

Том 4, № 2, 2020

# ПУБЛИЧНАЯ ПОЛИТИКА

*COVID-19 и социально-политические  
изменения: проблемы и возможности  
в условиях новой реальности*

*Коронавирус и публичная коммуникация:  
проблемы и тенденции*

*Постэпидемия. Основные изменения  
в России и мире*

*Пандемия и политические институты:  
специфика воздействия*

*Публичная политика и современные  
угрозы государственному управлению*

Балаян Александр, Томин Леонид

# Цифровая автократия. Институциональная специфика отношений государства и IT-компаний<sup>1</sup>

**Балаян Александр Александрович** –

кандидат политических наук, доцент  
департамента политологии и междуна-  
родных отношений НИУ ВШЭ – СПб.

Для связи с автором:  
[alexandr1138@mail.ru](mailto:alexandr1138@mail.ru)

**Томин Леонид Владимирович** –

кандидат политических наук, доцент  
кафедры политического управления  
Санкт-Петербургского  
государственного университета.

Для связи с автором:  
[leopolit@yandex.ru](mailto:leopolit@yandex.ru)

**Для цитирования:**

Балаян А.А., Томин Л.В. Цифровая  
автократия. Институциональная  
специфика отношений государства  
и IT-компаний // Публичная политика.  
2020. Т. 4. № 2.

<https://doi.org/10.31856/jpp/2020.2.6>

**Аннотация**

Статья посвящена исследова-  
нию генеалогии моделей цифровых  
автократий как исторической кон-  
стелляции экономических, полити-  
ческих и технологических факторов.  
Они сформировались как ответ на  
ряд вызовов: адаптация к трансфор-  
мирующейся неолиберальной эконо-  
мической системе, сохранение  
социально-политической стабильно-  
сти в условиях дальнейших рыночных  
реформ и реакция на ряд внешнепо-  
литических конфликтов.

**Ключевые слова:** цифрови-  
зация, управляемость, автократия,  
большие данные, неолиберализм.

<sup>1</sup> Работа выполнена при поддержке гранта РФФ «Политическая онтология цифровизации: исследование институциональных оснований цифровых форматов государственной управляемости» № 19-18-00210.

Balayan Alexandr, Tomin Leonid

# Digital autocracy. Institutional specifics of relations between the state and IT companies \*

**Balayan Alexandr Aleksandrovich –**

*Associate professor,  
Department of Political Science and  
International Affairs  
HSE Campus in St. Petersburg.*

*To contact the author:  
alexandr1138@mail.ru*

**Tomin Leonid Vladimirovich –**

*Associate professor,  
Department of political governance  
St. Petersburg University.*

*To contact the author:  
leopolit@yandex.ru*

**Abstract**

The article is devoted to the study of the genealogy of models of digital autocracies as a historical constellation of economic, political and technological factors. They were formed as a response to a number of challenges: adaptation to the transforming neoliberal economic system, the preservation of socio-political stability in the context of further market reforms and a reaction to a number of foreign policy conflicts.

**Keywords:** digitalization, governability, autocracy, big data, neoliberalism.

---

\* This work was supported with a grant from the Russian Science Foundation (grant 19-18-00210 “Political ontology of digitalization: Study of institutional bases for digital forms of governability”).

Одним из эффектов политики государств по контролю над перемещением населения в условиях пандемии коронавируса стало осознание многими гражданами механизмов мониторинга и контроля повседневной жизни посредством цифровой инфраструктуры [Rule, Cheng 2020]. Экстраординарные меры, предпринятые правительствами, воплотили в реальность алармистские прогнозы итальянского философа Д. Агамбена о «биополитике» как новой формирующейся модели управления и «перманентном чрезвычайном положении» [Agamben 2005].

В последние годы вышло множество работ, посвященных различным негативным эффектам цифровизации: растущему государственному и корпоративному контролю над жизнью граждан [Zuboff 2019; Bloom 2019], растущему экономическому неравенству [Eubanks 2018] и непрозрачности цифровых алгоритмов управления [Pasquale 2015; Bridle 2019]. Большинство подобных исследований посвящено государствам, которые в различных индексах (Polity IV, Freedom House) относят к демократиям. Цифровизация в условиях кризиса неolibеральной политико-экономической модели способствует дополнительному усилению ее технократических (и немажоритарных) практик управления [Майр 2019: 23–27].

Существуют отдельные работы, посвященные китайской системе социального кредита, но пока недостаточно концептуально осмыслен сам феномен использования цифровых технологий различными автократиями (однопартийными, популистскими, электоральными). Одной из центральных тем подобных будущих исследований может стать цифровизация государственного управления и экономики в автократиях. Ряд уже имеющихся работ демонстрирует, что цифровизация дает автократическим и гибридным режимам новые механизмы управления и социального контроля [Морозов 2014; Howard 2011].

В последние годы появляются эмпирические исследования механизмов функционирования цифровых автократий, осуществленные на примерах ряда стран [Burgers, Robinson 2016; Meissner, Wübbecke 2016]. Политологи для именованя этой новой модели используют различные названия: «цифровой авторитаризм» (*digital authoritarianism*), «сетевой авторитаризм» (*networked authoritarianism*) [Pearce, Kendzior 2012]. Тема «возвышения цифровых автократий» отмечена как главная в ежегодном докладе организации Freedom House, посвященном свободе интернета (2018 г.) [Freedom on the Net 2018]. События последних лет демонстрируют, что одним из механизмов стабилизации и легитимации режима правящие элиты автократий выбрали управляемую и контролируруемую сверху цифровизацию.

В 1990-е – начале 2000-х гг. в обсуждении цифровизации и влияния интернета доминировала оптимистическая (иногда даже утопическая)

точка зрения. Интернет описывался как децентрализованная (анархическая, ризоморфная) система, формирующая новую прогрессивную модель экономики (открытая, коллаборативная, экологичная) и политики (сетевые модели управления, возрождение прямой демократии). Авторитариям с их системами цензуры в этом цифровом мире не было места, считалось, что они не смогут выжить в условиях свободно циркулирующих информационных потоков. Кибероптимисты полагали, что для либерализации и демократизации необходимо лишь повсеместное распространение интернета и помощь гражданскому обществу [Томин, Балаян 2016: 61–64].

В тот период лишь отдельные исследователи отмечали амбивалентную роль интернета в процессе демократизации политического режима. В 2003 г. Ш. Калатхил и Т. Боас писали: «Основываясь на систематическом исследовании восьми кейсов: КНР, Куба, Сингапур, Вьетнам, Мьянма, Объединенные Арабские Эмираты, Саудовская Аравия и Египет, мы утверждаем, что интернет не обязательно представляет угрозу авторитарным режимам. Некоторые виды использования интернета могут формировать политические вызовы авторитарным правительствам и служить политическим изменениям в будущем. Несмотря на это, другие виды использования интернета укрепляют авторитарное правление, многие авторитарные режимы активно продвигают развитие интернета, служащего интересам, установленным государством» [Kalathil, Boas 2003].

Формирование политико-экономической модели цифровых автократий необходимо рассматривать в связи с особенностями адаптации ряда государств к неолиберализму. Появление цифровых автократий не было результатом изначального плана правящего класса по политическому использованию интернета. Это констелляция множества факторов, связанных с трансформацией неолиберализма и адаптацией к этому стран в различных регионах, с технологическим развитием экономики больших данных и конфликтами на международной арене.

Прежде чем перейти к анализу цифровых автократий, необходимо описать глобальные экономические изменения, сформировавшие цифровую инфраструктуру для экономики больших данных («капитализм платформ», «надзорный капитализм»). В качестве методологической основы для исследования трансформации неолиберализма, формирования платформенной экономики мы используем концепции неомарксистских теоретиков: Н. Срничека, Дж. Б. Фостера, Р. МакЧесни.

По мнению этих авторов, модель «капитализма платформ» (или «надзорного капитализма») стала результатом длительной трансформации капиталистической экономики под воздействием внутренних структурных противоречий. В 1960-е – начале 1970-х гг. в странах капиталистического ядра

произошел значительный спад уровня прибыли в промышленности, в середине 1970-х – 1980-е гг. в ходе неолиберальных реформ началась финансиализация экономики, позволившая поддержать рынки и отложить кризис [Срничек 2019: 18–20]. Произошел фундаментальный сдвиг от экономики, основанной на промышленном производстве, к доминированию финансового сектора. Однако эти меры не стабилизировали экономику в среднесрочной перспективе, финансовый капитал в погоне за прибылью стал создавать пузыри в различных секторах, сделав кризисное состояние перманентным [Foster, McChesney 2014].

Важнейшими структурными предпосылками формирования экономики больших данных были приватизация интернета и дерегулирование рынка телекоммуникаций. В США приватизация интернета проходила в несколько этапов и завершилась только в 1995 г. [Levine 2019: 116–128]. После приватизации National Science Foundation Network интернет-инфраструктура перешла во владение частных компаний. В 1996 г. администрация Б. Клинтона утвердила «Закон о телекоммуникациях», ликвидировавший многие регуляторные меры и ограничения. Итогом изменений стало повышение уровня концентрации во многих сферах. Например, большинство средств массовой информации оказались в руках всего нескольких медиакорпораций (Fox Corporation, AT&T, Comcast, ViacomCBS). В 1999 г. был принят «Закон о финансовой модернизации», в результате произошла еще большая концентрация капитала и финансиализация экономики.

В условиях возросшей финансиализации избыточному капиталу были необходимы новые сферы вложения, одной из них стала интернет-экономика. Первый бум «новой экономики» (1995–2001) продлился недолго – эйфория закончилась, когда лопнул пузырь доткомов. Итогом схлопывания пузыря доткомов стала концентрация и централизация капитала в интернет-экономике, по мечтам о децентрализованной экономике стартапов и небольших компаний был нанесен ощутимый удар. После мирового финансового кризиса 2008 г. IT-компании привлекли огромные объемы инвестиций, позволив на время решить проблему вложения избыточного капитала и поддержки финансового рынка [Срничек 2019: 35–36].

Дж. Б. Фостер и Р. МакЧесни отмечают: «...с конца 2010-х гг. интернет играет ключевую роль в процессе накопления капитала, компании, доминирующие в интернете, являются практически монополиями. Это не означает, что данные компании контролируют все 100 % объема продукции, – скорее, они продают достаточное количество, чтобы контролировать цену продукта и уровень конкуренции. В 2014 г. три из четырех крупнейших американских корпораций (по рыночной стоимости): Apple, Microsoft и Google – были интернет-монополиями. <...> Эти компании используют “сетевые эффекты”,

технические стандарты, патентное право и старые добрые входные барьеры для сохранения своей рыночной власти» [Foster, McChesney 2014].

Основа бизнес-модели платформенных компаний – монетизация пользовательских данных. Их сбор осуществляется посредством продуктов и сервисов, предоставляемых бесплатно (социальные сети, поисковые системы, приложения). Сформировалась интегрированная цифровая инфраструктура, постепенно включающая в себя традиционную физическую инфраструктуру. «В промышленную эпоху экономическая деятельность строилась на физической инфраструктуре, которая представлена железными дорогами, автодорогами и аэропортами. Для цифровых технологий нужна новая инфраструктура – информационная: сети и облачные вычисления. Развитие цифровой экономики расширило понятие цифровой инфраструктуры, включив в него широкополосные, беспроводные сети, а также цифровизацию традиционной физической инфраструктуры – например, установку датчиков на водопроводной магистрали, цифровые системы выключения, цифровые транспортные системы» [Хуатэн и др. 2019: 24].

В последние годы инфраструктура сбора данных стала многоуровневой. На нижнем уровне существуют продукты, способные извлекать данные из повседневной жизни индивидов (смартфоны, «умные часы», фитнес-браслеты). На среднем уровне – так называемый «умный дом» или интегрированная экосистема интернета вещей. Верхний уровень включен в существующие отдельные элементы системы «умных городов» (камеры видеонаблюдения, Wi-Fi, система датчиков).

Цифровая инфраструктура сбора данных является важнейшим маркетинговым инструментом: например, сайты с помощью cookie-файлов отслеживают интернет-серфинг и на основе его анализа предлагают персонализированную рекламу. Одна из проблем сегодня состоит в том, что сложно провести границу корпоративным (коммерческим) и государственным использованием пользовательских данных. На рынке больших данных, помимо платформенных компаний, активно действуют органы государственной власти и близкие к ним дата-корпорации (самый известный пример – Palantir).

Желание собирать данные о поведении и потребительских предпочтениях индивидов само по себе не является отличительной чертой «надзорного капитализма». Журналист и общественный деятель В. Паккард в 1964 г. писал об использовании в рекламных целях различных технологий сбора информации о частной жизни американцев [Packard 2014]. После публикации проблема защиты частной жизни была признана серьезной – был создан специальный подкомитет Конгресса США по проблеме вторжения в частную жизнь (Special Subcommittee on the Invasion of Privacy). Особенность нынешнего

времени заключается в том, что сейчас они располагают для этого наиболее эффективным инструментарием.

### Генеалогия «цифровых автократий»

Формирование моделей цифровых автократий мы проанализируем на двух примерах: Сингапура и Китайской Народной Республики (КНР). Проект Polity IV – комплексный индекс оценки политического режима, оценивает КНР как автократию, а Сингапур как «закрытую анократию» (*closed anocracy*) [Polity IV Project]. Концептуально «закрытая анократия» – более жесткий тип электоральной автократии, политического режима, где проводятся выборы, но к ним допускаются только партии и кандидаты от правящей элиты.

Если обратиться к международным индексам, оценивающим уровень цифровизации экономики и управления, мы увидим, что обе страны занимают достаточно высокие места, особенно когда оцениваются технологические или экономические показатели.

В Мировом рейтинге цифровой конкурентоспособности (The IMD World Digital Competitiveness) Сингапур два года подряд (2019, 2020) занимает 2-е место, а КНР (+Гонконг) в 2019 г. – 13-е, в 2020 г. – 11-е [The IMD World Digital Competitiveness 2020]. В Глобальном индексе сетевого взаимодействия (Global Connectivity Index), разработанном компанией Huawei, Сингапур в 2019 г. занял 4-е место, а КНР – 26-е [Global Connectivity Index 2019]. По Индексу развития электронного правительства (EGDI) Сингапур занимал в 2018 г. 7-е место, в 2020 г. – 11-е, а КНР (+Гонконг) в 2018 г. – 65-е, в 2020 г. – 45-е [E-Government Development Index 2020].

В индексах и рейтингах свободы интернета и свободы прессы картина совсем иная. В докладе Freedom House «Свобода в сети – 2020» КНР занимает 10-е место, Сингапур – 54-е [Freedom on the Net 2020]. По методике расчета рейтинга, чем выше место страны, тем хуже эксперты оценили уровень свободы в интернете. В рейтинге международной организации «Репортеры без границ» КНР занимает одно из последних мест – 177-е, а Сингапур – 158-е. В экспертном комментарии о Сингапуре подчеркивается использование государством элементов и практик, аналогичных китайской модели контроля интернета [Reporters without borders 2020].

В условиях цифровой автократии как специфического ассамбляжа (или исторической констелляции) складывается институциональная комплементарность – интегрированная цифровая инфраструктура, задачей которой является извлечение данных, эффективно функционирует как часть инструментария социального контроля для государства и механизм получения прибыли для компаний. Автократии могут выстраивать различные модели контроля над цифровой инфраструктурой от «суверенного интернета» до более мягких



форм – посредством аффилированных с государством IT-компаний. Автократии Восточной и Юго-Восточной Азии легитимируют проекты «цифровизации сверху» посредством ряда нарративов: технократического (технологические инновации), нарратива «общественной безопасности» и цивилизационного («азиатские ценности» – «социальная гармония», «лояльность и уважение к авторитетам»).

Рассмотрим подробнее формирование китайской и сингапурской моделей «цифровой автократии». Для этого необходимо остановиться на нескольких вопросах: адаптация политико-экономической системы страны к неолиберальному экономическому контексту, стратегия государства и аффилированных с ним IT-компаний по цифровизации экономики и управления и внешнеполитические и торговые конфликты, оказавшие влияние на формирование модели «цифровой автократии».

### Сингапур

После обретения независимости монополюльно управляющая страной партия «Народное действие» и ее генеральный секретарь и одновременно премьер-министр Ли Куан Ю сделали ставку на популярную в ту эпоху среди развивающихся и постколониальных стран модель – «государство развития» (*developmental state*). Это разновидность государственного капитализма, где правительство, используя индикативное планирование, определяет и финансирует развитие стратегически важных отраслей и человеческого капитала [Leftwich 1995: 402–404].

В период холодной войны многие страны использовали ее для ускоренной модернизации, с одной стороны, в качестве альтернативы либеральной рыночной экономике, а с другой – советской модели «государственного социализма». Сингапур, как и большинство «государств развития», имел автократический режим и модель экономического дирижизма, где крупные компании частного сектора сильно аффилированы с политической элитой. В подобных условиях возникает проблема коррупции, и в публичном пространстве широко известны «рецепты» Ли Куан Ю по борьбе с данным явлением [Ли Куан Ю 2010: 147–152].

Преимуществом Сингапура, помимо его геоэкономического положения, была рабочая сила – квалифицированная, дисциплинированная и относительно дешевая. Контроль и политическая интеграция рабочей силы осуществлялся через связанный с правящей партией единый официальный профсоюз. В 1990-е гг. перед Сингапуром и другими странами Юго-Восточной Азии встала необходимость адаптироваться к меняющемуся глобальному экономическому контексту. В этот период происходило перемещение производств из стран ядра капиталистической экономики в регионы с дешевой

рабочей силой, прежде всего в Восточную и Юго-Восточную Азию. У Сингапура, учитывая размер его территории и количество населения, не было возможности конкурировать с соседями по региону (КНР, Вьетнам) в качестве производственной базы корпораций.

Сингапур к этому времени благодаря своему геоэкономическому положению стал важнейшим региональным транспортным хабом. В этой ситуации правительство решило, что рациональнее всего продолжать развивать дальше эту модель. Возникла идея продвигать Сингапур как «ворота на рынок Юго-Восточной Азии» для международных компаний. Правительство страны для адаптации экономики к глобальному неолиберальному контексту начинает дерегулирование отдельных секторов, при этом сохраняя основные институты и практики «государства развития».

Ш. Калатхил и Т. Боас отмечают: «...региональный фактор, повлиявший на распространение интернета в Юго-Восточной Азии, – давление в пользу неолиберальных экономических реформ, которые включали бы в себя дерегулирование ключевых секторов. После Азиатского экономического кризиса в конце 1990-х гг., многие страны в Азии стали воплощать, кто добровольно, кто не совсем, экономические реформы из арсенала международных финансовых институтов, таких как Международный валютный фонд (МВФ). Рекомендации МВФ обычно включали в себя дерегулирование и открытие для инвесторов ряда секторов, в частности телекоммуникаций, одним из эффектов этого в дальнейшем и стало распространение интернета в регионе» [Kalathil, Boas 2003: 72].

Открытие сектора телекоммуникаций для инвесторов сыграло важнейшую роль в дальнейшем развитии цифровой инфраструктуры. Несмотря на частичное дерегулирование, государство продолжало играть основную роль в развитии цифровой инфраструктуры, помимо прочего создавая специальные экономические зоны с рядом налоговых, административных преференций для IT-стартапов.

Исследовав стратегию ряда государств по «цифровизации сверху» (на примерах Сингапура, Турции и Малайзии), Ф. Ховард отметил: «...они (Сингапур, Турция и Малайзия. – А. Б., Л. Т.) активно продвигают использование информационно-коммуникационных технологий (ИКТ) в экономической сфере. Они разрабатывают и реализуют меры по улучшению эффективности ценовых сигналов и прозрачности рынков, в то же время агрессивно препятствуют использованию ИКТ для повышения прозрачности политического процесса или формирования общественного мнения онлайн» [Howard 2011: 80].

Потенциал цифровой инфраструктуры как инструмент контроля актуализируется в социотехническом ассамбляже автократий нового типа. Ф. Ховард отметил, что «калифорнийская Кремниевая долина создала не только

продукты для распространения информации, но и технологии для ограничения информационных потоков. Кувейт, Оман, Саудовская Аравия, Судан, Тунис и ОАЭ используют Secure Computing, Йемен – Websense, а Сингапур – SurfControl. На Западе корпоративные клиенты используют эти программы для борьбы с игрой в интернет-казино и просмотром порнографии на рабочем месте. Клиенты из государственного сектора тоже могут блокировать доступ к сайтам, продвигающим пороки, но, кроме этого, они получают возможность цензурировать политический контент. Например, Websense предлагает опцию по блокировке сайтов групп интересов (*advocacy group*), описываемых как «продвигающие изменения или реформы публичной политики, общественного мнения, социальных практик, экономической активности и отношений» [Howard 2011: 173].

Обобщая список основных инструментов социального и политического контроля, связанных с цифровой инфраструктурой, прежде всего можно выделить:

1. Контроль государства и аффилированных с ним IT-компаний над цифровой инфраструктурой – в частности, интернет-провайдерами и операторами мобильной связи.

2. Использование цифровой инфраструктуры как инструмента контроля над обществом (системы камер с технологией распознавания лиц, сбор и анализ данных интернет-серфинга).

3. Специальное законодательство, работающее в условиях автократии как политический инструмент: акт о телерадиовещании (*broadcasting act*), закон о так называемых «фейковых новостях» (*Protection from Online Falsehoods and Manipulation*).

4. Контроль над цифровой инфраструктурой позволяет создать новую технологически оснащенную модель цензуры (блокировка сайтов средств массовой информации, правозащитных и антикоррупционных НГО, удаление контента со стриминговых сервисов).

Пример Сингапура особенно интересен тем, что он лишает последних аргументов кибероптимистов с их технодетерминистскими теориями демократизации посредством распространения интернета. Сингапур – один из мировых лидеров по индексам сетевого взаимодействия, «цифровой конкурентоспособности» и развития электронного правительства. Кибероптимисты долгое время утверждали, что автократии в цифровую эпоху смогут сохраниться, только став еще одной Северной Кореей, технологически отсталой страной, самоизолировавшейся от экономических и технологических эффектов глобализации.

Для Восточной и Юго-Восточной Азии в последние десятилетия Сингапур является очень важным ориентиром в вопросе экономической и политической

адаптации к неолиберизму. В 1980–1990-е гг. многие государства ориентировались на сингапурский пример при переходе от «государства развития» или «государственного социализма» к политико-экономической системе, которую ряд авторов называют авторитарным капитализмом [Каган 2010].

Политико-экономическая система авторитарного капитализма предполагает контролируемые сверху постепенные рыночные реформы в экономике с сохранением политического и социального контроля. Однопартийная (КНР, Вьетнам) или система с доминирующей партией (Сингапур) приспосабливается к новой среде за счет кооптации организаций, новых возникших в ходе реформ или существовавших ранее, но чья роль изменилась в ином социально-экономическом контексте [Диксон 2005: 85–107].

В процессе адаптации капиталистических автократий Восточной, Юго-Восточной Азии и других регионов к новой информационной среде, возникшей благодаря распространению интернета, Сингапур также играл ключевую роль. Ш. Калатхил и Т. Боас писали в начале 2000-х гг.: «Сингапур заслуживает особого внимания, поскольку правительство страны смогло достичь того, что многие считали невозможным: обширное развитие информационно-коммуникационных технологий с незначительной эрозией политического контроля. Важность этого достижения подчеркивается тем фактом, что другие авторитарные режимы, особенно КНР, проявили активный интерес к опыту Сингапура. <...> Пример Сингапура, возможно, демонстрирует стратегии, которые другие авторитарные и полуавторитарные режимы воплотят в будущем» [Kalathil, Boas 2003: 73].

### **Китайская Народная Республика**

О необходимости регулирования интернета власти КНР говорили с середины 1990-х гг., когда началось его активное распространение в стране. В 1997 г. была подготовлена система правил, регулирующая использование интернета и запрещающая его использование в целях «нанесения ущерба интересам государства или общества», «подрыва национального единства». После конфликта официальных властей страны с рядом американских IT-компаний, произошедшем из-за политики цензурирования сетевого контента, было принято решение о форсированном развитии общенациональной системы кибербезопасности – проекта «Золотой щит», разработка которого началась еще в 1998 г. На начальном этапе развития проект представлял собой интегрированную систему баз данных, аккумулирующую и упорядочивающую информацию о гражданах страны.

Важнейшей частью «Золотого щита» стал так называемый «Великий китайский файрвол» – система фильтрации интернет-контента. Система фильтрации постоянно совершенствуется, изначально она могла в основном

осуществлять блокировку доменных имен и IP-адресов, затем появилась технология фильтрации по ключевым словам, в последнее время основное внимание уделяется борьбе с обходом системы фильтрации с помощью VPN.

Одним из поворотных моментов формирования китайской модели управления интернетом стал запрет и блокировка крупнейших зарубежных социальных сетей и сервисов (Facebook, Instagram, Twitter, Tumblr, Pinterest), поисковиков (Google, Yahoo), видеохостингов (YouTube, Vimeo). Блокировка данных сервисов сопровождалась развитием китайских альтернативных продуктов, технологически и юридически встроенных в национальную систему управления интернетом (Renren, Baidu, Sina Weibo, Youku). Такие условия в интересах не только официальных властей; свою выгоду получают и IT-компании, не имеющие иностранных конкурентов на огромном китайском рынке.

Развитие цифровой инфраструктуры создало условия развития – системы социального кредита, общенационального индикатора оценки поведения граждан, основанного на обработке больших данных. Она собирает и обрабатывает «цифровые следы», оставленные гражданином в различных сферах (счета, налоги, кредиты, штрафы, покупки, интернет-поиск, активность в социальных сетях).

Государственная система социального кредита разработана на основе продукта компании Alibaba (Sesame Credit). Sesame Credit на основе анализа поведения пользователей начисляла им специальные баллы, позволяющие получать кредиты на льготных условиях, скидки на онлайн-покупки и т. д. Контроль государства над цифровой инфраструктурой позволил на основе маркетингового инструмента создать новую социотехническую модель управления.

В системе социального кредита центральным элементом сотрудничества государства и частных IT-компаний (Alibaba, Tencent) является программа развития «умных городов». Данная программа охватит около 500 городов, среди них почти все провинциальные центры и города уровня автономных префектур. Власти интегрировали в систему социального кредита сеть государственных и частных камер наблюдения (около 176 млн), оснащенных технологией распознавания лиц. С 2018 г. к гражданам, обладающим низким социальным рейтингом, стали применяться различные санкции [Томин, Балаян 2019: 79].

Протесты, в Гонконге начавшиеся в 2019 г., продемонстрировали новые модели массового протеста граждан в условиях цифровых автократий [Дудиков 2019]. Протестующие в Гонконге понимали, что цифровая инфраструктура (например, уличные камеры, оснащенные технологией распознавания лиц) – это репрессивный инструмент, используемый полицией.

В этой ситуации рождались новые практики сопротивления от простых (разрушение «умных столбов», оснащенных камерами и датчиками) до более сложных (очки с LED-лампами или арт-метод CV Dazzle).

Модель цифровой автократии, доказав свою эффективность в контроле информационных потоков и повседневной жизни граждан, предоставляет политическим элитам новый инструментарий управления и воспроизводства политического режима. Неудивительно, что данная модель или ее отдельные элементы начали стремительно распространяться по миру. В докладе о свободе интернета за 2018 г. эксперты Freedom House исследовали вопрос экспорта китайскими компаниями, аффилированными с государством, технологий и практик их использования по трем пунктам: цифровая инфраструктура, интегрированные системы камер с технологией распознавания лиц, тренинги для официальных лиц и журналистов. По всем трем пунктам идет сотрудничество с Пакистаном, Шри-Ланкой, Зимбабве, Замбией, Кенией, Венесуэлой. В 38 стран поставляется цифровая инфраструктура, в 18 – интегрированные системы камер с технологией распознавания лиц и в 36 странах проводятся тренинги официальных лиц и журналистов. Интересно, что из 57 исследованных стран, согласно докладу «Свобода в сети – 2018», 11 – свободные, 28 – частично свободные и 18 – несвободные [Freedom on the Net 2018].

Аналогично описывает положение ежегодный доклад «Международный индекс свободы прессы – 2020» организации «Репортеры без границ». В частности, в нем утверждается: «...опираясь на масштабное использование новых технологий, председатель Си Цзиньпин установил в КНР социальную модель, основанную на системе контроля над новостями и информацией и онлайн-слежке (*online surveillance*) за гражданами. Кроме того, он пытается экспортировать эту репрессивную модель, продвигая “новый мировой медиапорядок” основанный на влиянии КНР» [Reporters without borders 2020].

Важную роль в формировании цифровых автократий в последние годы сыграла политизация вопроса о контроле над цифровой инфраструктурой. Речь идет о политике администрации президента США Д. Трампа в отношении китайских IT-компаний (Huawei, TikTok, WeChat) и борьбе вокруг вопроса поставки, установки и налаживания работы сети мобильной связи пятого поколения (5G). У стран Европейского союза по отношению к экспансии китайской цифровой инфраструктуры однозначной политики нет. Из государств постсоветского пространства с КНР активно сотрудничают Российская Федерация, Беларусь, Казахстан и Азербайджан. В контексте пандемии коронавируса и последних политических событий в ряде стран региона можно предположить интенсификацию технологического сотрудничества с КНР и дальнейшую адаптацию сингапурской модели «умного города» для крупных городов.

### Источники

Диксон Б. 2005. *Красные капиталисты в Китае. Партия, частные предприниматели и перспективы политических перемен*. М.: Олимп-Бизнес.

Дудаков М. 2019. «Цифровая» революция в Гонконге. Роль онлайн-инструментов в массовых протестах 2019 г. Аналитический доклад Центра изучения новых коммуникаций. URL: <https://zn.center/upload/img/1452421253.pdf> (дата обращения: 10.08.2020).

Каган Р. 2010. *Возвращение истории и конец мечтаний*. М.: Прогресс-Традиция.

Ли Куан Ю. 2010. *Сингапурская история. 1965–2000 гг. Из третьего мира в первый*. М.: МГИМО-Университет.

Майр П. 2019. *Управляя пустотой. Размывание западной демократии*. М.: Изд-во Института Гайдара.

Морозов Е. 2014. *Интернет как иллюзия. Обратная сторона сети*. М.: АСТ; CORPUS.

Срничек Н. 2019. *Капитализм платформ*. М.: Издательский дом Высшей школы экономики.

Томин Л.В., Балаян А.А. 2016. Интернет и социальные медиа в современном политическом процессе: по ту сторону киберутопизма. – *Публичная политика – 2015*. С. 60–68.

Томин Л.В., Балаян А.А. 2019. Цифровой паноптикум. Как автократии используют технологическую инфраструктуру? – *Евразийская интеграция: экономика, право, политика*. № 3 (29). С. 77–83.

Хуатэн М., Чжаоли М., Дели Я., Хуалей В. 2019. *Цифровая трансформация Китая. Опыт преобразования инфраструктуры национальной экономики*. М.: Интеллектуальная литература.

Agamben G. 2005. *State of Exception*. Chicago: Chicago University Press.

Bloom P. 2019. *Monitored: Business and Surveillance in a Time of Big Data*. Polity.

Bridle J. 2019. *New Dark Age. Technology and the End of the Future*. Verso.

Burgers T., Robinson D. 2016. Networked Authoritarianism Is on the Rise. Sicherheit und Frieden (SF). – *Security and Peace*. Vol. 34. N 4. P. 248–252.

*E-Government Development Index*. 2020. URL: <https://publicadministration.un.org/egovkb/Data-Center> (дата обращения: 10.06.2020).

Eubanks V. 2018. *Automating Inequality. How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.

Foster J.B., McChesney R. 2014. *Surveillance capitalism. Monthly Review*. URL: <https://monthlyreview.org/2014/07/01/surveillance-capitalism/> (дата обращения: 10.06.2020).

*Freedom on the Net 2018. The Rise of Digital Authoritarianism.* Freedom House. URL: [https://freedomhouse.org/sites/default/files/2020-02/10192018\\_FOTN\\_2018\\_Final\\_Booklet.pdf](https://freedomhouse.org/sites/default/files/2020-02/10192018_FOTN_2018_Final_Booklet.pdf) (дата обращения: 10.06.2020).

*Freedom on the Net 2020. The Pandemic's Digital Shadow.* Freedom House. URL: [https://freedomhouse.org/sites/default/files/2020-10/10122020\\_FOTN2020\\_Complete\\_Report\\_FINAL.pdf](https://freedomhouse.org/sites/default/files/2020-10/10122020_FOTN2020_Complete_Report_FINAL.pdf) (дата обращения: 11.10.2020).

*Global Connectivity Index.* 2019. URL <https://www.huawei.com/minisite/gci/en/> (дата обращения: 10.06.2020).

Howard P. 2011. *The Digital Origins of Dictatorship and Democracy. Information Technology and Political Islam.* Oxford: Oxford University Press.

Kalathil S., Boas T. 2003. *Open Networks, Closed Regimes. The Impact of the Internet on Authoritarian Rule.* Carnegie Endowment for International Peace.

Leftwich A. 1995. Bringing politics back in: Towards a model of the developmental state. – *Journal of Development Studies.* Vol. 31. Issue 3. February. P. 400–427.

Levine Y. 2019. *Surveillance valley: the secret military history of the internet.* Icon Books Ltd.

Meissner M., Wübbecke J. 2016. IT-backed authoritarianism: Information technology enhances central authority and control capacity under Xi Jinping. MERICS Papers on China. URL: [http://www.merics.org/fileadmin/user\\_upload/downloads/MPOC/MPOC\\_ChinasCoreExecutive.pdf](http://www.merics.org/fileadmin/user_upload/downloads/MPOC/MPOC_ChinasCoreExecutive.pdf) (дата обращения: 10.08.2020).

Packard V. 2014. *The Naked Society.* Ig Publishing; Revised ed. edition.

Pasquale F. 2015. *The Black Box Society. The Secret Algorithms That Control Money and Information.* Harvard: Harvard University Press.

Pearce K., Kendzior S. 2012. Networked Authoritarianism and Social Media in Azerbaijan. – *Journal of Communications.* Vol. 62. Issue 2.

*Polity IV Project.* URL: <https://www.systemicpeace.org/polity/polity4.htm> (дата обращения: 10.08.2020).

*Reporters without borders.* 2020. World Press Freedom Index. URL: <https://rsf.org/en/china>, <https://rsf.org/en/singapore> (дата обращения: 10.08.2020).

Rule J. B., Cheng H. 2020. *Coronavirus and the Surveillance State.* Dissent Magazine. Summer.

*The IMD World Digital Competitiveness Ranking.* 2020. URL: [https://www.imd.org/globalassets/wcc/docs/release-2020/digital/digital\\_2020.pdf](https://www.imd.org/globalassets/wcc/docs/release-2020/digital/digital_2020.pdf) (дата обращения: 10.08.2020).

Zuboff S. 2019. *The age of surveillance capitalism: the fight for a human future at the new frontier of power.* PublicAffairs.