лечению и другое. Кроме того, приложение помогает анализировать запрос пользователя и подобрать наиболее подходящего лечащего врача или больницу. Пользователи могут использовать Baidu Health для того, чтобы получить необходимую медицинскую помощь, не выходя из дома, что делает доступной медицину в КНР даже для самых отдаленных населенных пунктов.

7. Naokan Shipin (好看视频) - платформа для создания и публикации коротких видеороликов. Фактически является аналогом приложения TikTok.

Учитывая количество пользователей и объемы информации, публикуемой на ресурсах Baidu, проблема модерации контента является наиболее актуальной. В этой связи стоит подчеркнуть, что Baidu находится в тесном взаимодействии с государственными структурами. Как отмечается в докладе компании от 2024 года, Baidu «со всей ответственностью подходит к вопросу управления общественно доступным контентом и обеспечения безопасности китайского сегмента Интернета»³¹⁶. Так, только в 2024 году с ресурсов Baidu было удалено около 91 млн единиц недостоверной информации в рамках ручной модерации контента, а также более 59,57 млрд единиц информации в рамках автоматизированных систем модерации контента. Кроме того, за 2023 год системы по обеспечению безопасности и модерации контента Baidu перехватили вредоносный контент более 61,95 млрд раз, а также отследили деятельность мошеннических сайтов почти 80,53 млн раз. Baidu уделяет серьезное внимание защите личных данных: в течение 2024 года конфиденциальная информация пользователей в среднем защищалась 270 тыс раз в день.

Tencent - это один из крупнейших холдингов в Китае, который был основан в 1998 году в Шэньчжэне, где в настоящее время и находится его штаб-квартира. Данная компания занимает лидирующие позиции по ежегодному доходу среди китайских мультимедийных компаний.

Основателем Tencent является Ма Хуатэн, который создавал компанию в качестве провайдера интернет-услуг. Со временем компания начала расширять

³¹⁶ Baidu 2024 Environmental, Social and Governance Report (Отчет Baidu в области экологии, социальной ответственности и корпоративного управления за 2024 год) [Электронный ресурс] // Официальный сайт компании Baidu. URL: <https://esgs.cdn.bcebos.com/2025/04/28/a2/39a2aaa4f728f4e2d0aebaff346c045e.pdf> (дата обращения: 10.06.2025).

свою деятельность и начала разрабатывать различные онлайн-сервисы и приложения. Так, в 2004 году была запущена платформа QQ, которая использовалась для мгновенного обмена сообщениями и обрела популярность среди китайских пользователей. Фактически данный мессенджер заложил основу для создания самого популярного приложения для общения на территории Китайской Народной Республики - WeChat.

Следующим этапом в развитии компании можно считать запуск WeChat (微信) - мессенджера, который является самым популярным на сегодняшний день приложением, используемым китайскими пользователями. Так, WeChat позволяет пользователям свободно обмениваться сообщениями, делиться фото- и видеоматериалами, приобретать авиабилеты, оплачивать покупки и многое другое.

В соответствии с данными ежегодного отчета компании, за 2024 год общая сумма выручки Tencent составила 660 млн долларов юаней. По сравнению с 2023 годом выручка компании увеличилась на 51 млн юаней³¹⁷.

Экосистема Tencent включает в себя мессенджеры, видеоплатформы, игровые сервисы, системы онлайн-банкинга и другое. Так, к основным сервисам, созданным и управляемым компанией, можно отнести:

1. WeChat - социальная сеть, запущенная в 2011 году и позволяющая пользователям обмениваться текстовыми, голосовыми и видео- сообщениями. Кроме того, данная платформа позволяет регистрировать публичные аккаунты для компаний и различных организаций, что делает взаимодействие с аудиторией более эффективным. Подобные публичные аккаунты фактически заменяют сайты. По состоянию на 2024 год общее число уникальных пользователей, зарегистрированных в WeChat, составляет

³¹⁷ Tencent Annual Report 2024 (Годовой отчет компании Tencent за 2024 год) [Электронный ресурс] // Официальный сайт компании Tencent. URL: <https://static.www.tencent.com/uploads/2025/04/08/1132b72b565389d1b913aea60a648d73.pdf> (дата обращения: 06.06.2025).

порядка 1,385 млрд человек³¹⁸. Несмотря на большую распространенность данного приложения среди населения Китайской Народной Республики, ежегодный прирост новых пользователей составляет в среднем 2-3% в год.

Кроме того, в платформу WeChat интегрированы мини-приложения, которые позволяют приобретать авиабилеты, оплачивать налоги, просматривать штрафы за нарушение ПДД. Также в WeChat интегрирована платежная система WeChat Pay, которая позволяет проводить оплату за приобретение товаров и услуг посредством сканирования QR-кода и переводить деньги другим пользователям.

WeChat Pay был запущен в 2013 году Tencent в сотрудничестве с компанией Tenpay. Интерфейс данной платформы позволяет пользователям прикрепить своим банковские карты к счету WeChat Pay и проводить любые транзакции с помощью телефона и аккаунта в WeChat. Услуги WeChat Pay предоставляют не только для жителей КНР: система доступна более чем в 60 странах и регионах и поддерживает проведение операций в 17 валютах³¹⁹.

2. QQ - платформа для обмена мгновенными сообщениями между пользователями на ПК и мобильных устройствах, которая была запущена в 1999 году. Данный мессенджер обладает широким перечнем функций, таких как возможность отправлять текстовые, голосовые и видеосообщения, обмениваться различными файлами, устанавливать игры, создавать групповые чаты и другое. По состоянию на конец 2024 года общее число уникальных пользователей, зарегистрированных в QQ составляет порядка 524 человек³²⁰. С появлением WeChat популярность QQ не уменьшалась, пользователи продолжали пользоваться данной платформой, но с 2021 года число уникальных пользователей мессенджера начало уменьшаться.

³¹⁸ Там же.

³¹⁹ Официальный сайт компании Tencent. Раздел Business [Электронный ресурс]. URL: <https://www.tencent.com/en-us/business.html> (дата обращения: 25.10.2024).

³²⁰ Tencent Annual Report 2024 (Годовой отчет компании Tencent за 2024 год) [Электронный ресурс] // Официальный сайт компании Tencent. URL:

<https://static.www.tencent.com/uploads/2025/04/08/1132b72b565389d1b913aea60a648d73.pdf> (дата обращения: 06.06.2025).

3. Tencent Video - видеохостинг для просмотра потоковых видео. По состоянию на конец 2024 года общее количество пользователей платформы, оформивших платную подписку, составило 113 млн человек³²¹, что делает Tencent Video четвертым в мире по популярности платным стриминговым сервисом после Netflix, Amazon Prime Video и Disney+.

4. Tencent Weishi - платформа для создания и публикации вертикальных оригинальных коротких роликов. Пользователи могут авторизоваться на данной платформе с помощью аккаунта на WeChat или QQ, что упрощает процесс подключения к Tencent Weishi.

5. Tencent News - бесплатная новостная платформа, разработанная компанией Tencent. Его основной целью является предоставление быстрого, объективного и беспристрастного новостного контента. Содержание новостей охватывает не только международную тематику, экономику и спорт, а также и внутригосударственную китайскую повестку, что позволяет пользователям быть в курсе всех последних событий.

Взаимодействие компании Tencent и правительства КНР основывается на соблюдении государственных интересов, строгом регулировании и поддержке со стороны властей. Tencent, будучи одной из крупнейших технологических корпораций Китая, является важным элементом в цифровой экосистеме страны и обязана сотрудничать с правительством в таких областях, как контроль и цензура контента, защита данных и развитие технологий.

В связи с тем, что компания Tencent обладает правами на мессенджеры WeChat и QQ, крупнейшие в КНР по числу пользователей, ее деятельность находится под вниманием государственных органов власти. Деятельность подобных сервисов контролируется государством в целях предотвращения распространения в китайском сегменте Интернета не соответствующей

³²¹ Там же.

действительности информации, которая может повлиять на стабильность общества. Исходя из этого на своих ресурсах компания Tencent обязана:

1. Создать систему цензурирования и фильтрации публикуемого контента, которая отслеживает и удаляет нежелательный контент;
2. Информировать органы власти и соответствующие ведомства обо всех случаях публикации информации, нарушающей законы КНР;
3. Реагировать на принятие государством новых нормативных актов, регулирующих деятельность пользователей в Интернете, и оперативно внедрять в работу платформ новые правила.

Кроме того, Tencent хранит данные всех пользователей на серверах, которые находятся на территории КНР, и в любой момент должна предоставлять к ним доступ по запросу соответствующих государственных ведомств³²².

Компания также принимает активное участие в реализации государственных программ по развитию сферы высоких технологий в КНР. Так, можно выделить проект «Сделано в Китае 2025»³²³ - стратегическую программу, объявленную китайским правительством в 2015 году и направленную на ускорение темпов цифровизации промышленного сектора, укрепление независимости КНР в области технологий. Властями Китайской Народной Республики были обозначены следующие цели реализации данной инициативы:

1. Усовершенствование технологической составляющей промышленного сектора посредством внедрения новых технологических решений, в том числе автоматизации и робототехники.

³²² Su C., Flew T. The Rise of Baidu, Alibaba and Tencent (BAT) and Their Role in China's Belt and Road Initiative (BRI) // *Global Media and Communication*. 2021. Vol. 17, no. 1. P. 75.

³²³ «中国制造 2025» (Программа «Сделано в Китае — 2025») [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/zhengce/zhengceku/2015-05/19/content_9784.htm (дата обращения: 20.11.2024).

2. Обеспечение технологической независимости с целью снижения и последующего отказа от закупки высокотехнологичных товаров из других стран;
3. Стимулирование проведения исследовательских работ в таких сферах как искусственный интеллект, Big Data, Интернет вещей, 5G;
4. Переход на энергосберегающие технологии, которые помогут снизить воздействие деятельности промышленных объектов на экологию.

Основное значение данной программы заключается в необходимости обеспечения долгосрочного устойчивого экономического развития Китайской Народной Республики, преодоления барьеров в технологической сфере, а также ускорения модернизации промышленности.

Компания Tencent принимает активное участие в реализации инициативы «Сделано в Китае 2025», развивая сферу высоких технологий, что соответствует поставленным в рамках программы целям по модернизации промышленности и внедрению высоких технологий в производство. Кроме того, компания реализует проекты по развитию технологий искусственного интеллекта, больших данных и облачных технологий. В рамках реализации программы «Сделано в Китае 2025» можно выделить следующие направления деятельности компании Tencent:

1. Развитие технологий искусственного интеллекта;

Подобные технологии используются компанией Tencent в работе WeChat для анализа данных и автоматизации внутренних процессов, в том числе модерации публикуемого контента. Кроме того технологический гигант активно проводит исследования в таких областях, как естественный язык, компьютерное зрение и анализ больших данных. Исследование и дальнейшее развитие национальных систем, использующих искусственный интеллект, позволит КНР закрепить независимость от западных ИИ-технологий.

2. Облачные хранилища и большие данные;

Одним из наиболее ярких примеров деятельности компании в сфере облачных технологий является одно из подразделений Tencent Cloud, которое развитие различные облачные системы, позволяющие реализовывать цифровую трансформацию в таких сферах, как здравоохранение, финансы и образование. Кроме того, компания Tencent взаимодействует с государственными структурами в вопросе поддержания работоспособности информационных ресурсов и IT-инфраструктуры, принадлежащих государственным ведомствам.

3. Защита персональных данных и обеспечение кибербезопасности;

Процесс интеграции цифровых технологий в сферы экономического и социального развития КНР в настоящее время находится в активной стадии. Так, к концу 2023 года вычислительные мощности дата-центров, расположенных на территории Китайской Народной Республики, выросли почти на 35%³²⁴. В целом, цифровая экономика является важнейшим фактором поддержания экономического роста и создания современной промышленной инфраструктуры на территории всей страны. В частности, правительство КНР предпринимает все меры по интеграции цифровых технологий в обрабатывающую промышленность, созданию цифровых промышленных кластеров и умных цепочек поставок. В данной сфере достаточно высокий уровень дохода обеспечивается за счет систем облачных вычислений, внедрения технологий «Интернета вещей» и строительства дата-центров, обеспечивающих обработку данных. В конце 2023 года в Китае было создано Государственное управление данных КНР, основной задачей которого является стимулирование цифровой трансформации китайского общества и экономики³²⁵.

³²⁴ 东数西算 (Национальный проект по строительству дата-центров «Восточные данные, западные вычисления») [Электронный ресурс] // Baidu Baike. URL: https://baike.baidu.com/item/东数西算/57984771?fr=ge_ala (дата обращения: 26.10.2024).

³²⁵ 国家数据局 (Государственное управление данных КНР) [Электронный ресурс] // Baidu Baike. URL: <https://baike.baidu.com/item/国家数据局/62745119> (дата обращения: 26.10.2024).

В октябре 2023 года Министерство промышленности и информатизации Китайской Народной Республики опубликовало дорожную карту по строительству в стране инфраструктуру для проведения вычислительных операций³²⁶. Так, в рамках реализации данной инициативы планируется увеличить вычислительные мощности КНР более чем в 1.5 раза.

Третьей компанией в БАТ является Alibaba, которая является одним из лидеров в сфере цифровой коммерции и технологий искусственного интеллекта. Alibaba Group была основана в 1999 году предпринимателем Ма Юном (马云) и начинала свою деятельность как платформа для оптовой продажи товаров.

В настоящее время в состав Alibaba входят три крупнейшие онлайн-площадки для электронной коммерции: Taobao, Tmall и Alibaba.com. На каждой из этих площадок предлагается широкий спектр товаров и услуг: от одежды и косметики до авиабилетов и бронирования гостиниц. Компания Alibaba работает в рамках единой экосистемы, объединяющей продавцов, поставщиков и потребителей³²⁷.

Согласно отчету компании, Alibaba является крупнейшей в мире компанией, занимающейся розничной торговлей, по показателям валового товарооборота. Основу бизнеса составляют Taobao, Tmall и другие платформы, гарантирующие компании значительную долю доходов (около 64%)³²⁸.

В 2022 году Alibaba стала самым крупным провайдером облачных услуг на территории Азиатско-Тихоокеанского региона, а также заняла третье место в мире по уровню доходов среди компаний, предоставляющих услуги в сфере облачных технологий. Alibaba Cloud имеет достаточно широкую сеть центров

³²⁶ Официальный сайт Министерства промышленности и информатизации КНР [Электронный ресурс]. URL: <https://www.miit.gov.cn/xwfb/index.html> (дата обращения: 26.10.2024).

³²⁷ Su C., Flew T. The Rise of Baidu, Alibaba and Tencent (BAT) and Their Role in China's Belt and Road Initiative (BRI) // Global Media and Communication. 2021. Vol. 17, no. 1. P. 78.

³²⁸ Alibaba Group Holding Limited Annual Report 2024 (Годовой отчет компании Alibaba Group за 2024 год) [Электронный ресурс] // Официальный сайт компании Alibaba Group. URL: <https://static.alibabagroup.com/reports/fy2024/ar/ebook/EN/14/index.html> (дата обращения: 17.05.2025).

по обработке информации, которые расположены в различных регионах мира, а также сотрудничает с крупными облачными провайдерами из других стран.

Alibaba Cloud предоставляет услуги по вычислениям и облачному хранению данных, машинному обучению, анализу больших данных, интеграции систем искусственного интеллекта, обучению и развертыванию моделей, основанных на ИИ. Также в 2023 году компанией была запущена языковая модель Tongyi Qianwen - система, созданная на основе искусственного интеллекта для обработки и генерирования текстовых документов на основе нейронов сети³²⁹.

В рамках сотрудничества с государством, компания Alibaba реализует масштабный проект Digital County Project по интеграции цифровых технологий в более чем 150 районов КНР. Основной целью проекта является развитие производства и внедрение современных технологий для ускорения экономического роста в сельской местности КНР. К целям проекта Digital County Project можно отнести:

1. Изучение и анализ особенностей местной экономики для того, чтобы выявить потенциальные точки роста;
2. Помощь в продвижении продуктов местного производства через Taobao и Tmall;
3. Строительство инфраструктуры и налаживание логистических путей;
4. Цифровая трансформация процессов в производстве, связанном с сельским хозяйством;
5. Обработка и анализ данных для повышения эффективности функционирования местных предприятий.

³²⁹ Alibaba Opens AI Model Tongyi Qianwen to the Public [Электронный ресурс] // Официальный сайт Reuters. URL: <https://www.reuters.com/business/retail-consumer/alibaba-opens-ai-model-tongyi-qianwen-public-2023-09-13/> (дата обращения: 26.10.2024).

Таким образом, можно сказать, что компании ВАТ (Baidu, Alibaba и Tencent) тесно взаимодействуют с государственными ведомствами в рамках реализации различных государственных инициатив, связанных с цифровизацией экономики, развитием технологий контроля и модерации контента, публикуемого в сети интернет, обеспечением кибербезопасности³³⁰.

Таким образом, государство и крупные цифровые компании в Китае (Baidu, Alibaba, Tencent) демонстрируют модель тесного и эффективного сотрудничества в рамках регулирования интернет-пространства. Взаимодействие основано на общности стратегических целей по развитию национальной цифровой экономики и обеспечению кибербезопасности. Корпорации, пользуясь поддержкой на защищенном рынке, выступают в качестве ключевых партнеров в реализации различных государственных инициатив. Они активно участвуют в развитии инфраструктуры, облачных технологий и систем искусственного интеллекта, способствуя технологическому прогрессу страны. Важным аспектом сотрудничества является совместная работа по поддержанию порядка в информационной сфере. Компании, соблюдая законодательство, внедряют передовые системы модерации контента и защиты данных пользователей, внося значительный вклад в создание безопасной и гармоничной интернет-среды.

3.2. Технологии и инструменты регулирования Интернет-пространства в КНР

В рамках изучения технологий, позволяющих фильтровать информацию, которая появляется в китайском сегменте Интернета, следует отметить проект «Золотой щит». Существование данной программы демонстрирует приверженность властей КНР защите национальных интересов государства также и в информационном пространстве.

³³⁰ Su C., Flew T. The Rise of Baidu, Alibaba and Tencent (BAT) and Their Role in China's Belt and Road Initiative (BRI) // Global Media and Communication. 2021. Vol. 17, no. 1. P. 81.

«Золотой щит» представляет собой систему, которая позволяет изучать большие объемы данных, выявлять информацию, которая не соответствует правилам и нормам поведения граждан в Интернете или распространяет ложные сведения, блокировать ее и анализировать различные источники информации на предмет потенциальных попыток публикации дезинформации. Кроме того, одной из важнейших целей данного проекта обозначалась защита граждан КНР от нежелательной информации, публикуемой из-за рубежа. Данный проект был формально запущен в 1996 году, но его активное функционирование началось в 2008 году³³¹. Наиболее значительным последствием функционирования данной системы стала блокировка на территории КНР доступа к таким социальным сетям и платформам, как Google, Facebook, Twitter, Instagram, WhatsApp, YouTube и другие. За время работы системы «Золотой щит» превратилась в эффективный инструмент контроля публикуемой в сети Интернет информации, который включает в себя как ручную работу модераторов, так и применение искусственного интеллекта для более точной и быстрой обработки информации и выявления проблемных факторов.

Проект «Великий щит» также называют «Великий Файрвол» (Great Firewall) - это название было дано западными СМИ запущенной КНР системе в 1997 году. Данный проект включает в себя информационную систему по управлению безопасностью, криминальные базы данных, системы по контролю миграции, а также информационную систему по контролю дорожного движения. Реализация проекта по созданию общегосударственной системы сетевой безопасности была инициирована Центральной комиссией по делам киберпространства КНР. Идеи о создании подобной системы начали появляться с 1994 года, когда Китай был подключен к глобальной сети Интернет, с помощью которой среди граждан начали активно распространять информацию,

³³¹ The Cybersecurity Act and the National Security Review System [Электронный ресурс] // People's Daily Online. URL: <http://theory.people.com.cn/n1/2016/0622/c40531-28469973.html> (дата обращения: 03.11.2024).

которая могла создать вызовы для общественной стабильности, а также западные идеологии, угрожающие национальному суверенитету Китайской Народной Республики.

В рамках изучения проекта «Золотой щит» можно выделить два основных этапа в его создании и дальнейшем формировании:

1. Этап 1 (1998-2006 гг.). Создание трехуровневой сети связи, баз данных и платформы общего пользования. В рамках первого этапа была заложена база для создания инфраструктуры и технологических решений, которая позволит превратить проект «Золотой щит» в эффективный инструмент по формированию национального сегмента сети Интернет в КНР.
2. Этап 2 (2006-2008 гг.). Строительство инфраструктуры, позволяющей обслуживать ежедневную работу системы «Золотой щит», включающую обработку большого объема данных и их анализ. Кроме того, происходило расширение информационных центров в центральных и западных провинциях КНР. Для эффективной и бесперебойной операционной деятельности системы были подключены операторы сотовой связи и провайдеры Интернета. Таким образом, с завершением второй фазы строительства проект «Золотой щит» стал намного более эффективно модерировать информацию в сети Интернет, удалять ложные сведения и блокировать ресурсы, распространяющие дезинформацию или информацию, которая противоречит законам КНР³³².

После того, как система «Золотой щит» была запущена, основная ее задача заключалась в блокировании нежелательных доменных имен и IP-адресов, а также в отсеивании действий пользователей, нарушающих законы. Для этого в точках доступа к Интернету через провайдеров было установлено специальное программное обеспечение, позволяющее проводить мониторинг

³³² 金盾工程 (Проект «Золотой щит») [Электронный ресурс] // Baidu Baike. URL: <https://baike.baidu.com/item/%E9%87%91%E7%9B%BE%E5%B7%A5%E7%A8%8B/9092338> (дата обращения: 03.11.2024).

информации, появляющейся в Интернете. Кроме того, например, пользователям интернет-кафе необходимо было предоставлять личные данные для того, чтобы пользоваться сетью и получить к ней доступ³³³. Провайдеров интернет-услуг (ISP) обязали проверять личные данные всех пользователей. Также начала становиться распространенной практика регистрации в различных мобильных приложениях только при предъявлении удостоверения личности гражданина КНР.

Вторым важным инструментом в работе системы «Золотой щит» стала система цензуры, которая была основана на фильтрации ключевых слов, появляющихся в сети Интернет. Работа данной системы подразумевает анализ содержимого тех сайтов, которые посещают пользователи, даже в том случае, если были использованы прокси-серверы. Если система обнаруживает «чувствительный контент», то доступ к данному сайту становится недоступен в связи с автоматической блокировкой подключения через сброс протокола TCP (протокол управления передачей). Примерами слов или словосочетаний, которые система относит к «чувствительному контенту» могут служить: «призывы чиновников», «незаконное задержание», «действия по преследованию», «антикоммунистические настроения»³³⁴.

В процессе улучшения работы системы «Золотой Щит» особое внимание уделялось борьбе с инструментами, которые позволяли обходить блокировки и получать доступ к заблокированным ресурсам. Особенно активно китайские власти боролись с VPN-сервисами³³⁵. Так, проводился анализ уязвимых факторов в различных VPN-протоколах (например, IPSec, L2TP/IPSec, PPTP),

³³³ Introduction on the Golden Shield [Электронный ресурс] // China.org.cn. URL: <http://www.china.org.cn/chinese/zhuanti/283732.htm> (дата обращения: 23.05.2023).

³³⁴ Hounsel A., Mittal P., Feamster N. Automatically Generating a Large, Culture-Specific Blocklist for China [Электронный ресурс] // 8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18). USENIX Association, 2018. URL: <https://www.usenix.org/system/files/conference/foci18/foci18-paper-hounsel.pdf> (22.07.2023).

³³⁵ How China Built the Great Firewall and How It Works [Электронный ресурс] // WeChat. URL: <https://mp.weixin.qq.com/s/J-NJm9we3q0zhLL0IzyMAA> (дата обращения: 11.09.23).

проводилось изучение характерных особенностей VPN-сервисов (например, работа через специфические порты), определялся след зашифрованных соединений и другое. Кроме того, в Китае проводилась активная блокировка доступа к популярным VPN-сервисам (например, таким как Free VPN, Green VPN, Jiguang VPN, Tianxing VPN и другие)³³⁶. Борьба с незаконными VPN-сервисами велась не только на уровне блокировки программного обеспечения, но также и на законодательном уровне: принимались нормативные акты, направленные против использования гражданами VPN-сервисов, а также против анонимности в сети Интернет. Условия пользования VPN-платформами на территории КНР постепенно добавлялись в редакцию Закона «Об управлении компьютерными информационными сетями, подключенными к международной сети в КНР». Так, с 2018 года пользование VPN-сервисами, которые функционируют без официального разрешения, были объявлены незаконными³³⁷.

Кроме того, 22 января 2017 года Министерством промышленности и информационных технологий КНР (МИИТ) было опубликовано заявление «Уведомление Министерства промышленности и информационных технологий о регулировании рынка услуг доступа к сети Интернет», в котором указывалось, что использование ресурсов, позволяющих проводить трансграничную деятельность, является нелегальным и рынок интернет-услуг должен регулироваться государственными ответственными органами³³⁸. Целью публикации данного документа и дальнейших действий Министерства являлась

³³⁶ Zhipeng Z. et al. VPN: A Boon or a Trap? A Comparative Study of MPLS, IPSec, and SSL Virtual Private Networks // 2018 Second International Conference on Computing Methodologies and Communication (ICCMC). Erode, 2018. P. 512.

³³⁷ China Moves to Block Internet VPNs from 2018 [Электронный ресурс] // Официальный сайт The Guardian. URL: <https://www.theguardian.com/world/2017/jul/11/china-moves-to-block-internet-vpns-from-2018> (дата обращения: 13.02.2024).

³³⁸ 工业和信息化部关于清理规范互联网网络接入服务市场的通知 (Уведомление Министерства промышленности и информатизации КНР о наведении порядка и регулировании рынка услуг доступа к интернет-сетям) [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: https://www.cac.gov.cn/2017-01/23/c_1120366809.htm (дата обращения: 03.11.2024).

борьба с незаконной деятельностью в сфере оказания услуг подключения к Интернету, в том числе деятельность центров обработки данных (IDC), Интернет-провайдеров (ISP), а также центров доставки контента (CDN). В рамках данного заявления было утверждено, что предоставление услуг VPN-каналов должно проводиться исключительно посредством получения специального разрешения от надземных органов.

Провайдеры, обеспечивающие подключение к сети Интернет, должны регистрировать и обеспечивать хранение данных пользователей, в том числе время подключения к сети и IP-адреса, с которых было зафиксировано подключение.

В заявлении, опубликованном Министерством промышленности и информационных технологий КНР также уточняются условия, при которых пользование VPN-сервисами допустимо. Так, например, в документе речь идет о деятельности международных компаний. Как отмечается, «международным компаниям, чья внутренняя операционная деятельность предполагает подключение к внешним источникам, разрешено использовать VPN-сервисы, но только при условии получения специальных разрешений и сертификатов от соответствующих органов». В заявлении подчеркивается, что подобные компании должны соблюдать законодательство КНР, регулирующее деятельность граждан в сети Интернет, а также использовать VPN-каналы исключительно в корпоративных целях. Первая кампания, направленная на очистку рынка предоставления интернет-услуг на территории КНР, продлилась до 31 марта 2018 года. Так, некоторые СМИ писали о случаях ареста граждан КНР по делам, связанным с использованием VPN-сервисов и попыткой продажей доступа к ним. Например, в декабре 2017 года, как пишет South China Morning Post, мужчину из южного Китая приговорили к 5,5 годам тюремного заключения, а также назначили штраф в размере 500 тыс юаней за продажу

доступа к VPN-платформе без наличия лицензии, разрешающей заниматься подобной деятельностью³³⁹.

В рамках изучения механизмов цензуры в современном Интернет-пространстве КНР стоит так отметить, что в китайском Интернете существует темы, обсуждение которых запрещено. Так, например, к таким темам можно отнести сепаратизм, проблема независимости Тибета и Синьцзян-Уйгурского автономного района, права мусульман в Китае, протесты на площади Тяньаньмэнь в 1989 году, движение «Фалуньгун» и другие³⁴⁰.

Кроме того, по информации Интернет-проекта China Digital Times, список слов, упоминание которых запрещено в китайском сегменте Интернета, составляет порядка 3,5 тысяч единиц и пополняется на постоянной основе³⁴¹. К таким словам можно отнести: «культурная революция», «культ личности», «унаследовать престол», «не согласен», «рабовладельческий строй», «1984».

Интересным примером словосочетания, которое нельзя активно употреблять в переносном значении в сообщениях в цифровом пространстве КНР, является «регистрация на рейс». Это связано с тем, что фраза «регистрация на рейс» (登机) звучит идентично словосочетанию «унаследовать престол» (登基).

Большое количество запретов на использование тех или иных слов и словосочетаний привели к тому, что пользователи начали использовать метафоры, сравнения, эвфемизмы и других обороты речи для того, чтобы

³³⁹ Man Jailed for Selling VPNs to Evade China's 'Great Firewall' [Электронный ресурс] // Официальный сайт газеты South China Morning Post. URL: <https://www.scmp.com/news/china/policies-politics/article/2109618/man-jailed-selling-vpns-evade-chinas-great-firewall> (дата обращения: 04.11.2024).

³⁴⁰ Люлина А.Г., Ефименко Е.С. Интернет-цензура в современном Китае: жесткий контроль и гибкая система урегулирования // Вестник Российского университета дружбы народов. Серия: Всеобщая история. 2022. Т. 14, № 2. С. 180.

³⁴¹ Sensitive Words [Электронный ресурс] // Официальный сайт China Digital Times. URL: <https://chinadigitaltimes.net/china/sensitive-words/> (дата обращения: 04.11.2024).

высказывать свое мнение по темам, обсуждение которых в китайском Интернете недопустимо³⁴²³⁴³.

В 2013 году американские специалисты, изучающие цензуру в КНР, провели эксперимент, в рамках которого пользователи из различных стран публиковали сообщения и оставляли комментарии на различные темы в китайских социальных сетях, а затем было проанализировано, какие из публикаций были заблокированы, какие допущены к публикации, а какие сообщения были отредактированы. Результатом данного эксперимента стало наблюдение, согласно которому сообщения, содержащие критику руководства КПК, почти не подвергались удалению, а вот сообщения с призывом объединяться по какой-либо общей проблеме, были заблокированы³⁴⁴. Авторы эксперты сделали вывод, что основной целью реализации политики цензуры в информационном пространстве, является не попытка изолировать пользователей от источников информации, а контроль конкретных тем, обсуждение которых может привести к дестабилизации ситуации в обществе, а также коллективным действиям со стороны некоторых граждан.

К одной из тем, обсуждение которых контролируется китайскими властями особым образом, является тема Вооруженных сил КНР, а также китайских военнослужащих. В июне 2021 года Министерством по делам ветеранов КНР был опубликован «Закон КНР о защите статуса, прав и законных интересов военнослужащих»³⁴⁵.

³⁴² Rudolph J. Sensitive Words: Xi to Ascend His Throne [Электронный ресурс] // China Digital Times. URL: <https://chinadigitaltimes.net/2018/02/sensitive-words-emperor-xi-jinping-ascend-throne/> (дата обращения: 20.11.2024).

³⁴³ Нуриева Л.Ф. Цензура и способы ее «обхода» в современной прессе Китайской Народной Республики // Modern Oriental Studies. 2019. № 2. С. 13.

³⁴⁴ King G., Pan Jennifer, Roberts M.E. Reverse-Engineering Censorship in China: Randomized Experimentation and Participant Observation [Электронный ресурс] // Science. 2014. Vol. 345, no. 6199. Article 1251722. URL: https://gking.harvard.edu/files/gking/files/experiment_0.pdf (дата обращения: 07.11.2024).

³⁴⁵ 中华人民共和国军人地位和权益保障法 (Закон КНР «О защите статуса, прав и законных интересов военнослужащих») [Электронный ресурс] // Официальный сайт Министерства по делам ветеранов КНР. URL: https://www.mva.gov.cn/sy/xx/bnxx/202106/t20210611_48036.html (дата обращения: 20.11.2024).

В соответствии с данным документом честь и репутация военнослужащих КНР защищены законом, а их очернение или оскорбление незаконны. В законе подчеркивается важность уважения к заслугам военных, а также к историческому прошлому КНР в целом. В отношении граждан, действия которых будут направлены против военных, затрагивают их честь и достоинство, оказывают негативное влияние на несение военными службы или создают условия для нарушения общественного порядка, будут подаваться иски от народных прокуроров.

Примером, продемонстрировавшим действие данного закона, стала ситуация, связанная с выходом в 2021 году в прокат исторического фильма «Битва при Чосинском водохранилище» (长津湖), который повествует о действиях китайских добровольцев, оказавших поддержку северокорейским солдатам в сражении против американских войск в период Корейской войны. После выхода в прокат данного фильма один гражданин КНР опубликовал сообщение, в котором усомнился в правильности действий китайских властей по оказанию помощи корейским войскам. Таким образом он поставил под сомнение решения, которые были приняты китайским руководством во время сражения при Чосинском водохранилище. После того, как данное сообщение было опубликовано, Центральное телевидение КНР подготовило сюжет об исторической памяти среди граждан Китая, необходимости помнить и чтить заслуги героев войн и не придавать сомнению действия китайского руководства в различные исторические периоды³⁴⁶. После этого сообщение данного гражданина было удалено, а аккаунт заблокирован.

Исходя из механизмов и алгоритмов функционирования цензуры в китайском сегменте Интернета можно сделать вывод о том, что самой острой и

³⁴⁶ Люлина А.Г., Ефименко Е.С. Интернет-цензура в современном Китае: жесткий контроль и гибкая система урегулирования // Вестник Российского университета дружбы народов. Серия: Всеобщая история. 2022. Т. 14, № 2. С. 183.

наиболее часто подвергаемой ограничениям темой для обсуждения является коллективная деятельность граждан: митинги, собрания, выступления, демонстрации и прочее. При этом не столь важно, что является основной целью проведение подобных коллективных мероприятий: критика государственно власти или, наоборот, ее поддержка³⁴⁷.

Важно подчеркнуть, что степень цензуры в китайском сегменте Интернета определяется и в зависимости от временного признака и тех политических событий, которые происходят в конкретный период на территории КНР. Особенно активно система цензуры в Китае начинает функционировать накануне, во время и после мероприятий государственного масштаба (съезд КПК, сессии Всекитайского собрания народных депутатов (ВСНП) и пр.), годовщин событий, имеющих историческую значимость для народа КНР, а также напоминающих о социальной нестабильности. К подобным событиям можно отнести: событие на площади Тяньаньмэнь 4 июня 1989 г., вооруженное сопротивление тибетцев против китайских властей в 1959 г., процентное движение последователей Фалуныгун в 1999 г.

Таким образом, в дни, когда отмечаются годовщины определенных исторических событий или в КНР проходят важные политические или партийные мероприятия, любые сообщения в Интернете, в которых есть упоминание запрещенных тем, будут автоматически удаляться. Исключением могут быть сообщения СМИ или любых других официальных источников, опубликованные в китайских социальных сетях или платформах. Иногда, если ситуация требует принятия более жестких мер, власти прибегают к полному отключению Интернета.

Так, например, во время протестных движений граждан в Синьцзян-Уйгурском автономном районе в июле 2009 года для того, чтобы

³⁴⁷ King G., Pan Jennifer, Roberts M.E. Reverse-Engineering Censorship in China: Randomized Experimentation and Participant Observation // Science. 2014. Vol. 345, no. 6199. P. 891.

стабилизировать ситуацию, властями было принято решение о полном отключении Интернета во всем автономном районе. Частично подключение к Интернету было восстановлено в конце 2009 года, а полный доступ ко всем онлайн-сервисам и ресурсам на территории СУАР был возобновлен только 14 Мая³⁴⁸.

Следует отметить, что механизмы регулирования информационного пространства в КНР зависят и от регионального фактора: уровень жесткости цензуры в Интернете отличается в разных провинциях и районах страны. Так, наиболее жесткие условия по пользованию Интернетом и ограничения по доступу к информации применяются в СУАР и Тибетском автономном районе.

Эксперты в сфере контроля Интернета подчеркивают, что цензура в китайском сегменте Интернета значительно усилилась после того, как в 2013 году пост председателя КНР занял Си Цзиньпин. По словам директора американского представительства Reportes Without Borders Д. Хэлганда, правительство Си Цзиньпина ужесточило меры по контролю информации, публикуемой в Интернете, особенно в отношении новостных источников, а также кибердиссидентов³⁴⁹.

3.3. Перспективы развития информационной политики КНР в контексте внешних угроз

Развитие информационной политики Китая играет ключевую роль в оптимизации процессов государственного управления, обеспечивая эффективное функционирование государственных институтов, повышение прозрачности и доступности государственных услуг, а также стимулирование инноваций и экономического роста. Кроме того, одним из наиболее важных

³⁴⁸ After Long Ban, Western China Is Back Online. Официальный сайт газеты New York Times. Электронный ресурс. URL: <https://www.nytimes.com/2010/05/15/world/asia/15china.html>. (дата обращения: 02.11.2024).

³⁴⁹ Statement by D. Halgand, US Director, Reporters Without Borders. Электронный ресурс. URL: <http://www.uscc.gov/sites/default/files/HalgandWritten%20Testimony.pdf> (дата обращения: 02.11.2024).

аспектов реализации информационной политики является обеспечение общественной и политической стабильности внутри страны, что также является фундаментом для технологического развития государства.

В центре внимания государственной информационной политики в ближайшее время будет оставаться контроль деятельности граждан в сети Интернет. Как отмечали СМИ, в июле 2024 года Администрация киберпространства КНР совместно с Министерством общественной безопасности предложила внедрение цифровых идентификаторов для пользователей интернета³⁵⁰. Введение обязательных цифровых идентификаторов предполагает, что каждый пользователь интернета в Китае должен будет зарегистрировать свою личность при доступе к онлайн-сервисам, таким как социальные сети, онлайн-платформы и другие интернет-услуги. В настоящее время не все онлайн-ресурсы на территории КНР требуют обязательной регистрации по документам. Эти идентификаторы, изначально предполагаемые как добровольные, могут значительно расширить возможности правительства по мониторингу онлайн-деятельности граждан.

Одним из направлений развития информационной политики КНР в ближайшее время будет являться электронное правительство. Так, несмотря на активное использование информационных технологий в рамках оказания государственных услуг, их цифровизация еще не выполнена в полной мере. В ближайшие годы КНР продолжит расширение спектра оказываемых в онлайн-формате государственных услуг, включая более масштабную интеграцию информационных услуг в сферу налогового документооборота, регистрации юридических лиц, получение медицинской документации и прочее. Кроме того, в работу государственных органов власти будут постепенно интегрироваться

³⁵⁰ China's Data Watchdog Plans Tighter Control of Internet Users [Электронный ресурс] // Официальный сайт газеты Financial Times. URL: <https://www.ft.com/content/63f2e491-e015-4cae-bb35-f4c447c595f1> (дата обращения: 14.12.2024).

технологии искусственного интеллекта для работы с большими данными, их эффективной обработки и повышения качества оказываемых гражданам услуг. Также искусственный интеллект может применять для обработки запросов, поступающих от граждан, автоматической работы с документами и принятия решений на основе данных по подобным запросам, что поможет ускорить процесс оказания государственных услуг гражданам. Как подчеркнул заместитель Генерального секретаря ООН по экономическим и социальным вопросам Ли Цзюньхуа, «цифровое правительство должно стать мощным катализатором для более справедливого и процветающего мира»³⁵¹. Развитие систем электронного правительства в КНР демонстрирует стремление китайских властей учитывать основные мировые тенденции в развитии информационных технологий.

Кроме того, власти КНР активно развивают концепцию «умных городов», где системы электронного правительства будут объединены с городской инфраструктурой, что позволит создать единый центр по контролю за ключевыми процессами жизнедеятельности города. Это включает использование «Интернета вещей» (Internet of Things) для управления работой транспортной системы, энергоснабжения, медицинских учреждений и прочее. Развитие умных городов на территории КНР имеет прямую связь со стратегическими целями центрального правительства и государственной поддержкой реализации подобных инициатив. Так, например, в 2020 году во время своего визита в провинцию Чжэцзян Си Цзиньпин заявил, что для создания «умных городов» важно активно использовать современные

³⁵¹ Исследование ООН: Электронное правительство 2024. Ускорение цифровой трансформации для устойчивого развития. С дополнением об искусственном интеллекте [Электронный ресурс] // Официальный сайт ООН. Департамент ООН по экономическим и социальным вопросам. С. 155. URL: <https://desapublications.un.org/sites/default/files/publications/2025-01/E-Government%20Survey%202024%20RUS-compressed.pdf> (дата обращения: 02.02.2025).

технологии, такие как большие данные, облачные вычисления и блокчейн³⁵². Он также отметил, что необходимо разрабатывать интеллектуальные инфраструктуры, которые смогут эффективно управлять ресурсами городов и улучшать качество жизни их жителей.

В апреле 2017 года Госсоветом КНР было объявлено о создании нового района Сюаньань (провинция Хэбэй), который был представлен как проект образцового «умного города»³⁵³. Проект направлен на создание инновационной городской инфраструктуры с использованием современных технологий, таких как искусственный интеллект, Интернет вещей и системы мониторинга для эффективного управления городскими ресурсами, включая водоснабжение, электроснабжение и транспорт. Проект будет реализовываться поэтапно, с внедрением различных технологических решений на каждом этапе. Ожидается, что Сюаньань станет моделью для создания умных, экологически чистых и устойчивых городов как в Китае, так и за его пределами³⁵⁴.

Одним из первых документов, регламентирующих деятельность государства по созданию «умных городов» стал «Четырнадцатый пятилетний план (2021-2025)»³⁵⁵. В данном документе подчеркивается, что строительство умных городов должно основываться на технологических достижениях Китая, но в то же время использовать технологии, позволяющие добиться энергоэффективности и снижения углеродного следа. Как отмечается, подобные проекты должны реализовываться в том числе с помощью сетей 5G, а также

³⁵² Xi Calls for Making Major Cities “Smarter” [Электронный ресурс] // Официальный сайт агентства «Синьхуа». URL: http://www.xinhuanet.com/english/2020-04/01/c_138937389.htm (дата обращения: 02.12.2024).

³⁵³ 雄安新区智能建造试点城市实施方案 (План реализации пилотного проекта по созданию города интеллектуального строительства в новом районе Сюаньань) [Электронный ресурс] // Официальный сайт нового района Сюаньань. URL: https://www.xiongan.gov.cn/2023-03/01/c_1211734232.htm (дата обращения: 03.12.2024).

³⁵⁴ 雄安新区智能城市数据标准体系指南 (Руководство по системе стандартов данных умного города в новом районе Сюаньань) [Электронный ресурс] // Официальный сайт нового района Сюаньань. 28 с. URL: https://www.xiongan.gov.cn/1210959746_16097396796461n.pdf (дата обращения: 02.12.2024).

³⁵⁵ 中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要 (План национального экономического и социального развития КНР на 14-ю пятилетку и перспективные цели до 2035 г.) [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/xinwen/2021-03/13/content_5592681.htm (дата обращения: 02.12.2024).

технологий больших данных (Big Data). В данном контексте сети 5G позволяют обеспечить быструю и стабильную связь, которая является основой функционирования приложений для управления городскими процессами: умный транспорт, телемедицина и прочее. Так, например, в китайском городе Шэньчжэнь реализацию получила система умного транспорта, которая позволяет оптимизировать работу общественного транспорта в режиме реального времени на основе обычных данных³⁵⁶. Кроме того, Шэньчжэнь стал первым в мире городом, в котором покрытие сетей 5G достигло 100 процентов: сети нового поколения доступна на территории всего города³⁵⁷.

Несмотря на большие успехи в рамках строительства «умных городов» на территории Китайской Народной Республики власти страны сталкиваются с некоторыми сложностями. Так, например, к одной из подобных проблем является вопрос стандартизации технологических решений: в условиях быстрого развития технологий требуется принятие единого стандарта для различных устройств, которые применяются при строительстве и эксплуатации «умных городов». Так, в Китае есть большое число производителей, которые предлагают решения для городского управления, однако на практике платформы, системы и механизмы, предполагаемые различными компаниями, могут быть несовместимы между собой. Таким образом, в некоторых ситуациях одну и ту же технологию нельзя применить в двух разных населенных пунктах, что создает барьеры для масштабирования подобных «умных решений» на территории всей страны.

Другим важным вызовом в рамках реализации проектов «умный город» являются вопросы информационной безопасности в сети и защиты

³⁵⁶ Ли Ино. Исследование современного состояния и тенденций будущего строительства умных городов в Китае // Современная Азия: политика, экономика, общество. 2024. № 3. С. 79.

³⁵⁷ Chinese Tech Hub Shenzhen Says It's the First City in the World to Have Full Stand-Alone 5G Coverage [Электронный ресурс] // Официальный сайт газеты South China Morning Post. URL: <https://www.scmp.com/abacus/tech/article/3097815/chinese-tech-hub-shenzhen-says-its-first-city-world-have-full-stand> (дата обращения: 02.12.2024).

конфиденциальной информации. С увеличением количества используемых устройств и носителей, расширением сети и доступа к ней, растет и риск хакерских атак, а также утечки личной информации³⁵⁸. В свою очередь, подобные кибератаки и утечки данных создают не только угрозы для безопасности граждан и функционирования городских систем, но и для политической стабильности в стране, обеспечение которой является одной из главных задач реализации информационной политики в КНР. Важным шагом в данном направлении будет являться создание и унификация нормативов, направленных на защиту городских систем от кибератак, а также их интеграция в качестве инструментов действующей информационной политики. Такой подход позволит повысить уверенность граждан в безопасности пользования государственными цифровыми сервисами.

Еще одним вызовом при реализации проектов по строительству «умных городов» на территории Китая является различие в экономическом развитии различных городов, провинций и регионов, что может создавать трудности в процессе реализации идентичных проектов в различных населенных пунктах. При строительстве «умных городов» необходимо учитывать географические и инфраструктурные особенности того или иного населенного пункта.

В ближайшее время одной из важнейших тенденций при создании «умных городов» будет являться расширение вовлеченности граждан в процессы управления городом. Основной целью подобных мер является создание прозрачных, инклюзивных и ориентированных на граждан городов. Активное участие граждан в различных процессах, связанных с принятием решений, позволит укрепить демократичность принятия решений по тем или иным вопросам и повысить лояльность граждан к властям. Подобный подход не

³⁵⁸ Ли Ино. Исследование современного состояния и тенденций будущего строительства умных городов в Китае // Современная Азия: политика, экономика, общество. 2024. № 3. С. 78.

только направлен на повышение качества имплементируемых решений, но и формированию чувства общности и работы «рука об руку» с городскими властями. В таком обществе риск возникновения дестабилизирующих факторов, способных оказать негативное влияние на отношений граждан к власти или привести к возникновению процентных настроений, сводится к минимуму.

Кроме того, в будущем «умные города» будут все теснее интегрированы с технологиями искусственного интеллекта, которые помогут оптимизировать процессы по обработке и анализу дынных, принятию решений и обеспечению бесперебойной работы всех городских систем.

Анализируя возможные тенденции развития государственной информационной политики КНР, следует также отметить планы по укреплению научно-технического потенциала, который является фундаментом для эффективной реализации государственных решений, в том числе и в информационном пространстве. В данной связи искусственный интеллект и новые технологии станут основой для реализации различных аспектов информационной политики Китая. В 2017 году Госсовет КНР опубликовал "**План развития искусственного интеллекта нового поколения**", в котором ставится цель занять лидирующие позиции в области ИИ к 2030 году³⁵⁹. В рамках этого плана страна будет направлять значительные средства на поддержку научных исследований, создание инфраструктуры для ИИ и стимулирование создания коммерческих приложений, использующих данные технологии. Ключевые направления плана:

1. **Научные исследования и технологии:** Продолжение исследований в области ИИ, таких как машинное обучение, обработка естественного языка и компьютерное зрение.

³⁵⁹ «新一代人工智能发展规划» (План развития искусственного интеллекта нового поколения) [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm (дата обращения: 03.12.2024).

2. **Инфраструктура:** Создание платформ для интеграции ИИ в различные отрасли, включая «умные» города, промышленность и здравоохранение.
3. **Нормативная база:** Разработка стандартов и этических норм для применения ИИ, с учетом вопросов конфиденциальности и безопасности данных.
4. **Кадры:** Образование и подготовка специалистов для работы в сфере ИТ и ИИ.
5. **Экономика и общество:** ИИ должен стать драйвером экономического роста и повышения качества жизни, модернизируя производство и улучшая социальные услуги.
6. **Международное сотрудничество:** Китай активно будет сотрудничать с другими странами и участвовать в международных инициативах по развитию ИИ.
7. **Этапы реализации:** К 2020 году планируется создание исследовательских и технологических платформ, к 2025 году Китай должен занять лидерские позиции в ИИ, а к 2030 году стать мировым лидером.

Китайское руководство прикладывает большие усилия для достижения планов по завоеванию лидерских позиций на рынке ИИ-технологий. Так, примером эффективной политики КНР в рамках развития технологий искусственного интеллекта на территории страны может послужить успех чат-бота на основе искусственного интеллекта от китайской компании Deepseek³⁶⁰. Компания запустила сайт и приложение 10 января 2025 года и уже к 27 января приложение Deepseek стало самым скачиваемым бесплатным приложением в магазине App Store в США и ряде других стран³⁶¹. До этого момента

³⁶⁰ Официальный сайт чат-бота DeepSeek [Электронный ресурс]. URL: <https://www.deepseek.com/> (дата обращения: 12.11.2025).

³⁶¹ China's DeepSeek AI Dethrones ChatGPT on App Store: Here's What You Should Know [Электронный ресурс] // Официальный сайт телеканала CNBC. URL: <https://www.cnbc.com/2025/01/27/chinas-deepseek-ai-tops-chatgpt-app->

лидирующую позицию занимал ChatGPT - чат-бот с генеративным искусственным интеллектом, разработанный американской компанией OpenAI. Стартап DeepSeek был основан в 2023 году в Ханчжоу и стала первой китайской компанией, занимающейся искусственным интеллектом, которая составила конкуренцию американскому Open AI. Как отмечали СМИ, после того, как приложение DeepSeek заняло лидирующие позиции по смачивания, стоимость акций американских технологических компаний обрушилась на \$1 трлн за один день³⁶². Одной из причин успеха китайского приложения стало то, что доступ к нему совершенно бесплатный. Кроме того, создание чат-бота DeepSeek и обучение модели обошлось в \$5,6 млн, тогда как в США разработка нейросети стоит от \$100 млн до \$1 млрд. Таким образом, можно сделать вывод о том, что

Китай будет продолжать инвестировать денежные средства в исследования искусственного интеллекта как для поддержания своей конкурентоспособности на международной арене, так и для повышения эффективности реализуемой им внутренней политики, в том числе и в информационной сфере.

В ответ на растущие угрозы в киберпространстве Китай продолжит усиливать меры по защите данных и обеспечению кибербезопасности. Развитие новых технологий для защиты информации и борьбы с киберугрозами будет играть важную роль в национальной безопасности. Председатель КНР Си Цзиньпин неоднократно подчеркивал, что кибербезопасность имеет тесную связь с национальной безопасностью и оказывает влияние на все сферы жизни, включая политику, экономику и культуру. Кроме того, китайский лидер отмечал, что «без сетевой безопасности не может быть национальной безопасности; если мы не сможем пройти испытание Интернетом, мы не

store-what-you-should-know.html (дата обращения: 27.01.2025).

³⁶² AI-Fueled Stock Rally Dealt \$1 Trillion Blow by Chinese Upstart [Электронный ресурс] // Официальный сайт агентства Bloomberg. URL: <https://www.bloomberg.com/news/articles/2025-01-27/nasdaq-futures-slump-as-china-s-deepseek-sparks-us-tech-concern> (дата обращения: 27.12.2025).

сможем пройти испытание долгосрочным управлением»³⁶³. Как подчеркивало неоднократно руководство КНР, в новой эпохе, в ближайшее время информационная безопасность и цифровизация будут являться важнейшими задачами для КПК, ориентированными на развитие страны, укрепление национальной безопасности и повышение благосостояния народа³⁶⁴.

Введение законов, направленных на защиту персональных данных, также будет одним из приоритетов: Китай продолжит регулировать использование данных, внедряя строгие меры по защите частной информации и предотвращению утечек данных.

В рамках реализации государственной информационной политики власти КНР продолжают контролировать информацию в сети Интернет, усиливая цензуру в социальных сетях, новостных платформах и других онлайн-ресурсах. Введенные ограничения и блокировки иностранных платформ (таких как Google, Facebook и Twitter) останутся в силе, с акцентом на дальнейшее развитие внутренних интернет-сервисов.

Китай будет продолжать регулировать медиа-пространство, укрепляя государственные средства массовой информации и повышая их роль в информационной политике страны. При этом будет сохраняться поддержка культурной политики, направленной на укрепление китайской идеологии в интернете.

Стратегия пропаганды и контроля за СМИ будет оставаться одной из важнейших задач для китайского правительства.

³⁶³ 习近平总书记关于网络安全部分论述 (Некоторые высказывания генерального секретаря Си Цзиньпина о кибербезопасности) [Электронный ресурс] // Официальный сайт Комитета по контролю и управлению государственными активами г. Уху. URL: <https://gzw.wuhu.gov.cn/ztl/qmgjaqjy/8595229.html> (дата обращения: 03.12.2024).

³⁶⁴ 习近平对网络安全和信息化工作作出重要指示 (Си Цзиньпин дал важные указания по работе в области кибербезопасности и информатизации) [Электронный ресурс] // Официальный сайт агентства «Синьхуа». URL: http://www.news.cn/politics/leaders/2023-07/15/c_1129751651.htm (дата обращения: 04.12.2024).

Таким образом, информационная политика Китая в ближайшие годы будет направлена на усиление внутреннего контроля, развитие высоких технологий, укрепление кибербезопасности, а также на продвижение китайских цифровых инициатив на международной арене.

* * *

Таким образом, по итогам анализа взаимодействия государства и цифровых корпораций, технологий регулирования интернет-пространства и перспектив информационной политики КНР выявлены ключевые особенности китайской модели управления цифровой средой.

Установлено, что государство и крупнейшие IT-компании (Baidu, Alibaba, Tencent) функционируют в рамках тесного партнерства, при котором корпорации выступают инструментом реализации государственной политики и контроля информационного пространства.

Показано, что регулирование интернет-пространства основано на сочетании технологических и административных механизмов (включая систему «Золотой щит»), направленных прежде всего на предотвращение социальной дестабилизации, а не на полную изоляцию информации.

Выявлено, что дальнейшее развитие информационной политики КНР будет связано с усилением цифрового контроля, внедрением искусственного интеллекта и развитием цифровых государственных сервисов.

Таким образом, китайская модель управления интернет-пространством представляет собой централизованную и технологически развитую систему, ориентированную на обеспечение политической стабильности и национальной безопасности в условиях цифровизации.

Заключение

Современный этап мирового технологического развития характеризуется активной цифровизацией, оказывающей существенное влияние на информационные потоки, коммуникацию и подходы к государственному регулированию. В этой связи государственная информационная политика, в частности политика по регулированию интернет-пространства, может рассматриваться в качестве важнейшего инструмента для сохранения национального суверенитета, управления данными, а также обеспечения безопасности информации и национальной безопасности. Подход Китайской Народной Республики к определению целей и инструментов для реализации государственной политики по регулированию Интернет-пространства делает ее предметом пристального внимания со стороны исследователей в области политических наук.

Необходимо подчеркнуть, что на территории КНР и за ее пределами важной частью информационной безопасности является защита от киберугроз, таких как хакерство, вывод серверов из строя, хищение и шпионаж данных государственного значения и информационное противоборство. Кроме того, существует проблема информационного воздействия и вмешательства во внутренние дела государства с помощью информационно-коммуникационных технологий. Развитие новейших технологий, таких как искусственный интеллект, блокчейн, 5G, создает новые угрозы безопасности государственной инфраструктуры, частной жизни граждан и социальной стабильности. Среди этих угроз можно выделить высокий риск утечки данных, кибератаки и связанные с ними интеллектуальные преступления.

В ходе настоящего исследования была осуществлена комплексная оценка политики КНР по регулированию интернет-пространства, её эволюции, особенностей и механизмов реализации в контексте цифровизации.

Прежде всего, в работе раскрыты основные концептуальные подходы управления Интернетом, а также сущность государственной информационной политики в условиях цифровизации. Установлено, что в современном мире, где Интернет стал важнейшим каналом социальной коммуникации, обмена знаниями и формирования общественного мнения, государственная информационная политика приобретает особую значимость для обеспечения суверенитета и национальной безопасности. В результате были достигнуты следующие ключевые выводы:

Реализация политики по регулированию интернет-пространства Китайской Народной Республики основывается на основной цели - обеспечении информационной безопасности страны и создания условий, при которых вмешательство во внутреннюю ситуацию на территории Китая будет невозможным. Угрозы информационной безопасности представляют опасность для всех сфер государственной деятельности: политической, экономической и социальной. Самыми важными аспектами информационной безопасности являются оригинальность информации, конфиденциальность данных, целостность, проверяемость и управляемость.

Отдел пропаганды ЦК КПК управляет идеологической работой, средствами массовой информации, образовательной политикой, а также деятельностью различных органов Госсовета КНР, региональных властей и культурных учреждений, осуществляя цензуру всех источников информации в Китае. Кроме того, Управление по делам киберпространства КНР (САС) принимает активное участие в процессах разработки и имплементации политических решений, направленных на регулирование деятельности граждан и компаний в сети Интернет. Данное ведомство напрямую подчиняется Руководящей группе ЦК КПК по вопросам информатизации и безопасности в Интернете, которая, в свою очередь, подчиняется Центральному комитету КПК. Важно подчеркнуть, что в рамках работы были проанализированы

теоретические и законодательные основания формирования государственной политики регулирования интернета в КНР. Важными нормативными документами стали «Закон о кибербезопасности» (2017 г.), «Закон о защите персональных данных» (2021 г.) и «Закон о борьбе с телекоммуникационным и интернет-мошенничеством» (2022 г.). Эти акты закладывают основы как для контроля над инфраструктурой Интернета, так и для регулирования деятельности цифровых платформ, а также устанавливают механизмы трансграничного контроля данных.

1. Социальные сети играют важную роль в вопросе управления Интернетом в КНР, являясь инструментом контроля информационных потоков, работы с общественным мнением, продвижения партийной идеологии и прочее.

В рамках политики по регулированию интернет-пространства Китайская Народная Республика создала свои национальные интернет-платформы и социальные сети, полностью отказавшись от западных ресурсов. Данный шаг привел к достижению информационной независимости Китая и способствует обеспечению национальной безопасности КНР. Так, в период с 2009 года власти КНР начали реализовывать план по активной цензуре, а затем и дальнейшей блокировке доступа к западным социальным сетям, сайтам и платформам. Так, в 2024 году на территории Китая заблокирован доступ к следующим сайтам: Google, Twitter, Facebook, WhatsApp, Instagram, Yahoo, Viber и другим. На сегодняшний день в Китайской Народной Республике созданы и активно функционируют такие платформы, как: Weibo, Wechat, Douyin, Bilibili, Tencent QQ, Kuaishou, Youku, Xiaohongshu, Toutiao, а также национальная поисковая система Baidu. Кроме того, установлена важная роль цифровых корпораций в реализации государственной политики регулирования интернета. Компании, такие как Tencent (разработчик WeChat) и ByteDance (создатель Douyin), обязаны интегрировать в свои продукты алгоритмы автоматической цензуры, а также сотрудничать с

государственными структурами при мониторинге информации. Например, в 2021 году в Китае был введён ряд требований к платформам по обязательной идентификации пользователей и своевременному удалению запрещённого контента.

Кроме того, выявлены процессы адаптации государственной власти Китая к новым вызовам, связанным с развитием социальных сетей. Так, с 2022 года в Douyin (китайской версии TikTok) введены жёсткие лимиты времени использования для несовершеннолетних — не более 40 минут в день. Введены специальные режимы публикации контента, ориентированные на продвижение "позитивной энергии" (正能量), что свидетельствует о стремлении не только ограничить вредную информацию, но и целенаправленно формировать информационную повестку.

2. Определены основные тенденции трансформации государственной информационной политики КНР в условиях усиливающихся внешних угроз. Ужесточение контроля над экспортом технологий из США привело к тому, что КНР усилила инвестиции в развитие собственных стандартов кибербезопасности и цифрового суверенитета. Создание операционных систем на национальной основе (например, HarmonyOS от Huawei) демонстрирует стремление к снижению зависимости от западных цифровых инфраструктур.
3. В китайском Интернете существуют темы, обсуждение которых запрещено. Так, например, к таким темам можно отнести сепаратизм, проблема независимости Тибета и Синьцзян-Уйгурского автономного района, права мусульман в Китае, протесты на площади Тяньаньмэнь в 1989 году, движение «Фалуньгун» и другие. Основной целью реализации политики цензуры в информационном пространстве, является не попытка изолировать пользователей от источников информации, а контроль конкретных тем, обсуждение которых может привести к дестабилизации ситуации в обществе,

а также коллективным действиям со стороны некоторых граждан. Самой острой и наиболее часто подвергаемой ограничениям темой для обсуждения является коллективная деятельность граждан: митинги, собрания, выступления, демонстрации и прочее. При этом не столь важно, что является основной целью проведение подобных коллективных мероприятий: критика государственно власти или, наоборот, ее поддержка. Важно подчеркнуть, что степень цензуры в китайском сегменте Интернета определяется и в зависимости от временного признака и тех политических событий, которые происходят в конкретный период на территории КНР. Особенно активно система цензуры в Китае начинает функционировать накануне, во время и после мероприятий государственного масштаба (съезд КПК, сессии Всекитайского собрания народных депутатов (ВСНП) и пр.), годовщин событий, имеющих историческую значимость для народа КНР, а также напоминающих о социальной нестабильности. Таким образом, в дни, когда отмечаются годовщины определенных исторических событий или в КНР проходят важные политические или партийные мероприятия, любые сообщения в Интернете, в которых есть упоминание запрещенных тем, будут автоматически удаляться.

4. Механизмы регулирования информационного пространства в КНР зависят и от регионального фактора: уровень жесткости цензуры в Интернете отличается в разных провинциях и районах страны. Так, наиболее жесткие условия по пользованию Интернетом и ограничения по доступу к информации применяются в СУАР и Тибетском автономном районе.
5. В рамках оценки значения китайского опыта для других государств, включая Россию, можно сделать вывод о том, что китайский опыт иллюстрирует возможность сочетания развития цифровой экономики с эффективным контролем над интернет-пространством. Для России, которая также делает акцент на цифровой суверенитет (например, через создание "суверенного

Рунета"), китайские подходы к разработке нормативной базы, сотрудничеству государства с цифровыми корпорациями и развитию отечественных платформ могут представлять особый интерес. Для России разработка, создание и дальнейшее продвижение собственных национальных интернет-платформ, которые будут ориентированы как на внутренний рынок, так и на внешнюю аудиторию, станет одной из наиболее эффективных мер в ответ на внешний угрозы, а также попытки изолировать Москвы в информационном пространстве.

В рамках исследования также подтверждена научная новизна исследования. Уточнены подходы к пониманию государственной информационной политики в условиях цифровизации; выявлены особенности вовлечения негосударственных акторов — таких как цифровые корпорации — в процессы государственного регулирования интернет-пространства. Проанализированы новые формы технологического контроля, такие как использование искусственного интеллекта для мониторинга сетевой активности.

Актуальность темы исследования подтверждена как внутренними, так и международными процессами. В условиях глобальной цифровой конкуренции контроль над интернет-пространством становится не только вопросом внутренней безопасности, но и инструментом внешнеполитического влияния. Китайская практика показывает, что своевременное развитие систем регулирования Интернета является ключевым элементом национальной безопасности.

Таким образом, проведённое исследование позволило всесторонне рассмотреть политику государственного регулирования интернет-пространства КНР в условиях цифровизации, выявить её закономерности, специфические черты и тенденции развития. Полученные результаты обладают как теоретической, так и прикладной значимостью и могут быть использованы для

дальнейших сравнительных исследований и формирования рекомендаций в области информационной политики в цифровую эпоху.

Список использованных источников и литературы

Источники

Нормативно-правовые акты

На китайском языке:

1. 新修订的保守国家秘密法今年5月1日起施行 (В Китае с 1 мая 2024 года вступает в силу пересмотренный закон о защите государственной тайны) [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/yaowen/liebiao/202402/content_6934629.htm (дата обращения: 28.10.2024).
2. 中华人民共和国计算机信息网络国际联网管理暂行规定 (Временное положение КНР об управлении международным соединением компьютерных информационных сетей) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/1996-02/06/c_126468621.htm (дата обращения: 12.10.2024).
3. 计算机信息网络国际联网管理暂行规定 (Временное положение об управлении международным соединением компьютерных информационных сетей) [Электронный ресурс] // Официальный сайт администрации Хэлиньгэра. URL: http://www.helin.gov.cn/zfxxgk/yfxz/qzqd_1/gaj/202110/t20211008_1186517.html (дата обращения: 17.04.2025).
4. 互联网文化管理暂行规定 (Временные положения об управлении интернет-культурой) [Электронный ресурс] // Официальный сайт Канцелярии

Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2011-02/18/c_1112139873.htm (дата обращения: 05.11.2024).

5. 即时通信工具公众信息服务发展管理暂行规定 (Временные положения об управлении развитием услуг публичной информации в средствах мгновенной связи) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2014-08/07/c_1111983456.htm (дата обращения: 18.03.2025).

6. 生成式人工智能服务管理暂行办法 (Временные правила управления сервисами генеративного искусственного интеллекта) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm (дата обращения: 27.09.2024).

7. 中华人民共和国反恐怖主义法 (Закон КНР «О противодействии терроризму») [Электронный ресурс] // Официальный сайт Министерства юстиции КНР. URL: https://www.moj.gov.cn/pub/sfbgw/flfggz/flfggzflty/fltysfxzgxgflfg/201812/t20181225_151327.html (дата обращения: 11.02.2025).

8. 中华人民共和国数据安全法 (Закон КНР «О безопасности данных») [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/xinwen/2021-06/11/content_5616919.htm (дата обращения: 09.07.2025).

9. 中华人民共和国军人地位和权益保障法 (Закон КНР «О защите статуса, прав и законных интересов военнослужащих») [Электронный ресурс] // Официальный сайт Министерства по делам ветеранов КНР. URL:

https://www.mva.gov.cn/sy/xx/bnxx/202106/t20210611_48036.html (дата обращения: 14.12.2024).

10. 中华人民共和国网络安全法 (Закон КНР «О кибербезопасности») [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm (дата обращения: 30.04.2025).

11. 网络安全审查办法 (Методика проверки кибербезопасности) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2022-01/04/c_1642894602182845.htm (дата обращения: 08.01.2025).

12. 互联网新闻信息服务单位内容管理从业人员管理办法 (Методы управления сотрудниками, занимающимися контент-менеджментом в новостных интернет-сервисах) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2017-10/30/c_1121877917.htm (дата обращения: 22.08.2025).

13. 规范互联网信息服务市场秩序若干规定 (Некоторые положения о нормализации рыночного порядка в сфере интернет-информационных услуг) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2011-12/30/c_1111550424.htm (дата обращения: 03.03.2025).

14. 中华人民共和国电信条例 (Положение КНР о телекоммуникациях) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL:

https://www.cac.gov.cn/2000-09/30/c_133142151.htm (дата обращения: 19.11.2024).

15. 未成年人网络保护条例 (Положение о защите несовершеннолетних в интернете) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2023-10/24/c_1699806932316206.htm (дата обращения: 17.06.2025).

16. 电信和互联网用户个人信息保护规定 (Положение о защите персональных данных пользователей телекоммуникаций и интернета) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2012-07/29/c_133142088.htm (дата обращения: 04.12.2024).

17. 互联网新闻信息服务单位约谈工作规定 (Положение о проведении собеседований с организациями, предоставляющими услуги интернет-новостей) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2015-04/28/c_1115112600.htm (дата обращения: 15.05.2025).

18. 互联网信息服务内容管理行政执法程序规定 (Положение об административных процедурах правоприменения в сфере управления интернет-контентом) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2017-05/02/c_1120902931.htm (дата обращения: 09.09.2024).

19. 互联网信息服务深度合成管理规定 (征求意见稿) (Положение об управлении дипфейками: проект для публичного обсуждения) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: http://www.cac.gov.cn/2022-01/28/c_1644970458520968.htm (дата обращения: 26.07.2025).
20. 互联网用户账号名称管理规定 (Положение об управлении названиями аккаунтов интернет-пользователей) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2015-02/04/c_1114246561.htm (дата обращения: 21.09.2024).
21. 互联网视听节目服务管理规定 (Положение об управлении услугами интернет-аудиовизуального вещания) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2007-12/21/c_1112139286.htm (дата обращения: 01.10.2024).
22. 网络出版服务管理规定 (Положение об управлении услугами онлайн-издательства) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2016-02/15/c_1118048596.htm (дата обращения: 28.11.2025).
23. 计算机信息网络国际联网安全保护管理办法 (Порядок управления обеспечением безопасности международного соединения компьютерных информационных сетей) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и

информатизации КНР. URL: https://www.cac.gov.cn/2014-10/08/c_1112737294.htm (дата обращения: 13.04.2025).

24. 互联网等信息网络传播视听节目管理办法 (Порядок управления трансляцией аудиовизуальных программ через интернет и другие информационные сети) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2004-08/01/c_1112728747.htm (дата обращения: 06.02.2025).

25. 互联网信息服务管理办法 (Порядок управления услугами интернет-информации) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2000-09/30/c_126193701.htm (дата обращения: 24.09.2024).

26. 互联网信息服务管理办法 (Порядок управления услугами интернет-информации) [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/gongbao/content/2000/content_60531.htm (дата обращения: 03.05.2025).

27. 国务院关于大力推进信息化发展和切实保障信息安全的若干意见 (国发〔2012〕23号) (Некоторые мнения Государственного совета КНР о форсированном продвижении развития информатизации и реальном обеспечении информационной безопасности, № 23, 2012 г.) [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/gongbao/content/2012/content_2192395.htm (дата обращения: 19.05.2025).

28. 儿童个人信息网络保护规定 (Правила защиты персональной информации детей в интернете) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2019-08/23/c_1124913903.htm (дата обращения: 03.10.2025).
29. 网络暴力信息治理规定 (Правила по борьбе с кибернасилием) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2024-06/14/c_1720043894161555.htm (дата обращения: 07.12.2024).
30. 互联网新闻信息服务许可管理实施细则 (Правила реализации лицензирования услуг интернет-новостей) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2017-05/22/c_1121015789.htm (дата обращения: 12.08.2025).
31. 互联网信息服务算法推荐管理规定 (Правила управления алгоритмическими рекомендациями в интернет-сервисах) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm (дата обращения: 23.03.2025).
32. 网络安全安全管理条例 (Правила управления безопасностью сетевых данных) [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/gongbao/2024/issue_11646/202410/content_6980863.html (дата обращения: 02.12.2025).

33. 互联网用户账号信息管理规定 (Правила управления информацией об учетных записях интернет-пользователей) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2022-06/26/c_1657868775333429.htm (дата обращения: 29.01.2025).

34. 互联网新闻信息服务新技术新应用安全评估管理规定 (Правила управления оценкой безопасности новых технологий и приложений в новостных интернет-сервисах) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2017-10/30/c_1121878049.htm (дата обращения: 18.10.2025).

35. 网络音视频信息服务管理规定 (Правила управления сервисами аудио- и видеоконтента в интернете) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2019-11/29/c_1576561820967678.htm (дата обращения: 09.11.2024).

36. 互联网弹窗信息推送服务管理规定 (Правила управления сервисами всплывающих уведомлений в интернете) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: <https://www.cac.gov.cn> (дата обращения: 22.07.2025).

37. 互联网信息服务深度合成管理规定 (Правила управления сервисами глубинного синтеза информации в интернете) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам

кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm (дата обращения: 05.10.2025).

38. 互联网跟帖评论服务管理规定 (Правила управления сервисами интернет-комментариев) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2022-11/16/c_1670253725725039.htm (дата обращения: 14.03.2025).

39. 互联网信息服务深度合成管理规定 (Правила управления услугами интернет-информации с использованием технологий глубокого синтеза) [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/zhengce/zhengceku/2022-12/12/content_5731431.htm (дата обращения: 10.06.2025).

40. 互联网新闻信息服务管理规定 (Правила управления услугами интернет-новостей) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2017-05/02/c_1120902760.htm (дата обращения: 16.09.2024).

41. 互联网信息搜索服务管理规定 (Правила управления услугами интернет-поиска) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2016-06/25/c_1119109085.htm (дата обращения: 04.04.2025).

42. 互联网直播服务管理规定 (Правила управления услугами интернет-трансляций) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР.

URL: https://www.cac.gov.cn/2016-11/04/c_1119847629.htm (дата обращения: 20.05.2025).

43. 微博客信息服务管理规定 (Правила управления услугами микроблоговых информационных сервисов) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2018-02/02/c_1122358726.htm (дата обращения: 01.12.2025).

44. 互联网群组信息服务管理规定 (Правила управления услугами обмена информацией в интернет-группах) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2017-09/07/c_1121623889.htm (дата обращения: 08.10.2024).

45. 网络信息内容生态治理规定 (Правила управления экосистемой сетевого контента) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm (дата обращения: 11.11.2025).

46. 关于加强网络直播规范管理工作的指导意见 (Руководящие указания по усилению управления трансляциями в интернете) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2021-02/09/c_1614442843753738.htm (дата обращения: 15.07.2025).

47. 关于加强党政机关网站安全管理的通知 (Уведомление об усилении управления безопасностью сайтов партийных и государственных учреждений) [Электронный ресурс] // Официальный сайт Канцелярии Центральной комиссии

по вопросам кибербезопасности и информатизации КНР. URL: https://www.cac.gov.cn/2014-05/10/c_1112142115.htm (дата обращения: 06.01.2025).

Документы стратегического планирования в сфере регулирования Интернета

На китайском языке:

48. 中华人民共和国国民经济和社会发展“九五”计划和 2010 年远景目标纲要 (План социально-экономического развития КНР в рамках 9-й пятилетки и перспективные цели до 2010 г.) [Электронный ресурс] // Официальный сайт Государственного комитета по развитию и реформам КНР. URL: <https://www.ndrc.gov.cn/fggz/fzzlgh/gjfzgh/200709/P020191029595686994247.pdf> (дата обращения: 14.10.2024).

49. 中共中央 国务院印发《国家创新驱动发展战略纲要》 (ЦК КПК и Государственный совет КНР опубликовали «План национальной стратегии инновационного развития») [Электронный ресурс] // Официальный сайт Министерства науки и технологий КНР. URL: https://www.most.gov.cn/szyw/yw/201605/t20160520_125675.html (дата обращения: 22.03.2025).

50. 2006–2020 年国家信息化发展战略 (Государственная стратегия по развитию информатизации на период с 2006 по 2020 г.) [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/gongbao/content/2006/content_315999.htm (дата обращения: 09.11.2024).

51. 国家网络空间安全战略 (Национальная стратегия кибербезопасности) [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: https://www.cac.gov.cn/2016-12/27/c_1120195926.htm (дата обращения: 17.06.2025).
52. 《新时代的中国网络法治建设》白皮书 (Белая книга «Развитие правовой системы управления интернетом в Китае в новую эпоху») [Электронный ресурс] // Официальный сайт Пресс-канцелярии Государственного совета КНР. URL: http://www.scio.gov.cn/zfbps/ndhf/49551/202303/t20230320_709279.html (дата обращения: 03.12.2025).
53. 《携手构建网络空间命运共同体》白皮书 (Белая книга «Совместное формирование сообщества единой судьбы в киберпространстве») [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: https://www.cac.gov.cn/2022-11/07/c_1669457523014880.htm (дата обращения: 28.02.2025).
54. 《“十四五”国家信息化规划》 (Национальный план информатизации в рамках XIV пятилетки) [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: http://www.cac.gov.cn/2021-12/27/c_1642205314518676.htm (дата обращения: 11.09.2024).
55. 中华人民共和国国民经济和社会发展“九五”计划和 2010 年远景目标纲要 (План социально-экономического развития КНР в рамках 9-й пятилетки и перспективные цели до 2010 г.) [Электронный ресурс] // Официальный сайт Государственного комитета по развитию и реформам КНР. URL: <https://www.ndrc.gov.cn/fggz/fzzlgh/gjgzgh/200709/P020191029595686994247.pdf> (дата обращения: 25.07.2025).

56. 中共中央 国务院印发《国家创新驱动发展战略纲要》 (ЦК КПК и Государственный совет КНР опубликовали «План национальной стратегии инновационного развития») [Электронный ресурс] // Официальный сайт Министерства науки и технологий КНР. URL: https://www.most.gov.cn/szyw/yw/201605/t20160520_125675.html (дата обращения: 06.04.2025).
57. 2006–2020 年国家信息化发展战略 (Государственная стратегия по развитию информатизации на период с 2006 по 2020 г.) [Электронный ресурс] // Официальный сайт Государственного совета КНР. URL: https://www.gov.cn/gongbao/content/2006/content_315999.htm (дата обращения: 19.12.2024).
58. 国家网络空间安全战略 (Национальная стратегия кибербезопасности) [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: https://www.cac.gov.cn/2016-12/27/c_1120195926.htm (дата обращения: 07.08.2025).
59. 《新时代的中国网络法治建设》白皮书 (Белая книга «Развитие правовой системы управления интернетом в Китае в новую эпоху») [Электронный ресурс] // Официальный сайт Пресс-канцелярии Государственного совета КНР. URL: http://www.scio.gov.cn/zfbps/ndhf/49551/202303/t20230320_709279.html (дата обращения: 24.10.2025).
60. 《携手构建网络空间命运共同体》白皮书 (Белая книга «Совместное формирование сообщества единой судьбы в киберпространстве») [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: https://www.cac.gov.cn/2022-11/07/c_1669457523014880.htm (дата обращения: 13.01.2025).

61. 《“十四五”国家信息化规划》 (Национальный план информатизации в рамках XIV пятилетки) [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: http://www.cac.gov.cn/2021-12/27/c_1642205314518676.htm (дата обращения: 21.11.2025).

Выступления и комментарии политических деятелей

На китайском языке:

62. Си Цзиньпин: реформируем нашу родину от интернет-страны к кибердержаве [习近平: 把我国从网络大国建设成为网络强国] // Официальный сайт новостного агентства «Синьхуа». Электронный ресурс. Режим доступа: http://www.xinhuanet.com/politics/2014-02/27/c_119538788.htm (дата обращения: 08.03.2026).

63. Си Цзиньпин: Пусть достижения развитого Интернета принесут пользу 1,3 миллиардам китайцев [习近平: 让互联网发展成果惠及 13 亿中国人民] // Официальный сайт Всемирной интернет-конференции. Электронный ресурс. Режим доступа: https://www.cac.gov.cn/2014-11/19/c_1113319307.htm (дата обращения: 10.08.2025).

Научные монографии

Исследования на русском языке:

64. Панарин И.Н., Панарина Л.Г. Информационная война и мир. М.: ОЛМА-ПРЕСС, 2003.

65. Попов И.М. Война будущего: взгляд из-за океана. М.: АСТ-Астрель, 2004.

66. Суверенитет государства в международном праве / под ред. А.А. Моисеева. М.: Восток–Запад, 2009.
67. Трощинский П. В. Правовая система Китая. М.: ИДВ РАН, 2016.
68. Трощинский П. В. Эволюция правовой системы Китайской Народной Республики (1949–2018 гг.): историко-правовой аспект (с перечнем действующих законов КНР). М.: ВКН, 2018.
69. Чжи Ян, Тянь Юехун. Современная журналистика Китая: вечерняя пресса, региональное радио. Минск, 2011.

Научные статьи

Исследования на русском языке:

70. Антипов К. Киберконфликт в китайско-американских отношениях и поиски диалога // Проблемы Дальнего Востока. 2013. № 6. С. 39–54.
71. Афонина Л. А. Система партийной пропаганды в Китае // Новая эпоха: Китай после XIX съезда КПК. 2018. С. 115–133.
72. Ашмаров И.А. Электронная коммерция в Китае как источник роста страны // Вестник Воронежского института экономики и социального управления. 2019. № 1. С. 21–27.
73. Барышников Д.Н., Туленков А.Ю. «Цифровая дипломатия» и государственный суверенитет в эпоху глобализации // Вестник Санкт-Петербургского университета. Серия 6. Философия. Культурология. Политология. Право. Международные отношения. 2012. № 4. С. 121–128.
74. Бен Р.М. Город как продукт в условиях современного маркетинга // Архонт. 2018. № 6 (9). С. 56–60.

75. Бондарева Т.А., Чекменёва Т.Г. На новом этапе глобальной конкуренции: материалы Международной научно-практической студенческой конференции. Воронеж: ВГТУ, 2013. С. 101–106.
76. Бредихин А.В. Приграничные агломерации в процессах наднациональной интеграции ЕАЭС и Китая // Журнал исторических, политологических и международных исследований. 2016. № 2 (58). С. 93–102.
77. Булавин А.В. О подходах США и Китая к обеспечению кибербезопасности // Общество: политика, экономика и право. 2014. № 1.
78. Быков И.А. Управление Интернетом как одна из проблем современных международных отношений // ПОЛИТЭКС. 2008. № 2. С. 164–174.
79. Васильковский С.А., Игнатов А.А. Управление Интернетом: системные диспропорции и пути их разрешения // Вестник международных организаций: образование, наука, новая экономика. 2020. Т. 15, № 4. С. 7–29
80. Верник А.Г. Цензура в интернете: исторический аспект, современный опыт и перспективы [Электронный ресурс] // Дискуссия. 2015. № 11(52). С. 174–182. URL: <https://cyberleninka.ru/article/n/tsenzura-v-internete-istoricheskiy-aspekt-sovremennuyu-opyt-i-perspektivy> (дата обращения: 17.01.2023).
81. Вершинина Т.В., Карпович О.Г., Ногмова А.Ш. Проблемы кибербезопасности в эпоху COVID-19 // Вестник ученых-международников. – 2022. – № 1(19). – С. 12-27.
82. Вильданов Р.Р., Кутушева Э.Н. Система государственного регулирования интернета в Китайской Народной Республике // Вестник УГНТУ. Наука, образование, экономика. Серия: Экономика. 2021. № 3. С. 115–122.

83. Володенков С.В. Интернет-пространство в системе глобального политического управления: основные сценарии трансформации // Вестник Российской нации. 2017. № 4(56). С. 147–161.
84. Вэй С. Вопросы кибербезопасности и защиты данных в умных городах // Безопасность и технологии. 2022. № 14(4). С. 201–218.
85. Гаврилов Е.О. Цифровой суверенитет в условиях глобализации: философский и правовой аспекты // Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки. 2020. Т. 4, № 2(14). С. 146–152.
86. Герман М.А. Специфика подхода КНР к обеспечению стабильности государства // Общество и государство в Китае. 2016.
87. Глазунов О.Н., Авдеенко В.В. Специфика правового регулирования сети Интернет в Китайской Народной Республике // Общество: политика, экономика, право. [нужно уточнить: год]. № 2. С. 93–96.
88. Горян Э.В. Нормативно-правовая основа обеспечения национальной безопасности в киберпространстве: опыт Китайской Народной Республики // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2021. Т. 13, № 1. С. 115–124.
89. Дегтерев Д.А., Рамич М.С., Пискунов Д.А. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // Вестник международных организаций: образование, наука, новая экономика. 2021. Т. 16, № 3. С. 7–33.
90. Денисов И.Е., Зуенко И.Ю. От мягкой силы к дискурсивной силе: новые идеологемы внешней политики КНР. М.: МГИМО-Университет, 2022.

91. Дмитриев М.Г. Региональная информационная политика как фактор формирования информационного пространства: дис. ... канд. полит. наук. М., 2004. 137 с.
92. Дремлюга Р.И. Интернет как способ и средство совершения преступления // Информационное право. 2008. № 4. С. 27–31.
93. Евдокимов Е.В. Политика Китая в глобальном информационном пространстве // Международные процессы. 2011. Т. 9. № 1. С. 74–83.
94. Ефименко Е.С., Люлина А.Г. Китайский язык: иероглифическое письмо и его «след» на сознании и менталитете // Языки и культуры: перспективы развития в XXI веке. М.: Цифровичок, 2021. С. 378–380.
95. Ефремов А.А. Государственный суверенитет в условиях цифровой трансформации // Правоведение. 2019. Т. 63, № 1. С. 47–61.
96. Журавская А.О. Процесс социального манипулирования: структура, факторы и технологии // Архонт. 2024. № 2 (41). С. 57–61.
97. Засурский Я.Н. Журналистика и мир на рубеже тысячелетий. М.: Изд-во Московского университета, 2000. 384 с.
98. Зиновьева Е.С. Международное управление Интернетом: проблемы, подходы, перспективы // Вестник МГИМО. 2010. № 6. С. 167–174.
99. Зубофф Ш. Эпоха надзорного капитализма: битва за человеческое будущее на новых рубежах власти / пер. с англ. А.Ф. Васильева; под науч. ред. Я. Охонько, А. Смирнова. М.: Издательство Института Гайдара, 2022. 781 с.
100. Ибрагимова Г. Стратегия КНР в области управления Интернетом и обеспечения информационной безопасности // Индекс безопасности. 2013. № 1 (104). С. 169–184.

101. Игнатов А.А. Управление Интернетом в повестке БРИКС // Вестник международных организаций: образование, наука, новая экономика. 2022. № 2. С. 86–109.
102. Имин Ч., Сяоцзюнь Л., Хуй Ч. Влияние искусственного интеллекта на транспортные системы Пекина // Умные города. 2021. № 14 (3). С. 155–169.
103. Исаев А.С. Российско-китайское взаимодействие по вопросам обеспечения информационной безопасности // Китай в мировой и региональной политике. История и современность. 2018.
104. Истомин Н.А. Модель участия заинтересованных сторон в управлении Интернетом на международном уровне // Право и политика. 2020. № 5. С. 90–109.
105. Карасев П.А. Управление интернетом – тенденции и перспективы // International Journal of Open Information Technologies. 2023. Т. 11, № 9. С. 59–65.
106. Касенова М.Б., Воронина Е.П. Европейский союз на пути к цифровому суверенитету? // Интернет изнутри. 2023. № 19. С. 41–44.
107. Кашин В.Б., Кокошин А.А. О подходах руководства КНР и китайских силовых структур к противоборству в киберпространстве // Военная мысль. 2022. № 6. С. 119-127.
108. Кирилюк О.В. Международно-правовые основы саморегулирования в киберпространстве // Право. Журнал Высшей школы экономики. 2016. № 1. С. 177–188.
109. Косинова С.Н. Обеспечение безопасности интернет-пространства посредством новой многополярности // Национальная безопасность. 2022. № 1. С. 1–11.

110. Кочетков А.П., Мамычев А.Ю. Государственная политика России в цифровую эпоху: основные тренды, сценарии и регуляторные практики // Полис. Политические исследования. 2023. № 1. С. 96–113. DOI: 10.17976/jpps/2023.01.08; Кочетков А.П., Маслов К.В. Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе // Вестник Московского университета. Серия 12. Политические науки. 2022. № 2. С. 31–45.
111. Кошурникова Н.А. Особенности информационной политики современного Китая // Китай: история и современность: материалы IX Международной научно-практической конференции. Екатеринбург, 2016. С. 279–284.
112. Куркемова Э.Т. Интернет-технологии как ресурс активности политических акторов // Каспийский регион: политика, экономика, культура. 2016. № 2(47). С. 101–108.
113. Кутюр С., Тоупин С. Что означает понятие «суверенитет» в цифровом мире? // Вестник международных организаций: образование, наука, новая экономика. 2020. Т. 15, № 4. С. 48–69.
114. Кучерявый М.М. Государственная политика информационного суверенитета России в условиях современного глобального мира // Управленческое консультирование. 2015. № 2. С. 8–15.
115. Лексютина Я.В. Политика китайского руководства в вопросах контроля и регулирования Интернета // Проблемы Дальнего Востока. 2014. № 2. С. 202–214.
116. Ли Личи. Роль новых медиа в создании имиджа правительства Китая: магистерская диссертация. СПб.: Санкт-Петербургский государственный университет, 2020. 124 с.

117. Ли Сяо. Китайские новостные приложения на мировом рынке новых медиа: магистерская диссертация. СПб.: Санкт-Петербургский государственный университет, 2017. 130 с.
118. Лэй В., Сяохун Л. Развитие умных городов в Китае: ретроспектива и перспективы // Городские исследования. 2020. № 58 (10). С. 2039–2057.
119. Лэй В., Тао Ч. Умные города и экологическая устойчивость: китайский подход // Урбанизация и технологии. 2021. № 36 (1). С. 45–62.
120. Лю Я. Публичная сфера под контролем: современный опыт регулирования Интернет-журналистики в КНР // Ойкумена. Регионоведческие исследования. 2016. № 2. С. 32–43.
121. Люлина А.Г., Ефименко Е.С. Интернет-цензура в современном Китае: жесткий контроль и гибкая система урегулирования // Вестник Российского университета дружбы народов. Серия: Всеобщая история. 2022. Т. 14, № 2. С. 175–188.
122. Маркелов К.В. Общественный идеал как объект информационной политики: дис. ... д-ра полит. наук: 10.01.10. М., 2006. 350 с.
123. Минь Ч. Международное сотрудничество в развитии умных городов: анализ китайских инициатив // Международное планирование и развитие. 2021. № 25 (2). С. 112–127.
124. Миньхуа В., Юньпэн Ч. Сравнительный анализ глобальных стратегий по борьбе с социальным неравенством на фоне пандемии COVID-19 // Архонт. 2024. № 1 (40). С. 76–85.
125. Мистюков В.В. Информационная политика современной России в контексте формирующегося гражданского общества: дис. ... канд. полит. наук. М., 2012. 166 с.

126. Михалевич Е.А. Концепция киберсуверенитета Китайской Народной Республики: история развития и сущность // Вестник Российского университета дружбы народов. Серия: Политология. 2021. Т. 23, № 2. С. 254–264.
127. Надежкина Е.С. Имидж России в Китае в XXI веке на основе анализа медиа-платформ китайского сегмента сети Интернет: дис. ... канд. полит. наук. М.: Московский государственный университет, 2023. 210 с.
128. Никонов В.А., Воронов А.С., Сажина В.А. [и др.] Цифровой суверенитет современного государства: содержание и структурные компоненты (по [нужно уточнить: материалам?] экспертного исследования) // Вестник Томского государственного университета. Философия. Социология. Политология. 2021. № 60. С. 206–216.
129. Пашенцев Е.Н. Злонамеренное использование искусственного интеллекта: новые угрозы для международной информационно-психологической безопасности и пути их нейтрализации // Государственное управление. Электронный вестник. 2019. № 76. С. 279–300.
130. Пашенцев Е.Н., Базаркина Д.Ю., Мэттью К. Системные конструкты международной безопасности: индикаторы социальных изменений как путь к разрешению конфликтов. 2022.
131. Петрунин А.Н. Институт связей с общественностью Министерства обороны России в государственной информационной политике: особенности и направления оптимизации: автореф. дис. ... канд. полит. наук: 23.00.02. М., 2011. 22 с.
132. Подшибякина Т.А. «Золотой щит» Китая: политика управления мнемоническими интернет-практиками // Вестник Российского университета дружбы народов. Серия: Политология. - 2020. - Т. 22. - №2. - С. 194-204.

133. Полончук Р.А. Политика КНР по обеспечению кибербезопасности в условиях нарастающего противодействия со стороны США // Информационные войны. 2019. № 2(50). С. 60–63.
134. Прохоров Е. П. Журналистика и демократия. М., Изд. Аспект Пресс, 2001. - 352 с.
135. Разумов Е.А. Политика КНР по обеспечению кибербезопасности // Россия и АТР. 2017. № 4 (98). С. 156–170.
136. Романова Т.А., Малова А.Н. Проблема применения категории «стрессоустойчивость» в политике кибербезопасности Евросоюза // Вестник Московского университета. Серия 25: Международные отношения и мировая политика. 2019. Т. 11, № 1. С. 20–46.
137. Сахаров А.В., Шелепов А.В. Политика Китайской Народной Республики в сфере регулирования цифровых платформ // Вестник международных организаций. 2024. Т. 19, № 2. С. 145–160.
138. Срничек Н. Капитализм платформ / пер. с англ.; под науч. ред. М. Добряковой. М.: Изд. дом ВШЭ, 2019. 128 с.
139. Сяоцзюнь Л., Чжиюн В., Цянь Ч. Зеленые технологии и устойчивое развитие умных городов // Экологическое планирование и технологии. 2022. № 19 (3). С. 123–138.
140. Ткаченко И.Ю. Проблемы развития цифровых технологий // Российский внешнеэкономический вестник. 2018. № 9. С. 76–87.
141. Трощинский П. В. Эволюция правовой системы Китайской Народной Республики (1949–2018 гг.): историко-правовой аспект (с перечнем действующих законов КНР). М.: ВКН, 2018.

142. Трощинский П.В. Цифровой Китай до и в период коронавируса: особенности нормативно-правового регулирования // Право и цифровая экономика. 2021. № 1. С. 44–58.
143. Трощинский П.В., Молотников А.Е. Особенности нормативно-правового регулирования цифровой экономики и цифровых технологий в Китае // Правоведение. 2019. Т. 63. № 2. С. 309–326.
144. Федоров А.П. Об опыте Китая по противодействию манипуляционным технологиям в социальных сетях Интернета // Вестник Московского государственного областного университета. Электронный журнал. 2018. № 2. С. 179–188.
145. Федорченко С.Н. Эффект палладиума: ценности великих держав в эпоху искусственного интеллекта // Журнал политических исследований. 2023. Т. 7. № 4. С. 3–32.
146. Ханьянцзы Л. Внешнеполитический курс современного Китая в отражении национальных СМИ // Век информации. СМИ и внешняя политика Китая. 2014. С. 31–32.
147. Хунвэй Л., Лян С. Системы телемедицины и экологического мониторинга в стратегии умного города Шанхая // Городское планирование и развитие. 2022. № 148 (2). С. 123–135.
148. Цзинь Хань. Влияние новых медиа на социализацию подростков Китая: дис. ... канд. филол. наук. М.: Российский университет дружбы народов, 2024. 215 с.
149. Цзянь Л., Чжиюн В., Тао Ч. Новая инфраструктура и ее роль в развитии умных городов в Китае // Технологии в урбанизации. 2021. № 35 (4). С. 211–225.

150. Чекменёва Т.Г. Технократия как принцип управления современным постиндустриальным обществом: «за» и «против» // Государство, общество, церковь в истории России XX–XXI веков. 2015. С. 712–719.
151. Чекменёва Т.Г., Прибытков А.А. Историческая память и национально-гражданская идентичность россиян как объекты информационно-психологических атак // Информационные войны. 2018. С. 734–750.
152. Чекменёва Т.Г., Прибытков А.А. Проблемы обеспечения информационной безопасности молодежи в современной России: психологический аспект // Психологическое благополучие современного человека. 2018. С. 121–128.
153. Чекменёва Т.Г., Прибытков А.А. Россия в сфере информационного противоборства: проблемы и перспективы // Конфликты в современном мире. 2016. С. 218–223.
154. Чжан Жун. СМИ и власть в Китае: проблемы взаимодействия: на примере анализа содержания газеты «Пекинская молодежь»: дис. ... канд. филол. наук: 10.01.10. М., 2011. 217 с.
155. Чжан Шуан. Роль социальных сетей в формировании имиджа Китая // Вестн. Амурского гос. ун-та. 2014. Вып. 2(140). С. 257–260.
156. Шапкин В.В. Методологические основания институционализма // Проблемы современной экономики. 2011. № 2 (38). С. 58–62.
157. Шевченко Я.Н. Цифровой суверенитет Европы в контексте политики глобального управления данными // Политическая наука. 2021. № 3. С. 251–270.

158. Шестопал С.С., Мамычев А.Ю. Суверенитет в глобальном цифровом измерении: современные тренды // Балтийский гуманитарный журнал. 2020. Т. 9. № 1 (30). С. 398–403.
159. Шипулин В.О. Трансформации суверенитета в эпоху информационной глобализации // Ученые записки Новгородского государственного университета. 2022. № 2 (41). С. 255–259.
160. Ширин С.С. Российские инициативы по вопросам управления Интернетом // Вестник МГИМО. 2014. № 6 (39). С. 73–81.
161. Штодина Д.Д. Глобальное управление Интернетом: российский законодательный подход // Евразийский юридический журнал. 2022. № 3 (166). С. 30–34.
162. Штоль В.В., Задохин А.Г. Информационно-коммуникационные технологии и информационная безопасность России // Обозреватель. 2022. № 5–6 (388–389). С. 66–78.
163. Шугуров М.В. «Группа восьми» (G8) и дилеммы глобального управления Интернетом: международно-правовой аспект // Право и политика. 2012. № 6. С. 1098–1127.
164. Щербакова Е.Н., Гурулева Т.Л. Интернет-цензура в Китае // Успехи современного естествознания. 2013. № 11. С. 197.

Исследования на китайском языке:

165. Ван Жун. Историческое развитие, особенности и основные тенденции регулирования Интернета в Китае [王融. 中国互联网监管的历史发展、特征和

- 重点趋势] // Пекинское общество исследования законодательства в сфере коммуникаций [北京通信法制研究会]. – 2017. – С. 52–65.
166. Ван Сучжи. Споры вокруг проектов международного законодательства о киберпреступности и предложения Китая [王肃之. 网络犯罪国际立法的模式之争与中国方案] // Нанкинский юридический журнал [南大法学]. – 2021. – № 5. – С. 107–124.
167. Ван Сяовэй, Яо Юй (Wang Xiaowei, Yao Yu). 网络主权与全球互联网治理 (Сетевой суверенитет и глобальное управление Интернетом) // 哲学分析 (Философский анализ). 2018. № 9(01). С. 116–125, 198.
168. Ван Хухуа, Чжан Лэй (Wang Huhua, Zhang Lei). 国家主权与互联网国际行为准则的制定 (Государственный суверенитет и разработка международных правил поведения в Интернете) // 河北法学 (Хэбэйская юридическая наука). 2015. № 33(12). С. 11–20.
169. Ван Хухуа, Чжан Лэй. Государственный суверенитет и разработка международных правил поведения в Интернете [王虎华, 张磊. 国家主权与互联网国际行为准则的制定] // Хэбэйская юридическая наука [河北法学]. – 2015. – № 33(12). – С. 11–20.
170. Го Цзяньцян, Юань Гуан. Дилемма, с которой столкнулось китайское сетевое правоприменение, и пути ее решения [郭渐强, 袁光. 我国网络执法面临的困境及其出路] // Современное экономическое управление [当代经济管理]. – 2016. – Т. 38. – № 12. – С. 33–39.

171. Гун Чэнбо, Сунь Цзы. Эволюция дискурса генерального секретаря Си Цзиньпина о медиаконвергенции СМИ [宫承波, 孙宇. 习近平总书记关于媒体融合重要论述的演进脉络及目标指向] // Китайское издательское дело [中国出版]. – 2021. – № 2. – С. 5–6.
172. Е Хао (Ye Hao). 政府新闻学：传媒管理新办法 (Дела правительственной журналистики: новые методы правительства в отношении СМИ). Нанкин: Издательство Университета Фудань, 2007. 192 с.
173. Куан Вэньбо, Фаньюань (Kuang Wenbo, Fang Yuan). 网络空间命运共同体理念下的全球互联网治理体系变革 (Трансформация глобальной системы управления Интернетом в соответствии с концепцией Сообщества судьбы в киберпространстве) // 武汉大学学报(哲学社会科学版) (Журнал Уханьского университета. Издание по философии и социальным наукам). 2023. № 76(05). С. 38–46.
174. Лан Пин (Lang Ping). 网络空间国际治理与博弈 (Международное управление и игры в киберпространстве). Пекин: China Social Sciences Press, 2022. 332 с.
175. Ли Сигуан (Li Xiguang). 畸形的媒体 (Аномальная пресса). Шанхай: Издательство Университета Фудань, 2003. 345 с.
176. Ли Чжи, Тан Жуньхуа (Li Zhi, Tang Runhua). 多利益攸关方模式: 构建全球互联网治理体系的路径研究 (Модель участия многих заинтересованных сторон: исследование пути к созданию глобальной системы управления Интернетом) // 传媒观察 (Наблюдение за СМИ). 2020. № 12. С. 21–28.

177. Линь Хуа. Механизм государственного управления сетевыми слухами: правовые границы и ограничения власти [林华. 网络谣言治理的政府机制: 法律界限与权力约束] // Финансово-юридические исследования [财经法学]. – 2019. – № 3. – С. 121–130.
178. Ло Синь, Цай Юйтин (Luo Xin, Cai Yuting). 全球互联网治理规则制定的分布格局与中国进路 (Структура распространения нормотворческой деятельности в области глобального управления Интернетом и подход Китая) // 现代传播(中国传媒大学学报) (Современные коммуникации. Журнал Коммуникационного университета Китая). 2022. № 44(03). С. 68–75.
179. Лу Вэй (Lu Wei). 坚持尊重网络主权原则 推动构建网络空间命运共同体——学习习近平总书记在第二届世界互联网大会上重要讲话精神的体会与思考 (Придерживаться принципа уважения сетевого суверенитета и содействовать формированию сообщества единой судьбы в киберпространстве: размышления о ключевых положениях выступления Генерального секретаря на Второй Всемирной интернет-конференции) // 中国信息安全 (Информационная безопасность Китая). 2016. № 3. С. 34–35.
180. Лу Вэй. Придерживаться принципа уважения сетевого суверенитета и содействовать формированию сообщества единой судьбы в киберпространстве: размышления о ключевых положениях выступления Генерального секретаря на Второй Всемирной интернет-конференции [鲁炜. 坚持尊重网络主权原则 推动构建网络空间命运共同体——学习习近平总书记在第二届世界互联网大会上重要讲话精神的体会与思考] // Информационная безопасность Китая [中国信息安全]. – 2016. – № 03. – С. 34–35.

181. Лу Чуаньин (Lu Chuanying). 主权概念的演进及其在网络时代面临的挑战 (Эволюция концепции суверенитета и вызовы, с которыми она сталкивается в эпоху Интернета) // 国际关系研究 (Исследования международных отношений). 2014. № 1. С. 73–81.
182. Лун Синьтао, Лян Юйжуй. Исследование регулирования интернет-индустрии коротких видео в Китае [龙新涛, 梁玉蕊. 中国短视频的互联网监管研究] // Наука о новостной коммуникации [新闻传播科学]. – 2024. – Т. 12. – № 3. – С. 752–758.
183. Лю Божань, Хуан Фэнчжи. Анализ международной политической игры за власть в киберпространстве [刘勃然, 黄凤志. 网络空间国际政治权力博弈问题探析] // Исследования социализма [社会主义研究]. – 2013. – С. 120–126.
184. Лю Линь, Цуй Шуай. Исследование контрмер по обеспечению верховенства закона в управлении киберпространством в новую эпоху [刘林, 崔帅. 新时代网络空间治理法治化对策研究] // Вестник Ляонинского университета радио и телевидения [辽宁广播电视大学学报]. – 2022. – № 2. – С. 84–86.
185. Лю Хуажун (Liu Huarong). 大众传媒与政治 (СМИ и политика). Пекин: Издательство Пекинского университета, 2001. 284 с.
186. Лю Чжицзюнь, Дай Гаюань, Тянь Бао и др. Анализ рисков и архитектура защиты безопасности системы доменных имен [刘志军, 戴高远, 田葆, 等. 域

- 名系统风险分析及安全防护架构] // Гуандунские коммуникационные технологии [广东通信技术]. – 2023. – Т. 43. – № 8. – С. 42–45.
187. Мэн Сяоян, Фэн Бобо. Механизм, этика и регулирование производства коротких видеороликов [蒙晓阳, 冯博博. 短视频内容生产的机制、伦理及规制] // Молодой журналист [青年记者]. – 2021. – № 19. – С. 41–43.
188. Се Синьчжоу, Чжу Яоин. Анализ проблем, возникающих в связи с популярностью коротких видеороликов [谢新洲, 朱垚颖. 短视频火爆背后的问题分析] // Издательская наука [出版科学]. – 2019. – Т. 27. – № 1. – С. 86–91.
189. Сун Ин. Недостатки и преимущества законодательства о национальной безопасности в КНР [宋颖. 我国国家安全立法的不足与完善] // Ганьсуские общественные науки [甘肃社会科学]. – 2021. – № 5. – С. 136–143.
190. Сюй Лян. Новые вызовы сетевой безопасности и стратегии реагирования [徐亮. 网络安全面临的新挑战和应对策略] // Технологии и применение сетевой безопасности [网络安全技术与应用]. – 2021. – С. 148–149.
191. Сюй Цзе. Анализ механизма распространения и управления мобильными короткими видеороликами [徐杰. 移动短视频的传播机制与治理探析] // Медиа [传媒]. – 2021. – № 20. – С. 53–55.
192. Сюн Гуанцин, Ван Жуй (Xiong Guangqing, Wang Rui). 全球互联网治理中的网络主权: 历史演进、国际争议和中国立场 (Сетевой суверенитет в

- глобальном управлении Интернетом: историческая эволюция, международные споры и позиция Китая) // 学习与探索 (Обучение и исследования). 2024. № 4 (总第 345 期). С. 24–33.
193. Ся Цююэ, Чэнь Хунмэй. Текущее состояние и проблемы функционирования видеоплатформ для коротких роликов, таких как «Доуинь» [夏秋悦, 陈红梅. “抖音”等短视频平台的发展现状及存在问题] // Китайское радиовещание [中国广播]. – 2020. – № 3. – С. 47–50.
194. Сяо Чэньхуэй. Вызовы безопасности и меры реагирования на «внезапные сетевые атаки» в информационную эпоху [肖晨卉. 信息时代“突发性网络攻击”的安全挑战与应对] // Журнал разведывательной информации [情报杂志]. – 2021. – С. 74–79.
195. Тянь Лицзя, Ван Гуанхоу. Исследование текущей ситуации с безопасностью киберпространства в Китае [田立加, 王光厚. 中国网络空间安全现状研究] // Журнал Шаньсийского датунского университета. Серия: Общественные науки [Journal of Shanxi Datong University (Social Science)]. – 2015. – С. 12–14.
196. У Юйтун. Исследование деятельности киберполиции [吴雨桐. 网络警察执法研究]: магистерская диссертация. – Шанхай: Восточно-Китайский университет политических наук и права [华东政法大学]. – 2017.
197. Фан Юй. Нормативная логика и обоснование института уведомления об утечке данных в контексте защиты персональной информации [方禹. 个人信

- 息保护中数据泄露通知制度的规范逻辑及其证成] // Авангардные дисциплины [学科前沿]. – 2022. – № 5. – С. 91–107.
198. Фэн Юйвэй. Исследование вопросов верховенства права в управлении безопасностью киберпространства в новую эпоху – с точки зрения общей концепции национальной безопасности [冯玉卫. 新时期网络空间安全治理中的法治问题探究——基于总体国家安全观的视角] // Практика верховенства права [《法治实务》集刊 2023 年第 3 卷——国家安全工作研究文集]. – Шанхай: Восточно-Китайский педагогический университет [华东师范大学]. – 2023. – С. 5.
199. Ху Ли, Ци Айминь (Hu Li, Qi Aimin). 论“网络疆界”的形成与国家领网主权制度的建立 (Формирование «сетевых границ» и создание системы государственного сетевого суверенитета) // 法学论坛 (Юридический форум). 2016. № 2 (общ. № 164). С. 59–66.
200. Ху Ли, Ци Айминь, Хэ Цзиньхай (Hu Li, Qi Aimin, He Jinhai). 国家网络空间主权战略 (学者建议稿) (Стратегия национального суверенитета в киберпространстве: проект научного предложения) // 河北法学 (Хэбэйская юридическая наука). 2018. Т. 36, № 6. С. 80–88.
201. Ху Ли, Ци Айминь. Формирование «сетевых границ» и создание системы государственного сетевого суверенитета [胡丽, 齐爱民. 论“网络疆界”的形成与国家领网主权制度的建立] // Юридический форум [法学论坛]. – 2016. – № 2 (总第 164 期). С. 59–66.

202. Ху Цзяньшэн, Хуан Чжисюн. Дилеммы и перспективы реализации механизмов международного права для борьбы с киберпреступностью [胡健生, 黄志雄. 打击网络犯罪国际法机制的困境与前景——以欧洲委员会《网络犯罪公约》为视角] // Исследования международного права [国际法研究]. – 2016. – № 6. – С. 21–34.
203. Цзоу Сюйи (Zou Xuyi). 全球互联网治理困境与网络空间命运共同体构建的价值取向 (Дилемма глобального управления Интернетом и ценностная ориентация построения сообщества судьбы в киберпространстве) // 天津社会科学 (Тяньцзиньские социальные науки). 2020. № 2. С. 83–87.
204. Цзоу Цзюнь (Zou Jun). 全球互联网治理:未来趋势与中国议题 (Глобальное управление Интернетом: будущие тенденции и проблемы Китая) // 新闻与传播研究 (Журналистика и коммуникационные исследования). 2016. № 23(S1). С. 5–13, 125.
205. Цзэн Делинь, Цай Цзявэй, Оуян Таохуа (Zeng Delin, Cai Jiawei, Ouyang Taohua). 数字化转型研究: 整合框架与未来展望 (Исследование цифровой трансформации: интеграционная рамка и перспективы будущего) // 外国经济与管理 (Foreign Economics & Management). 2021. Т. 43, № 5. С. 63-76.
206. Ци Шанцай (Qi Shangcai). 全球互联网治理困境: 制度缺失与治理赤字 (Дилемма глобального управления Интернетом: институциональные недостатки и недоработки в управлении) // 廊坊师范学院学报(社会科学版) (Журнал педагогического университета Ланфан. Издание по социальным наукам). 2020. № 36(04). С. 19–27.

207. Цуй Баого (Cui Baoguo). 网络空间治理模式的争议与博弈 (Противоречивая и игровая модель управления киберпространством) // 新闻与写作 (Журналистика и писательство). 2016. № 10. С. 23–26.
208. Цуй Цунцун. Административный надзор и развитие защиты персональной информации [崔聪聪. 个人信息保护的行政监管及展开] // Вестник Сучжоуского университета. Серия: Философия и общественные науки [苏州大学学报：哲学社会科学版]. – 2022. – № 5. – С. 73–84.
209. Чжан Шудянь, Линь Жуйсинь. Влияние Интернета на эрозию и укрепление государственного суверенитета [张淑钿, 林瑞鑫. 论互联网对国家主权的侵蚀和强化] // Наука, технологии и право [科技与法律]. – 2005. – № 4. – С. 71–74.
210. Чжан Синьбао, Сюй Кэ (Zhang Xinbao, Xu Ke). 网络空间主权的治理模式及其制度构建 (Модель управления суверенитетом в киберпространстве и ее институциональное построение) // 中国社会科学 (Китайские общественные науки). 2016. № 8. С. 319-339.
211. Чжан Тэнцзюнь (Zhang Tengjun). 再论国际电信联盟在全球互联网治理中的地位和作用 (Еще одна дискуссия о статусе и роли Международного союза электросвязи в глобальном управлении Интернетом) // 改革与开放 (Реформа и открытость). 2019. № 16. С. 14–16.
212. Чжан Хуэй (Zhang Hui). 新时代中国共产党网络战略论析——学习习近平总书记关于网络战略讲话的精神 (Обсуждение и анализ сетевой стратегии Коммунистической партии Китая в новую эпоху: изучение духа речей

- генерального секретаря Си Цзиньпина о сетевой стратегии) // 新闻传播 (Новостные коммуникации / News Dissemination). 2019. № 7. С. 141–144.
213. Чжан Цихоу и др. Серийные функциональные управления Министерства общественной безопасности КНР [張起厚 et al. 中共公安部的序列號職能局] // Журнал «Перспективы и исследования» [展望與探索月刊]. – 2011. – Т. 9. – № 3. – С. 99–121.
214. Чжан Чжаньцзян. Перспективы антимонопольного законодательства в области защиты персональной информации [张占江. 个人信息保护的反垄断法视角] // Китайская и зарубежная юриспруденция [中外法学]. – 2022. – Т. 34. – № 3. – С. 690–691.
215. Чжан Шудянь, Линь Жуйсинь (Zhang Shudian, Lin Ruixin). 论互联网对国家主权的侵蚀和强化 (Влияние Интернета на эрозию и укрепление государственного суверенитета) // 科技与法律 (Наука, технологии и право). 2005. № 4. С. 71–74
216. Чжан Янсэнь, Пэн Юаньюань, Дуань Юйсян, Чжэн Цзя, Ю Цзяньцин (Zhang Yang-Sen, Peng Yuan-Yuan, Duan Yu-Xiang, Zheng Jia, You Jian-Qing). 基于评论异常度的新浪微博谣言识别方法 (Метод выявления слухов в Sina Weibo на основе аномальности комментариев / The Method of Sina Weibo Rumor Detecting Based on Comment Abnormality) // 自动化学报 (Acta Automatica Sinica). 2020. Т. 46, № 8. С. 1689–1702.
217. Чжоу Ханьхуа. Об Интернет-законодательстве [周汉华. 论互联网法] // Китайская юридическая наука [中国法学]. – 2015. – № 3. – С. 31–32.

218. Чжу Шибин (Zhu Shibing). 世界范围内网络主权的主要观点综述 (Обзор основных взглядов на сетевой суверенитет в мировом масштабе) // 中国工程科学 (Инженерные науки Китая). 2016. № 18(06). С. 89–93.
219. Чэнь Хунмэй (Chen Hongmei). 全球互联网治理法治化思考 (Размышления о легализации глобального управления Интернетом) // 湘潭大学学报(哲学社会科学版) (Журнал Сянтаньского университета. Издание по философии и социальным наукам). 2019. № 43(01). С. 82–86.
220. Чэнь Чуньянь (Chen Chunyan). 试析《俄罗斯互联网主权法》的背景与影响 (Анализ предпосылок и влияния «Закона об интернет-суверенитете России») // 传媒: :MEDIA (Медиа). 2020. № 12. С. 50–55.
221. Ши Юци, Юй Сянпин. Ущемление свободы выражения мнений пользователей правом на регулирование онлайн-платформ и его регулирование в публичном праве [石佑启; 余相萍. 网络平台监管权对用户言论自由的侵害及其公法治理] // Гуандунские общественные науки [广东社会科学]. – 2023. – № 6. – С. 230–244.
222. Ши Яньхун, Цзо Лиминь. Интеграция интернет-технологий в работу сетевого законодательства Китая [史艳红, 左丽敏. 试论互联网技术对我国网络立法工作的推动] // Вестник Шэньсийского университета радио и телевидения [陕西广播电视大学学报]. – 2020. – Т. 25. – № 2. – С. 70–73.
223. Ян Линьюй (Yang Linyu). 网络主权视野下的互联网建设、运用、管理——“谷歌事件”的理性解读及其启示 (Строительство, использование и управление Интернетом в перспективе сетевого суверенитета: рациональная

интерпретация «инцидента Google» и его значение) // 云南行政学院学报 (Вестник Административного института Юньнани). 2011. № 1. С. 105–108.

224. Ян Фэн (Yang Feng). 全球互联网治理、公共产品与中国路径 (Глобальное управление Интернетом, общественные блага и путь Китая) // 教学与研究 (Преподавание и научные исследования). 2016. № 9. С. 51–58.

225. Ян Яньлэй. Обсуждение дилеммы реализации и контрмер по решению закона о сетевой безопасности [杨彦蕾. 《网络安全法》的实施困境与解决对策探讨] // Технологии и применение сетевой безопасности [网络安全技术与应用]. – 2022. – № 11. – С. 78–79.

Исследования на английском языке:

226. Alshehri M., Drew S. Implementation of E-Government: Advantages and Challenges // Proceedings of IASK E-ALT2010 Conference. 2010. P. 79–86.

227. Ayers C.E. Rethinking Sovereignty in the Context of Cyberspace // U.S. Army War College Journal, 2016. 1. P. 13–44.

228. Bilotta N. Beyond the Digital Tax: The Challenges of the EU's Scramble for Technological Sovereignty // International Organisations Research Journal. 2020. Vol. 15, no. 4. P. 30–47.

229. Brown R.E. The Global Foundations of Public Relations: Humanism, China and the West. Abingdon-on-Thames: Routledge, 2021. 232 p.

230. Caster M. The securitization of social media in China // China Brief. 2014. Vol. 14. Is. 3. URL: <http://www.jamestown.org/programs/chinabrief/single/>

txttnews%5Bttnews%5D=41934&txttnews%5BbackPid%5D=758&nocache=1(дата обращения: 03.11.2022)

231. Cohen J.E. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. – Oxford: Oxford University Press, 2019. – 366 p.
232. Cohen J.E. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford: Oxford University Press, 2019. 366 p.
233. Cook S. Testimony by S. Cook. 15.05.2014. URL: <http://www.uscc.gov/sites/default/files/CookWritten%20Testimony.pdf> (дата обращения: 02.11.2023)
234. Creemers R. Cybersecurity Law and Regulation in China: Securing the Smart State // *China Law and Society Review*. 2023. Vol. 6, no. 2. P. 111–145.
235. Deibert R. *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. Toronto: Signal (McClelland & Stewart), 2013. 336 p.
236. DeNardis L. *The Global War for Internet Governance*. New Haven: Yale University Press, 2014. – 288 p.
237. DeNardis L., Musiani F. Governance by Infrastructure // *The Turn to Infrastructure in Internet Governance*. London: Palgrave Macmillan, 2014. P. 3–21.
238. Denyer, Simon (23 May 2016). "China's scary lesson to the world: Censoring the Internet works" // *Washington Post*. URL: https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html (дата обращения 16.11.2020).
239. Ding Wei. The Making of Data Security Law in China: Framework, Issues and Future Trends // *Macau Journal of Global Legal Studies*. 2024. № 1. P. 141–185.

240. Du Ping, Yu Shiyang, Yang Daoling. The Development of E-Governance in China: Improving Cybersecurity and Promoting Informatization as Means for Modernizing State Governance. Research Series on the Chinese Dream and China's Development Path. New York: Springer, 2019. 357 p.
241. Erickson A.S. China Defense White Papers – 1995–2019. 23.07.2019. URL: <https://www.andrewerickson.com/2019/07/china-defense-white-papers-1995-2019-download-complete-set-read-highlights-here/> (дата обращения: 12.10.2023).
242. Esarey A., Kluver R. The Internet in China: Cultural, Political, and Social Dimensions (1980s–2000s). Great Barrington, MA: Berkshire Publishing Group, 2015. 272 p.
243. Greenleaf G. China's Completed Personal Information Protection Law: Rights Plus Cyber-security // Privacy Laws & Business International Report. 2021. No. 172. P. 20–23.
244. Halgand D. Statement by D. Halgand, US Director, Reporters Without Borders. 15.05.2014. URL: <http://www.uscc.gov/sites/default/files/HalgandWritten%20Testimony.pdf> (дата обращения: 02.11.2024)
245. Hillman J.E. The Digital Silk Road: China's Quest to Wire the World and Win the Future. New York: Harper Business, 2021. 368 p.
246. Holmes D. Communication theory: media, technology, society. N.Y.: SAGE Publications Ltd, 2005.
247. Hoti L., Dermaku K., Klaiqi S., Dermaku H. Protection and Exchange of Personal Data on the Web in the Registry of Civil Status // Emerging Science Journal. 2023. Vol. 7. P. 38–49.

248. Jiang M. Managing the Micro-Self: The Governmentality of Real Name Registration Policy in Chinese Microblogosphere // *Information, Communication & Society*. 2016. Vol. 19, no. 2. P. 203–220.
249. Jiang Y. *Social Media and e-Diplomacy in China: Scrutinizing the Power of Weibo*. New York: Palgrave Pivot, 2017. 159 p.
250. Kaye D. *Speech Police: The Global Struggle to Govern the Internet*. New York: Columbia Global Reports, 2019. 142 p.
251. Kello L. *The Virtual Weapon and International Order*. New Haven: Yale University Press, 2017. 336 p.
252. King G., Pan J., Roberts M. Reverse-engineering censorship in China: randomized experimentation and participant observation // *Science*. 2014. Vol. 345. No. 6199.
253. Kostka G. China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval // *New Media & Society*. 2019. Vol. 21, no. 7. P. 1565–1593.
254. Lum Th. *Internet development and information control in the PRC*. Washington, DC, 2006.
255. Lyon D. *Surveillance Studies: An Overview*. Cambridge: Polity Press, 2007. 243 p.
256. Major P. Internet Governance: Trends and Realities. Part 1 // *Biznes-Informatika*. 2015. № 4(34). P. 7–14. DOI: 10.17323/1998-0663.2015.4.7.14; Major P. Internet Governance: Trends and Realities. Part 2 // *Biznes-Informatika*. 2016. № 1(35). P. 20–25.
257. Mark L., Chang M. Strictest Amendment to China's Cybersecurity Law in Effect [Электронный ресурс] // Haynes Boone. 4 p. URL:

<https://www.haynesboone.com/news/alerts/strictest-amendment-to-chinas-cyber-security-law-in-effect.pdf> (дата обращения: 2.03.2026).

258. Martin P. *China's Civilian Army: The Making of Wolf Warrior Diplomacy*. Oxford: Oxford University Press, 2021. 320 p.
259. Mckune S. & Ahmed S. The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda // *International Journal of Communication*, 2018. 12. P. 35–55.
260. Moss G. Digital Regulation and Questions of Legitimacy // *Policy & Internet*. 2025. P. 1–10.
261. Mueller M. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: The MIT Press, 2010. 320 p.
262. Nissenbaum H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press, 2009. 304 .
263. Nwambuko, Temple C., Eyikorogha, Q., Chigozie, Joy N. (2025). Digital Governance and E-Government Transformation in Public Service Delivery in Nigeria. *International Journal of Current Science Research and Review*, 8(10), pp. 5038-5047.
264. Nye J. *Cyber Power*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010. 24 p.
265. Oberheitmann A., Heupel T., Yang J., Wang Z. *German and Chinese Contributions to Digitalisation: Opportunities, Challenges and Impacts*. München: Springer Gabler, 2020. 383 p.
266. Perry H., Adan S.N., Malik N., Knight S. *Advancing Digital Rights in 2025: Trends, Challenges, and Opportunities in the UK, EU and Global Landscape // Demos*. 2025. 80 p.

267. Qiuqing Tai. China's Media Censorship: A Dynamic and Diversified Regime // *Journal of East Asian Studies*, 14 (2014). P. 185–209.
268. Rid T. *Cyber War Will Not Take Place*. Oxford: Oxford University Press, 2013. 218 p.
269. Sacks S. *Addressing the Data Security Risks of U.S.-China Technology Entanglement*. – Washington, DC: Brookings Institution, 2020. – (report, PDF).
270. Sacks S. *Addressing the Data Security Risks of US-China Technology Entanglement* [Электронный ресурс]. Washington, DC: Brookings Institution, 2020. URL: <https://www.brookings.edu/wp-content/uploads/2020/11/Samm-Sacks.pdf> (дата обращения: 12.02.2023).
271. Schneider F. *China's Digital Nationalism*. New York: Oxford University Press, 2018. 291 p.
272. Seifert J.W., Chung J. *Using E-Government to Reinforce Government Citizen Relationships: Comparing Government Reform in the United States and China*. London: Routledge, 2020. 184 p.
273. Shlaeger J. *E-Government in China: Technology, Power and Local Government Reform*. China Policy Series. London: Routledge, 2020. 184 p.
274. Sullivan J. A Tale of Two Microblogs in China // *Media, Culture & Society*. 2012. Vol. 34, no. 6. P. 773–783.
275. Testimony by S. Cook. 15.05.2014. URL: <http://www.uscc.gov/sites/default/files/CookWritten%20Testimony.pdf> (дата обращения: 02.11.2023)
276. Toma P.-S. An Overview of China's Development in Cyberspace // *International Journal of Cyber Diplomacy*. 2024. Vol. 5. P. 41–52.
277. Tufekci Z. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven; London: Yale University Press, 2017. 360 p.

278. Valeriano B., Jensen B., Maness R. Cyber Strategy: The Evolving Character of Power and Coercion. New York: Oxford University Press, 2018. 288 p.
279. Wang A. Cyber Sovereignty at its Boldest: a Chinese Perspective // The Ohio State Technology Law Journal. 2020. 16 (2). P. 395–466.
280. Webster G. (ed.). Translation: Data Security Law of the People’s Republic of China (Effective Sept. 1, 2021). – Stanford, CA: DigiChina (Stanford University), 2021.
281. West D.M. E-Government and the Transformation of Service Delivery and Citizen Attitudes // Public Administration Review. 2004. Vol. 64, no. 1. P. 15–27.
282. Zhou Q., Ge E., Chen X., Xu X. Digital Government Leads to Economic Development: Mechanism and Evidence // Journal of Management Science China. 2023. Vol. 40. P. 49–68.

Статистические и аналитические материалы:

На китайском языке:

283. 第 47 次《中国互联网络发展状况统计报告》(47-й «Статистический отчет о состоянии развития интернета в Китае») [Электронный ресурс] // Официальный сайт CNNIC. URL: <https://www.cnnic.com.cn/IDR/ReportDownloads/202104/P020210420557302172744.pdf> (дата обращения: 24.01.2025).
284. 第 53 次《中国互联网络发展状况统计报告》发布：我国网民规模达 10.92 亿人 (53-й «Статистический отчет о развитии интернета в Китае»: численность интернет-пользователей достигла 1,092 млрд человек)

- [Электронный ресурс] // Официальный сайт газеты «Жэньминь жибао». URL: <http://finance.people.com.cn/n1/2024/0322/c1004-40201311.html> (дата обращения: 24.01.2025).
285. 中国信息社会发展报告 2016 (Доклад о развитии информационного общества в Китае, 2016 г.) [Электронный ресурс] // Официальный сайт Государственного информационного центра КНР. URL: https://www.sic.gov.cn/sic/82/566/0518/6358_pc.html (дата обращения: 24.01.2026)
286. 《数字中国发展报告 (2024 年) 》 (Доклад о развитии цифрового Китая, 2024 г.) [Электронный ресурс] // Официальный сайт Национального управления по делам данных КНР. URL: <https://www.nda.gov.cn/sjj/zhuanti/sjzgzxd/szzgbg/0605/ff808081-96b465bf-0197-3dd5a76f-05c7.pdf> (дата обращения: 24.01.2026).
287. 中国数字经济发展指数报告 2023 (Доклад об индексе развития цифровой экономики Китая, 2023 г.) [Электронный ресурс] // Официальная публикация Пятого исследовательского института Министерства промышленности и информатизации КНР. URL: <https://13115299.s21i.faiusr.com/61/1/ABUIABA9GAAG1c2ypwYotKiqzQQ.pdf> (дата обращения: 24.01.2026).
288. 国家互联网信息办公室发布《数字中国发展报告 (2022 年) 》 (Национальное управление по делам киберпространства опубликовало «Доклад о развитии цифрового Китая, 2022 г.») [Электронный ресурс] // Официальный сайт Центрального интернет-информационного офиса КНР. URL: https://www.cac.gov.cn/2023-05/22/c_1686402318492248.htm (дата обращения: 24.01.2025).

289. 《中国互联网发展报告 2024》和《世界互联网发展报告 2024》蓝皮书发布 (Публикация синих книг «Доклад о развитии интернета в Китае 2024» и «Доклад о развитии мирового интернета 2024») [Электронный ресурс] // Официальный сайт Всемирной интернет-конференции. URL: https://cn.wicinternet.org/2024-11/21/content_37691639.htm (дата обращения: 24.01.2026).
290. 2024 年版《中国信息产业年鉴》出版发行 (Публикация издания 2024 года «Ежегодник информационной индустрии Китая») [Электронный ресурс] // Официальный сайт Национального исследовательского центра по промышленной информационной безопасности КНР. URL: https://www.cics-cert.org.cn/webapp/webpage/articlecontent_103005_1995786318059147265.html (дата обращения: 12.12.2025).
291. 中国互联网络发展状况统计报告 (Статистический доклад о развитии интернета в Китае: 53-й, 54-й, 55-й доклады, 2024–2025 гг.) [Электронный ресурс] // Официальный сайт CNNIC. URL: <https://www.cnnic.com.cn/IDR/ReportDownloads/> (дата обращения: 24.01.2026).
292. 中国统计年鉴 2021 (Статистический ежегодник Китая, 2021 г.) [Электронный ресурс] // Официальный сайт Национального бюро статистики КНР. URL: <https://www.stats.gov.cn/sj/ndsj/2021/indexch.htm> (дата обращения: 24.01.2025).
293. 中国统计年鉴 2022 (Статистический ежегодник Китая, 2022 г.) [Электронный ресурс] // Официальный сайт Национального бюро статистики КНР. URL: <https://www.stats.gov.cn/sj/ndsj/2022/indexch.htm> (дата обращения: 24.01.2025).

294. 中国统计年鉴 2023 (Статистический ежегодник Китая, 2023 г.)
[Электронный ресурс] // Официальный сайт Национального бюро статистики КНР. URL: <https://www.stats.gov.cn/sj/ndsj/2023/indexch.htm> (дата обращения: 24.01.2025).
295. 中国统计年鉴 2024 (Статистический ежегодник Китая, 2024 г.)
[Электронный ресурс] // Официальный сайт Национального бюро статистики КНР. URL: <https://www.stats.gov.cn/sj/ndsj/2024/indexch.htm> (дата обращения: 24.01.2025).
296. 中国统计年鉴 2025 (Статистический ежегодник Китая, 2025 г.)
[Электронный ресурс] // Официальный сайт Национального бюро статистики КНР. URL: <https://www.stats.gov.cn/sj/ndsj/2025/indexch.htm> (дата обращения: 24.01.2026).
297. 中国电子信息产业统计年鉴 (Статистический ежегодник электронной и информационной промышленности Китая) [Электронный ресурс] // Информационный ресурс по отраслевой статистике КНР. URL: <https://www.shujuku.org/electronic-information-industry-statistical-yearbook.html> (дата обращения: 12.01.2026).

На английском языке:

298. Barroca J., Kishnani P., Eggers W.D., Manstof J. Seven Pivots for Government's Digital Transformation: How COVID-19 Proved the Importance of "Being" Digital [Электронный ресурс] // Deloitte Insights. URL: <https://www.deloitte.com/us/en/insights/industry/government-public-sector-services/government-digital-transformation-strategy.html> (дата обращения: 12.04.2024).

299. Alibaba Group Holding Limited Annual Report 2023 (Годовой отчет Alibaba Group Holding Limited за 2023 финансовый год) [Электронный ресурс] // Официальный сайт компании Alibaba Group. URL: <https://static.alibabagroup.com/reports/fy2023/ar/ebook/en/index.html> (дата обращения: 26.10.2024).
300. Tencent Annual Report 2024 (Годовой отчет Tencent Holdings Limited за 2024 год) [Электронный ресурс] // Официальный сайт компании Tencent. URL: <https://static.www.tencent.com/uploads/2025/04/08/1132b72b565389d1b913aea60a648d73.pdf> (дата обращения: 24.04.2025).
301. 国家统计局 2023 年法治政府建设年度报告 (Годовой отчет о работе Национального бюро статистики КНР по построению правового правительства за 2023 год) [Электронный ресурс] // Официальный сайт Национального бюро статистики КНР. URL: https://www.stats.gov.cn/zt_18555/tjfz/tjfzjs/fzjsdt/202406/t20240607_1954458.html (дата обращения: 24.03.2025).
302. Baidu 2023 Environmental, Social and Governance Report (Отчет Baidu в области экологии, социальной ответственности и корпоративного управления за 2023 год) [Электронный ресурс] // Официальный сайт компании Baidu. URL: https://esg.baidu.com/Uploads/Baidu_2023_ESG_Report.pdf (дата обращения: 24.01.2025).
303. Baidu 2024 Environmental, Social and Governance Report (Отчет Baidu в области экологии, социальной ответственности и корпоративного управления за 2024 год) [Электронный ресурс] // Официальный сайт компании Baidu. URL: https://esg.baidu.com/Uploads/Baidu_2024_ESG_Report.pdf (дата обращения: 24.05.2025).

Материалы СМИ

На китайском языке:

304. 抖音启动暑期未成年人网络保护专项治理 将重点关注不良内容等五大问题 (Douyin запускает специальную летнюю кампанию по защите несовершеннолетних в интернете, сосредоточив внимание на пяти основных проблемах, включая вредный контент) [Электронный ресурс] // Информационная служба «Синьхуа Финанс». URL: <http://www.xinhuanet.com/tech/20230705/4d961a0ba2314206a177d70332221ef9/c.html> (дата обращения: 26.04.2025).
305. 中央网信办首次面向社会公开选拔 9 名处级干部 (Впервые Управление по делам киберпространства публично выбрало 9 руководителей на уровне департаментов) [Электронный ресурс] // Информационное агентство «Синьхуа». URL: https://web.archive.org/web/20141111204433/http://news.xinhuanet.com/renshi/2014-10/27/c_1112997728.htm (дата обращения: 08.03.2026).
306. 国务院印发《新一代人工智能发展规划》 (Государственный совет КНР опубликовал «План развития искусственного интеллекта следующего поколения») [Электронный ресурс] // Baidu Baike. URL: https://baike.baidu.com/reference/22036716/475aVSLX5I8spJvSGGHMyw8mvoxctVt_Glu5CFwg0c28t0ivPCaMbFjhNwFj6JCrHppJRq0DPztfj2xdGckvww4ubLMxtlRcnCXolzuhPnzOT6ye (дата обращения: 08.03.2026).
307. 全国网警部门集体在抖音开账号，将建“网警一键举报”机制 (Департаменты сетевой полиции по всей стране коллективно открыли учетные записи в Douyin; будет создан механизм «сообщить сетевой полиции в один клик») [Электронный ресурс] // Интернет-портал Sohu. URL: https://www.sohu.com/a/253861358_161795 (дата обращения: 08.03.2026).

308. 武汉市委网信办：加快建设国家网络安全人才与创新基地 (Информационное бюро по делам интернета Уханьского муниципального комитета партии: ускорение создания Национального центра инноваций и подготовки кадров в сфере информационной безопасности) [Электронный ресурс] // Интернет-портал Sohu. URL: https://www.sohu.com/a/414443513_697216 (дата обращения: 08.03.2026).
309. 国家网信办重组：国务院授权其负责互联网内容管理执法 (Реорганизация Управления по делам киберпространства: Государственный совет КНР уполномочил его отвечать за регулирование интернет-контента и надзорно-правоприменительную деятельность) [Электронный ресурс] // Guancha.cn. URL: http://www.guancha.cn/politics/2014_08_28_261572.shtml (дата обращения: 08.03.2026).
310. 中国网警化暗为明 亮相执法 (Сетевая полиция Китая выходит из тени и впервые публично приступает к правоприменению) [Электронный ресурс] // Газета Liberty Times. URL: <https://news.ltn.com.tw/news/world/paper/885594> (дата обращения: 08.03.2026).
311. 快速崛起的国家网安基地吸引各国专家目光 (Стремительный рост Национального центра инноваций и подготовки кадров в сфере информационной безопасности привлекает внимание экспертов со всего мира) [Электронный ресурс] // Baidu Baike. URL: https://baike.baidu.com/reference/23211018/8350akGjPXOt0d90mTXZmmGt87i_HJcPNKiVtVYjao42yE5CQKZQtswbvh4zDXYhoD-8Jx7VdSZ7stcb2eIliCii23ZxDcBhbS_BgNRVr2o (дата обращения: 08.03.2026).
312. 加强网络法治建设 促进新技术新应用健康有序发展 (Укрепление правового регулирования киберпространства для содействия здоровому и упорядоченному развитию новых технологий и приложений) [Электронный

- ресурс] // Информационное агентство «Синьхуа». URL: <http://www.xinhuanet.com/tech/20240621/3e34ba6feada4a73ae55384973365d34/c.html> (дата обращения: 26.04.2025).
313. 中共中央印发《深化党和国家机构改革方案》(Центральный комитет Коммунистической партии Китая издал «План углубления партийных и государственных институциональных реформ») [Электронный ресурс] // Информационное агентство «Синьхуа». URL: https://web.archive.org/web/20200530162114/http://www.xinhuanet.com/2018-03/21/c_1122570517.htm (дата обращения: 08.03.2026).
314. 中共中央印发《深化党和国家机构改革方案》(Центральный комитет Коммунистической партии Китая опубликовал «План углубления партийных и государственных институциональных реформ») [Электронный ресурс] // Информационное агентство «Синьхуа». URL: http://www.xinhuanet.com/zgjx/2018-03/21/c_137054755.htm (дата обращения: 08.03.2026).
315. 中共中央 国务院印发《数字中国建设整体布局规划》(ЦК КПК и Государственный совет КНР выпустили «Всесторонний план построения цифрового Китая») [Электронный ресурс] // Информационное агентство «Синьхуа». URL: https://www.news.cn/politics/2023-02/27/c_1129401407.htm (дата обращения: 08.03.2026).
316. 中共中央 国务院印发《党和国家机构改革方案》(ЦК КПК и Государственный совет КНР выпустили «План партийно-государственных институциональных реформ») [Электронный ресурс] // Baidu Baike. URL: https://baike.baidu.com/reference/62745119/ea95yQiBuN-ymwY-wXLIYUuoTWg5y7iTrsNGfOPrXgRfouDYAtAP83JFOd9_FrM93E3KVvrAAzF

AY4YVr9r9P4Iqzu5K0PQACS5Ke8sX0HC1OgoNs0Z-XXQ (дата обращения: 08.03.2026).

317. 中共中央印发《深化党和国家机构改革方案》(ЦК КПК издал «План углубления партийных и государственных институциональных реформ») [Электронный ресурс] // Baidu Baike. URL: https://baike.baidu.com/reference/4179928/f0f11Tl5ShjN-gBevQ73zF70U-F-t6mUFssv7ZD4hWJ3vWvIIPqZP8iDpAyHWAdmupiuFYUWTnD1-N8KVZPY51N5QricNakhDu_9ysQGyz2synkCW_h_doZZ (дата обращения: 08.03.2026).

На английском языке:

318. China Launches Artificial Intelligence Platform to Boost Judicial Efficiency (Китай запускает платформу искусственного интеллекта для повышения эффективности правосудия) [Электронный ресурс] // Официальный сайт газеты China Daily. URL: <https://www.chinadaily.com.cn/a/202412/02/WS674d1673a310f1265a1d0785.html> (дата обращения: 26.04.2025).
319. China Strives to Protect Underage Internet Users (Китай прилагает усилия для защиты несовершеннолетних пользователей Интернета) [Электронный ресурс] // Официальный сайт China Daily Hong Kong. URL: <https://www.chinadailyhk.com/hk/article/289656> (дата обращения: 26.04.2025).
320. China Tightens Restrictions on Messaging Apps (Китай ужесточает ограничения для приложений обмена сообщениями) [Электронный ресурс] // Официальный сайт The Wall Street Journal. URL: <http://online.wsj.com/articles/china-issues-new-restrictions-on-messaging-apps-1407405666> (дата обращения: 25.10.2023).

321. China's Cyberspace Environment Improves amid Intensified Efforts (Киберпространственная среда Китая улучшается на фоне активизации усилий) [Электронный ресурс] // Официальный сайт газеты China Daily. URL: <https://www.chinadaily.com.cn/a/202407/30/WS66a85568a31095c51c510baf.html> (дата обращения: 26.04.2025).
322. China's Great Firewall Descends on Hong Kong Internet Users (Великий китайский файрвол спускается на интернет-пользователей Гонконга) [Электронный ресурс] // Официальный сайт The Guardian. URL: <https://www.theguardian.com/world/2020/jul/08/china-great-firewall-descends-hong-kong-internet-users> (дата обращения: 09.03.2024).
323. China's Internet: 30 Years of Control and Censorship (Интернет Китая: 30 лет контроля и цензуры) [Электронный ресурс] // Официальный сайт BBC News. URL: <https://www.bbc.com/news/technology-35112856> (дата обращения: 08.03.2026).
324. China's Search Engines Have More than 66,000 Rules Controlling Content, Report Says (Поисковые системы Китая имеют более 66 000 правил, контролирующих контент, говорится в докладе) [Электронный ресурс] // Официальный сайт The New York Times. URL: <https://www.nytimes.com/2023/04/26/business/china-censored-search-engine.html> (дата обращения: 26.04.2024).
325. China's Xi Pitches Shared Future in Cyberspace at Internet Forum amid Decoupling Fears (Си Цзиньпин призывает к совместному будущему в киберпространстве на интернет-форуме на фоне опасений по поводу разделения) [Электронный ресурс] // Официальный сайт газеты South China Morning Post. URL: <https://www.scmp.com/tech/policy/article/3287342/chinas-xi-pitches-shared-future-cyberspace-internet-forum-amid-decoupling-fears> (дата обращения: 26.04.2024).

326. Cyberspace Agencies to Work Harder to Prevent Online Bullying (Киберпространственные ведомства будут активнее работать над предотвращением онлайн-травли) [Электронный ресурс] // Официальный сайт газеты China Daily. URL: <https://www.chinadaily.com.cn/a/202303/16/WS64129dbea31057c47ebb4d76.html> (дата обращения: 26.04.2025).
327. Cyberspace Cleanup Targets Rumormongering Accounts (Очистка киберпространства направлена против аккаунтов, распространяющих слухи) [Электронный ресурс] // Официальный сайт газеты China Daily. URL: <https://www.chinadaily.com.cn/a/202305/29/WS64740268a310b6054fad583b.html> (дата обращения: 26.04.2025).
328. How China's Internet Police Went from Targeting Bloggers to Their Followers (Как китайская интернет-полиция перешла от преследования блогеров к их подписчикам) [Электронный ресурс] // Официальный сайт The Guardian. URL: <https://www.theguardian.com/world/article/2024/sep/02/how-chinas-internet-police-went-from-targeting-bloggers-to-their-followers> (дата обращения: 08.03.2026).
329. How the Chinese Communist Party Controls China's Internet (Как Коммунистическая партия Китая контролирует китайский интернет) [Электронный ресурс] // Официальный сайт Foreign Policy. URL: <https://foreignpolicy.com/2024/02/18/china-internet-control-ccp-technology-cyber-surveillance-policy-sentinel-state/> (дата обращения: 08.03.2026).
330. Is TikTok Different in China? Here's What to Know (Чем отличается TikTok в Китае? Вот что нужно знать) [Электронный ресурс] // Официальный сайт ABC News. URL: <https://abcnews.go.com/Business/tiktok-china/story?id=108111708> (дата обращения: 26.04.2025).

331. Security in Cyberspace Facing New Challenges (Безопасность в киберпространстве сталкивается с новыми вызовами) [Электронный ресурс] // Официальный сайт газеты China Daily. URL: <https://www.chinadaily.com.cn/a/202110/12/WS6164d8d5a310cdd39bc6e3c8.html> (дата обращения: 26.04.2025).
332. The Chinese Version of TikTok Is Limiting Kids to 40 Minutes a Day (Китайская версия TikTok ограничивает использование детьми до 40 минут в день) [Электронный ресурс] // Официальный сайт CNN. URL: <https://www.cnn.com/2021/09/20/tech/china-tiktok-douyin-usage-limit-intl-hnk/index.html> (дата обращения: 26.04.2025).
333. Xi Calls for Letting Internet Better Benefit People of All Countries (Си Цзиньпин призвал обеспечить, чтобы Интернет лучше служил народам всех стран) [Электронный ресурс] // Официальный сайт агентства «Синьхуа». URL: <https://english.news.cn/20231108/2b2fc5176a334f408c80980ceb0814e3/c.html> (дата обращения: 26.04.2024).
334. Xi Jinping Calls for ‘Solid’ Security Barrier around China’s Internet (Си Цзиньпин призывает создать прочный барьер безопасности вокруг китайского Интернета) [Электронный ресурс] // Официальный сайт агентства Reuters. URL: <https://www.reuters.com/world/china/xi-calls-solid-security-barrier-around-chinas-internet-2023-07-15/> (дата обращения: 26.04.2025).
335. Xi: Take Cyberspace to New Level (Си Цзиньпин: вывести киберпространство на новый уровень) [Электронный ресурс] // Официальный сайт газеты China Daily. URL: <https://www.chinadaily.com.cn/a/202311/09/WS654c17d8a31090682a5ed302.html> (дата обращения: 26.04.2025).

336. Xinhua Headlines: Xi Outlines Blueprint to Develop China's Strength in Cyberspace (Главные новости «Синьхуа»: Си Цзиньпин представил план по укреплению позиций Китая в киберпространстве) [Электронный ресурс] // Официальный сайт агентства «Синьхуа». URL: http://www.xinhuanet.com/english/2018-04/21/c_137127374.htm (дата обращения: 26.04.2025).