DOI 10.22394/1726-1139-2021-11-21-33

Политические эффекты цифровой трансформации городского управления (на примере г. Москвы)*

Балаян А. А.[1, *], *Томин Л. В.*[2]

[1]Национальный исследовательский университет «Высшая школа экономики» Санкт-Петербург, Российская Федерация; *alexandr1138@mail.ru
[2]Санкт-Петербургский государственный университет, Санкт-Петербург, Российская Федерация

РЕФЕРАТ

Статья посвящена исследованию отдельных политических эффектов цифровизации городского управления в Российской Федерации. На основе концепции «надзорного капитализма» и исследований цифровой трансформации государственного управления анализируются структура и логика функционирования модели «умного города» на примере г. Москвы. На материале уличных акций протеста рассматриваются политические эффекты использования властями города цифровой инфраструктуры, в частности, системы камер с технологией распознавания лиц. Изучение российской ситуации соотносится с последними решениями совета по правам человека Организации Объединенных Наций (ООН) и инициативами Европейского Союза по контролю над технологиями удаленного биометрического распознавания.

Ключевые слова: цифровизация, городское управление, большие данные, политический режим, демократия, права человека

Для цитирования: *Балаян А. А., Томин Л. В.* Политические эффекты цифровой трансформации городского управления (на примере г. Москвы) // Управленческое консультирование. 2021. № 11. С. 21–33.

Political Effects of Digital Transformation of Urban Governance (On the Example of Moscow)

Alexandr A. Balayan[1, *], *Leonid V. Tomin*[2]

[1]HSE Campus in St. Petersburg, Saint Petersburg, Russian Federation; *alexandr1138@mail.ru
[2]Saint-Petersburg State University, Saint-Petersburg, Russian Federation

ABSTRACT

The paper is devoted to the study of particular political effects of digitalization of urban governance in the Russian Federation. Based on the concept of «surveillance capitalism» and research on the digital transformation of public administration, the authors analyzes the structure and logic of functioning of the «smart city» model using the example of Moscow. Based on the material of street protests, the political effects of the use of digital infrastructure by the city authorities, in particular, camera systems with face recognition technologies, are examined. The study of the Russian situation correlates with the latest decisions of the United Nations (UN) Human Rights Council and the European Union's initiatives to control remote biometric recognition technologies.

Keywords: digitalization, urban governance, big data, political regime, democracy, human rights

For citing: Balayan A. A., Tomin L. V. Political Effects of Digital Transformation of Urban Governance (On the Example of Moscow) // Administrative consulting. 2021. N 11. P. 21–33.

* Работа выполнена при поддержке гранта РНФ «Политическая онтология цифровизации: исследование институциональных оснований цифровых форматов государственной управляемости» № 19-18-00210.

Введение

В последние годы изучение политических эффектов цифровизации государственного управления и публичной политики становится все более актуальным. Меры цифрового контроля за перемещением людей, предпринятые правительствами в условиях пандемии коронавируса, казалось, воплотили в реальность концепции Ж. Делеза о новой кибернетической модели власти в «обществе контроля» [7, с. 227–232] или Дж. Агамбена о «биополитике» как новой модели управления и «перманентном чрезвычайном положении» [1, с. 7–8]. «Умные города» и экономика больших данных в новых условиях возрождают управленческую ментальность «высокого модернизма» (термин Дж. Скотта) с присущей ему верой в технологии, проектирование и моделью управления, близкой к социальной инженерии [10, с. 21–22]. Формирование интегрированной цифровой инфраструктуры, систем «умного города» паноптизируют городское пространство, создавая потенциал для авторитарных управленческих практик [24, p. 14–16]. Особая опасность политического использования новых технологий существует в автократиях и гибридных режимах, элиты которых используют «цифровизацию сверху» как основу формирования социотехнической модели управления, для описания которой исследователи используют различные термины: цифровая автократия [2], сетевой авторитаризм [16].

По-нашему мнению, в российских научных и экспертных дискуссиях по данной проблематике существуют определенные лакуны. Специалисты по политическим режимам не уделяют должного внимания *диффузии централизованных моделей государственного контроля над интернетом, прежде всего китайской и сингапурской* [27, p. 5–6]*. И главное — основополагающей роли данных моделей в трансформации* управленческих практик и механизмов стабилизации автократий и гибридных режимов. Эмпирически ориентированные исследователи «умных городов», в свою очередь, рассматривают их чисто технологически, вне контекста борьбы государств и корпораций или существующего в конкретной стране политического режима. Кроме того, существует категория — кибероптимистов, продолжающих описывать интернет языком середины 1990-х — начала 2000-х годов как децентрализованную (анархическую) систему, формирующую новую модель экономики (открытую, коллаборативную) и политики (прямая демократия). Этот оптимистический (иногда утопический) нарратив не способен описать и проанализировать современные тенденции к концентрации и монополизации контроля над цифровой инфраструктурой и пользовательскими данными [15, p. 25–28].

В данной статье мы сделаем попытку объединить материал наших предыдущих публикаций [2] с имеющимися работами политологов [11], социологов [26] и IT-специалистов, анализирующих политические эффектов цифровизации городского управления и совместить это с концептуальной рамкой исследований легитимации и воспроизводства политических режимов. Мы сосредоточим свое внимание на анализе отдельных негативных политических эффектов цифровизации городского управления, это не означает, что мы отрицаем существующие и будущие положительные эффекты процесса цифровизации различных сфер. Нам лишь хотелось бы отметить, что исследование данных процессов должно носить контекстуальный характер и учитывать борьбу различных акторов. В связи с этим необходимо вспомнить слова одного из первых теоретиков интернета, писателя Брюса Стерлинга. Комментируя дискуссии об интернете вещей, он отметил: «Первое, что нужно знать в истории об «интернете вещей», это то, что она не о вещах, подключенных к интернету. Это кодовое слово, используемое могущественными стейкхолдерами для собственных целей. Им нравится словосочетание «интернет вещей», поскольку оно звучит миролюбиво и прогрессивно. Оно скрывает борьбу за власть, деньги и влияние» [28, p. 8].

Борьба за цифровую инфраструктуру

Сегодня борьба за контроль над инфраструктурой интернета стала очевидной. Она имеет межстрановое измерение, в виде глобального конфликта США и КНР вокруг распространения сетей 5G и обвинений в кибератаках и кибершпионаже. Кроме того, существует противостояние отдельных государств с IT-корпорациями в связи с антимонопольным регулированием, уплатой налогов и установлением новых правил хранения пользовательских данных. И есть третье поле борьбы — за общественный контроль над технологиями, создающими потенциальную угрозу правам и свободам граждан. В этом году совет по правам человека Организации Объединенных Наций (ООН) принял резолюцию о правах в интернете[1]. Власти ряда стран в периоды политических акций оппозиции или локальных конфликтов прибегают к политически мотивированному отключению интернета (politically motivated internet shutdown). Например, в августе 2020 г., в период поствыборного политического кризиса, власти Республики Беларусь в дни уличных акций оппозиции неоднократно прибегали к подобным мерам.

Совместный доклад международной правозащитной группы «Агора» и общественной организации «Роскомсвобода» гласит, что в Российской Федерации за последние два года зафиксировано восемь случаев политически мотивированного отключения интернета[2]. Среди них наиболее значимые примеры:

1) отключение мобильного интернета во время протестов в Ингушетии (осень 2018 г.));
2) отключение мобильного интернета и Wi-Fi сетей на месте проведения митингов в Москве (3 августа 2019 г.);
3) отключение мобильного интернета во время протестов с требованием отмены результатов выборов в Улан-Удэ (сентябрь 2019 г.);
4) отключение мобильного интернета во время протестов против строительства мусорного полигона в Шиесе (23 октября 2019 г.).

Резолюция совета по правам человека ООН осуждает подобные действия властей, кроме того, она поручила управлению Верховного комиссара ООН по правам человека работу над специальным докладом об имевших место случаях политически мотивированного отключения интернета[3].

Среди элементов «умного города» у общественных и правозащитных организаций наибольшую озабоченность вызывают интегрированные системы камер с технологией распознавания лиц. Международная некоммерческая организация Access Now инициировала кампанию, конечная цель которой — запрет «биометрической слежки», прежде всего использования правительствами, правоохранительными органами и частными компаниями — технологии распознавания лиц и других механизмов удаленного биометрического распознавания. По мнению инициаторов кампании, данные технологии подрывают фундаментальные гражданские права и свободы[4].

Особо отмечено, что использование властями данных технологий подвергает эрозии права граждан на свободу собраний и ведет к криминализации протеста[5].

---

[1] United Nations adopts resolution on human rights on the internet // CIVCUS [Электронный ресурс]. URL: https://civicus.org/index.php/media-resources/news/united-nations/geneva/5170-human-rights-council-adopts-new-resolution-on-human-rights-on-the-internet (дата обращения: 20.07.2021).

[2] Доклад о свободе интернете — 2019 // Агора [Электронный ресурс]. URL: https://2019.runet.report (дата обращения: 20.06.2021).

[3] United Nations adopts resolution on human rights on the internet.

[4] Ban biometric surveillance // Access Now [Электронный ресурс]. URL: https://www.accessnow.org/ban-biometric-surveillance/ (дата обращения: 21.07.2021).

[5] Там же.

Инициаторы общественной кампании требуют:

1) прекратить государственные инвестиции в использование распознавания лиц и удаленных биометрических технологий, которые делают возможным массовое наблюдение и дискриминационное целевое наблюдение;
2) запретить использование этих технологий в общедоступных местах как государственными, так и частными компаниями, где такое использование может сделать возможным массовое наблюдение или дискриминационное целевое наблюдение.

По данным на июль 2021 г., к кампании, инициированной Access Now, присоединилось уже более 170 общественных организаций со всего мира, из российских: «Общество защиты интернета», «Сетевые свободы», «РосКомСвобода», «Теплица социальных технологий»[1].

В апреле 2021 г. обнародован проект регламента Европейского Союза по искусственному интеллекту[2]. Помимо искусственного интеллекта (ИИ), он затрагивает и использование технологии распознавания лиц. Проект регламента предлагает запретить или строго регламентировать применения ИИ в системах камер с технологией распознавания лиц в общественных местах. Исключение делается только для установленных судом кейсов, связанных с предотвращением террористических актов[3]. В Соединенных Штатах Америки в 2020 г. Конгресс рассматривал, но пока не принял два законопроекта, посвященных регулированию использования технологии распознавания лиц: закон об этическом использовании распознавания лиц (The Ethical Use of Facial Recognition Act) и закон о распознавании лиц и биометрических технологиях (Facial Recognition and Biometric Technology Moratorium Act). В Российской Федерации отсутствует специальный закон, запрещающий или регулирующий использование данной технологии.

От «демократии с прилагательными» к «информационной автократии»

Переходя к вопросу о политическом контексте функционирования цифровой инфраструктуры и умных городов в РФ, необходимо сначала рассмотреть дискуссии о характере политического режима. Когда стало очевидно, что «третья волна» демократизации завершилась и начался откат, первым концептуальным нововведением, предложенным для осмысления реальности политических режимов, не укладывающихся в дихотомию демократия/авторитаризм, стало определение — «демократия с прилагательными» («democracy with adjectives») [17]. Этот зонтичный термин должен обозначить государства, где процесс формирования демократических институтов, начавшись, столкнулся с различными препятствиями. Но в целом взгляд исследователей был достаточно оптимистичным, эти препятствия со временем будут преодолены, они не ставили под сомнение общее направление движения стран к демократии. Концепция «демократии с прилагательными» стала популярной среди специалистов по Латинской Америке и постсоветскому пространству.

В начале 2000-х на постсоветском пространстве в ряде стран, в том числе Российской Федерации, исследователи стали фиксировать нарастающее усиление авторитарных тенденций [25, p. 186–209]. Для концептуализации новой политической ситуации были предложены термины: соревновательный авторитаризм (С. Левицкий, Л. Вэй) [8] и электоральный авторитаризм (А. Шэдлер, Г. Голосов) [18].

---

[1] Там же.

[2] Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts // EUR-Lex [Электронный ресурс]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206 (дата обращения: 20.07.2021).

[3] Там же.

Нам представляется, что второй термин более точно отражает логику функционирования и воспроизводства политического режима в РФ. В рамках электорального авторитаризма выборы сохранили свое значение, но «формальные и неформальные правила таких выборов предполагают высокие входные барьеры для участия в них, заведомо неравный доступ участников кампаний к ресурсам (от финансовых до медийных), систематическое использование государственного аппарата в целях максимизации голосов за правящие партии и кандидатов, и злоупотребления в пользу последних на всех стадиях выборов, в том числе при подсчете голосов», — отмечает В. Гельман [4, с. 2].

Электоральный авторитаризм с точки зрения механизма кооптации федеральным центром региональных элит может быть описан как «компромисс между местными элитами: правящая группа требует от них политической поддержки в вопросах общегосударственной важности, а также обеспечения «правильного» голосования на федеральных выборах, а взамен дарует им монопольный контроль над «своими» регионами» [6, с. 33]. Контролируемые выборы являются важным элементом в системе электорального авторитаризма, позволяющим правящей элите получить внутреннюю и внешнюю легитимацию.

В период с 2011 по 2014 г., начавшийся с массовых митингов после выборов в Государственную Думу и завершившийся присоединением к Российской Федерации Крыма, в механизме воспроизводства легитимности власти произошло важное структурное изменение. Резко возросла роль прямого политического использования властью информационного ресурса, особенно после санкций, связанных с ситуацией вокруг Украины [20, p. 2–3]. Для анализа ситуации в РФ и сходных тенденций в других государствах Д. Трейсман и С. Гуриев предложили термин «информационная автократия». По их мнению, воспроизводство легитимности в информационных автократиях происходит не за счет идеологии или репрессий, которые осуществляются, но носят ограниченный характер. Главный инструмент подобных режимов — использование новых информационных технологий для формирования общественного мнения, маргинализации независимых средств массовой информации и политиков [21].

По нашему мнению, Д. Трейсман и С. Гуриев правы в интенции исследования новых механизмов функционирования и воспроизводства автократий в новом технологическом контексте. В предыдущих публикациях, посвященных КНР и Сингапуру [2, с. 107–113], мы, соглашаясь с рядом зарубежных авторов [23], писали о формировании нового типа режима — цифровой автократии. Данная социотехническая модель управления основана на контроле государства над цифровой инфраструктурой. Автократии могут выстраивать различные модели контроля над цифровой инфраструктурой от «суверенного интернета» до более мягких форм — посредством аффилированных с государством IT-компаний. Автократии легитимируют проекты «цифровизации сверху» посредством ряда нарративов: технократического (технологические инновации), «общественной безопасности», иногда, как в Восточной и Юго-Восточной Азии, цивилизационного («азиатские ценности», «социальная гармония») или, наконец, геополитического («цифровой суверенитет» как инструмент защиты от внешних врагов).

Анатомия цифровой автократии

В качестве теоретической основы для исследования процесса формирования цифровых автократий мы используем концепцию «надзорного капитализма» («surveillance capitalism») Ш. Зубофф [29] и Дж. Б. Фостера, Р. МакЧесни [19]. Основа бизнес-модели «надзорного капитализма» — монетизация пользовательских данных. Их сбор осуществляется посредством продуктов и сервисов, предоставляемых бесплатно.

За последние годы 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 информационная инфраструктура: 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» [12, с. 24].

В последние годы инфраструктура сбора данных стала многоуровневой. На нижнем уровне существуют устройства, способные извлекать данные из повседневной жизни индивидов (смартфоны, «умные часы», фитнес-браслеты). На среднем уровне — «умный дом» или интегрированной экосистемы интернета вещей. Верхний уровень включен в существующие отдельные элементы системы «умных городов» (камеры видеонаблюдения с технологией распознавания лиц, сети Wi-Fi, система датчиков).

В условиях цифровой автократии как специфического ассамбляжа складывается институциональная комплементарность — цифровая инфраструктура, задачей которой является извлечение данных, эффективно функционирует как часть инструментария социального контроля для государства и механизм получения прибыли для компаний. Исследовав стратегию ряда государств по «цифровизации сверху», Ф. Ховард отметил, «они активно продвигают использование информационно-коммуникационных технологий 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» [22, p. 80].

Многие эксперты справедливо говорили, что московская система «умного города» во многом повторяет пример Сингапура. В процессе адаптации капиталистических автократий Восточной, Юго-Восточной Азии и других регионов к новой информационной среде, возникшей благодаря распространению интернета, Сингапур сыграл ключевую роль. Сингапурская модель для политологов интересна тем, что она лишает сторонников технодетерминистских теорий «демократизации посредством распространения интернета» последних аргументов. Сингапур один из мировых лидеров по индексам: сетевого взаимодействия, «цифровой конкурентоспособности» и развития электронного правительства. Если попытаться обобщить основные черты сингапурской модели, можно выделить следующие:

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 независимых средств массовой информации, правозащитных и антикоррупционных организаций) [2, с. 110].

Информационные системы автократий собирают и анализируют данные граждан, и на этой основе формируется система «перевернутой подотчетности» [5]. Это

означает, что не государство становится более прозрачным и контролируемым, а наоборот — общество. Городское управление, основанное на больших данных, в условиях не ограничено в использовании собранной информации. Информационные системы собирают избыточное, с точки зрения нужд управления, количество данных. Информационные системы — непрозрачны, граждане не знают, кем и как используются их данные.

Цифровые автократии активно внедряют и используют специальные цифровые сервисы (городские платформы, приложения), направленные на вовлечение активных граждан в обсуждение низовых малозначимых с точки зрения «большой политики» вопросов, например благоустройства территорий. Формируется специфическая деполитизированная система обратной связи с гражданами. Причем эта система создает «эффект индивидуализации», воспроизводя модель субъективности изолированного частного субъекта. Один из авторов исследования российских городских цифровых платформ И. Быков справедливо отметил, что «по сути дела, граждане специально держатся в атомизированном состоянии, что позволяет администрации управлять текущими хозяйственными вопросами, выступая в качестве единственного дееспособного института в стране» [3, с. 192].

Согласно исследованию компании Comparitech, Российская Федерация занимает второе место из 47 стран в рейтинге «надзорных государств» (surveillance states). На первом — КНР, после РФ идут Индия, Малайзия, Тайланд. Комплексный рейтинг составляется на основе оценки стран по ряду показателей, среди которых: обеспечение неприкосновенности частной жизни (privacy enforcement), функционирование систем видеонаблюдения (visual surveillance), использование и обмен пользовательских данных (data-sharing), мониторинг и перехват информации в каналах связи (communication interception) [13].

Централизованный контроль государства над цифровой инфраструктурой вместе со специальным законодательством создает угрозу нарушения прав и свобод граждан. Организация Human Rights Watch подчеркнула, что «последние события в области регулирования интернета в России, связанные с ужесточением государственного контроля над сетевой инфраструктурой, внедрением новых технических средств отслеживания пользовательской активности и фильтрации и перенаправления трафика, а также с наращиванием возможностей правительства по блокированию контента, противоречат стандартам свободы выражения мнений и неприкосновенности частной жизни, охраняемым Международным пактом о гражданских и политических правах и Европейской конвенцией о правах человека»[1].

Москва как лаборатория

Москва как столица стала первым из российских мегаполисов, где тестировалась новая социотехническая модель управления, основанная на извлечении и анализе пулов больших данных. С. Собянин с 2008 г. занимал должность главы аппарата правительства РФ и курировал программу по цифровизации государственных услуг («Информационное общество»). Став мэром Москвы, он с 2012 г. инициировал программу формирования модели «умного города», основанного на интегрированной цифровой инфраструктуре и системы сбора и анализа данных («Информационный город»). Процесс формирования цифровой инфраструктуры и пулов данных начался с государственных услуг и сервисов и создания интеллектуальной транспортной системы управления трафиком. Цифровая инфраструктура позволила из-

[1] Россия: Нарастающая изоляция, контроль и цензура в интернете // Human Rights Watch [Электронный ресурс]. URL: https://www.hrw.org/ru/news/2020/06/18/375397 (дата обращения: 20.07.2021).

влекать данные постоянно и почти из всех действий горожан. Пулы данных, собираемые мэрией о горожанах, можно разделить на несколько потоков:

1. Геоаналитические данные операторов сотовой связи. Начиная с 2015 г., мэрия закупает их у всех основных операторов (Tele2, МТС, Билайн, Мегафон).
2. Данные о передвижении по городу: общественный и личный транспорт, службы такси, каршеринг, прокат велосипедов, парковки (система «Безопасный транспорт»). Интеллектуальная транспортная система оснащена оборудованием видео- и фотосъемки, позволяющим в режиме онлайн определить местоположение любого транспортного средства и данные о его владельце.
3. Данные, поступающие от сети публичного Wi-Fi. По соглашению с пользователем при входе в сеть Wi-Fi, оператор использует технологию Deep Packet Inspection (DPI) для анализа трафика, данные о действиях пользователя записываются в cookie-файл. В дальнейшем эти файлы сопоставляются друг с другом, если система полагает, что это один и тот же человек. Формируются профили пользователей, объединенные по различным параметрам. Единый оператор публичной сети Wi-Fi имеет доступ к базам телефонных номеров и способен с помощью алгоритма (связь проездного билета метро и подключение через номер телефона в Wi-Fi сеть) определять личность гражданина.
4. Данные порталов и их мобильных версий mos.ru (Московские госуслуги), ag.mos.ru («Активный гражданин») и gorod.mos.ru («Наш город»). С помощью системы СТАТС собираются данные (IP-адреса, тип устройства и браузер), причем она специально приспособлена для деанонимизации пользователей (технология fingerprint)[1].

Кроме того, мэрия обладает базами данных и системами мониторинга, например, Система поддержки принятия решений и управления информационными рисками Аппарата Мэра и Правительства Москвы, осуществляет мониторинг средств массовой информации и социальных сетей с целью поиска упоминаний правительства Москвы и мэра[2]. Официальные лица мэрии утверждают — пул данных обезличен, но многие технические специалисты полагают, что это не соответствует действительности. На примере анализа созданной в метро «Системы персональных коммуникаций», они продемонстрировали, что, согласно государственному контракту с поставщиком данных «МаксимаТелеком», телефонные номера передаются не в привычном для коммерческого рынка зашифрованном формате (hash). По контракту они могут быть расшифрованы и переданы в виде обычного номера телефона[3].

Одним из наиболее важных элементов цифровой инфраструктуры Москвы как «умного города» является система камер видеонаблюдения, оснащенных функцией распознавания лиц. Все они интегрированы в Единую систему хранения и обработки данных. Камеры расположены: на улицах, в метро, в государственных учреждениях, во дворах и подъездах домов, больницах, школах. Важно отметить, что в период пандемии коронавируса контроль над перемещением граждан получил новый импульс. Например, данные геолокации телефона и система камер наблюдения использовались для наказания нарушителей режима карантина. Согласно исследованию Comparitech, по количеству камер на 1000 человек Москва входит в первую двадцатку городов мира. Все остальные города, кроме одного (Лондон), расположившиеся в списке выше Москвы — китайские мегаполисы: Тайюань, Уси, Чанша, Пекин и др. [14].

В последние несколько лет эксперты зафиксировали ряд примеров политического использования цифровой инфраструктуры в столице. 3 августа 2019 г. перед

---

[1] *Захаров А.* «Умный город» или «Старший брат»? // BBC [Электронный ресурс]. URL: https://www.bbc.com/russian/features-52219260 (дата обращения: 20.07.2021).

[2] Там же.

[3] Там же.

выборами в Московскую городскую Думу проходила акция протеста, связанная с отказом в регистрации оппозиционным кандидатам. В этот день в местах проведения митингов зафиксировано отключение мобильного интернета и Wi-Fi сетей кафе и других заведений, находящихся поблизости от мест проведения уличных акций оппозиции. Лаборатория NetBlocks зафиксировала, что «период отключения сервиса, по поступившим документам, должен был продолжаться с 13:00 по 23:00 3 августа. Фактический перерыв в оказании услуг у одного из операторов был с 13:15 по 19:33». В их докладе отмечается, что измерения с приложения Android Network Cell Info Lite показали — часть станций операторов мобильной связи работали в режиме GSM-only[1].

23 января 2021 г. в тех частях Москвы, где проходили акции в поддержку А. Навального, NetBlocks зафиксировала аналогичное отключение интернета[2]. Кроме политически мотивированного отключения интернета для задержания участников митинга полиция использовала систему камер с технологией распознавания лиц[3]. Аналогичная ситуация сложилась после акции 21 апреля, по данным средств массовой информации сотрудники правоохранительных органов составили протоколы как минимум на 289 человек. Из этого числа — 69 человек были вычислены по камерам видеонаблюдения, 64 из них — в Москве [9].

В мае по подозрению в участии в митинге (21 апреля) была задержана Юлия Щербакова, муниципальный депутат района Черемушки. В качестве доказательства ее присутствия на уличной акции в поддержку А. Навального, следователи предъявили распечатки изображений с системы камер. У Ю. Щербаковой были доказательства того, что во время митинга она находилась в другом месте, несмотря на это ее отвезли в суд. Суд в итоге вернул дело обратно в органы внутренних дел на доработку[4]. Так же, на основе данных систем камер, были осуждены два депутата: Е. Шувалова (Мосгордума) и В. Залищак (муниципальный депутат Донского района)[5]. Они присутствовали на митинге 21 апреля не в качестве участников акции, а как представители власти, чтобы при необходимости принять предусмотренные законодательством меры по обеспечению прав, свобод и интересов своих избирателей. Во время проведения митинга полиция не имела к депутатам каких-либо претензий или замечаний. В итоге В. Залищак был осужден на 15 суток ареста без возможности получить юридическую помощь, Е. Шувалова была осуждена заочно, на нее был наложен штраф.

Элементы московской модели «умного города» постепенно будут воспроизводиться в других российских мегаполисах (Санкт-Петербург, Казань). Прежде всего, си-

---

[1] Evidence of internet disruptions in Russia during Moscow opposition protests // NetBlocks [Электронный ресурс]. URL: https://netblocks.org/reports/evidence- of-internet-disruptions-in-russia-during-moscow-opposition-protests-XADErzBg (дата обращения: 22.07.2021).

[2] Internet disrupted in Russia amid opposition protests // NetBlocks [Электронный ресурс]. URL: https://netblocks.org/reports/internet-disrupted-in-russia-amid-opposition-protests-98aRXQAo (дата обращения: 22.07.2021).

[3] Камалетдинов Д. Система распознавания лиц в Москве теперь ищет протестующих // TJournal [Электронный ресурс]. URL: https://tjournal.ru/tech/333457-sistema-raspoznavaniya-lic-v-moskve-teper-ishchet-protestuyushchih-kak-ona-ustroena-i-chto-sdelat-dlya-zashchity (дата обращения: 20.07.2021).

[4] Депутат Юлия Щербакова: «Распознавание надо использовать во благо, а не выворачивать всё наизнанку» // Роскомсвобода [Электронный ресурс]. URL: https://roskomsvoboda.org/post/deputat-julia-scherbakova-raspoznavanie/ (дата обращения: 20.07.2021).

[5] Депутат Мосгордумы: «о суде по результатам видеонаблюдения за мной я узнала после того, как он уже прошел» // Роскомсвобода [Электронный ресурс]. URL: https://roskomsvoboda.org/post/elena-schuvalova-deputat-raspoznavanie/; Распознавание лиц применяют для необоснованных обвинений видна политическая ангажированность // Роскомсвобода [Электронный ресурс]. URL: https://roskomsvoboda.org/post/vladimir-zalischak-raspoznavanie/ (дата обращения: 20.07.2021).

стема «Безопасный город», через пять лет правительство планирует создать единую платформу видеонаблюдения (ГИС «Национальная платформа видеонаблюдения»), которая объединит и подключит все городские системы камер к единому контуру.

Рассмотрение примеров политического использования цифровой инфраструктуры на примере митингов в Москве подтверждает основные положения резолюции о правах в интернете совета по правам человека ООН. «Умный город» в условиях автократии функционирует как паноптический «надзорный город» (surveillance city). Происходит дальнейшая эрозия права граждан на свободу собраний и криминализация уличного протеста. Различные модели цифровизации в одних странах усилили роль IT-корпораций, в других — государства. Цифровая инфраструктура, которой пронизан город, делает его единым пространством функционирования новых социотехнических практик управления и извлечений прибыли в логике экономии больших данных. Эмансипаторные движения неизбежно столкнутся с практиками политического использования инфраструктурой власти «умного города», что доказывают примеры Юго-Восточной Азии и постсоветского пространства.

Литература

1. *Агамбен Дж.* Homo sacer. Чрезвычайное положение. М. : Европа, 2011.
2. *Балаян А. А., Томин Л. В.* Цифровая автократия. Институциональная специфика отношений государства и IT-компаний // Публичная политика. 2020. Т. 4. № 2. С. 101–115.
3. *Быков И. А.* Деполитизация социально значимых проблем в цифровых платформах государственного управления // Медиа в современном мире. 60-е Петербургские чтения: сборник материалов Международного научного форума. В 2 т. СПб. : Медиапапир, 2021. С. 192–193.
4. *Гельман В. Я.* Расцвет и упадок электорального авторитаризма в России // Центр исследований модернизации [Электронный ресурс]. URL: https://eusp.org/sites/default/files/archive/M_center/Electoral_Authoritarianism_in_Russia.pdf (дата обращения: 20.07.2021).
5. *Гельман В. Я.* Цифровизация в России: (полу)прозрачность без подотчетности // Riddle [Электронный ресурс]. URL: https://www.ridl.io/ru/cifrovizacija-v-rossii-polu-prozrachnost-bez-podotchetnosti/ (дата обращения: 20.07.2021).
6. *Голосов Г. В.* Электоральный авторитаризм в России // Pro et Contra. 2008. № 1. С. 22–35.
7. *Делез Ж.* Переговоры. СПб. : Наука, 2004.
8. *Левицкий С., Вэй Л.* Подъем конкурентного авторитаризма // Неприкосновенный запас. Дебаты о политике и культуре. 2018. № 5. С. 29–47.
9. *Полоротов А.* За месяц после акции в поддержку Навального правоохранительные органы составили протоколы на 289 человек // Seldon News [Электронный ресурс]. URL: https://news.myseldon.com/ru/news/index/251176822 (дата обращения: 20.07.2021).
10. *Скотт Дж.* Благими намерениями государства. М. : Университетская книга, 2005.
11. *Сморгунов Л. В.* Институты публичного управления интернетом: сравнительный анализ России, Беларуси и Казахстана // Управленческое консультирование. 2020. № 12. С. 24–39.
12. *Цифровая* трансформация Китая. Опыт преобразования инфраструктуры национальной экономики. М. : Альпина Паблишер. 2019.
13. *Bischoff P.* Data privacy laws and government surveillance by country: Which countries best protect their citizens? // Comparitech [Электронный ресурс]. URL: https://www.comparitech.com/blog/vpn-privacy/surveillance-states/ (дата обращения: 21.07.2021).
14. *Bischoff P.* Surveillance camera statistics: which cities have the most CCTV cameras? // Comparitech [Электронный ресурс]. URL: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/ (дата обращения: 22.07.2021).
15. *Bory P.* The Internet Myth: From the Internet Imaginary to Network Ideologies. University of Westminster Press. 2020.
16. *Burgers T., Robinson D.* Networked authoritarianism is on the rise // Security and Peace. 2016. Vol. 34. N 4. P. 248–252.
17. *Collier D., Levitsky S.* Democracy with Adjectives: Conceptual Innovation in Comparative Research // World Politics. 1997. Vol. 49. N 3. P. 430–451.

18. *Electoral* Authoritarianism: The Dynamics of Unfree Competition, Boulder. Lynne Rienner, 2006.
19. *Foster J. B., McChesney R.* Surveillance capitalism // Monthly Review [Электронный ресурс]. URL: https://monthlyreview.org/2014/07/01/surveillance-capitalism/ (дата обращения: 20.07.2021).
20. *Greene S., Robertson G.* Affect and Autocracy: Emotions and Attitudes in Russia after Crimea // Perspectives on Politics, 2020. First view. P. 1–15.
21. *Guriev S., Treisman D.* A theory of informational autocracy // Journal of Public Economics. 2020. Vol. 186.
22. *Howard P.* The Digital origins of dictatorship and democracy. Information technology and political Islam. Oxford University Press, 2011.
23. *Kendall-Taylor A., Frantz E., Wright J.* The Digital Dictators. How Technology Strengthens Autocracy // Foreign Affairs [Электронный ресурс]. URL: https://www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators (дата обращения: 20.07.2021).
24. *Krivy M.* Towards a critique of cybernetic urbanism: the smart city and the society of control // Planning theory. 2016. N 17 (1). P. 8–30.
25. *Levitsky S., Way L.* Competitive Authoritarianism. Hybrid regimes after the Cold War. Cambridge University Press, 2010.
26. *Melgaço L., Van Brakel R.* Smart Cities as Surveillance Theatre // Surveillance & Society. 2021. N 19 (2). P. 244–249.
27. *Polyakova A., Meserole C.* Exporting digital authoritarianism // The Brookings Institution [Электронный ресурс]. URL: https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190826_digital_authoritarianism_polyakova_meserole.pdf (дата обращения: 20.07.2021).
28. *Sterling B.* The Epic Struggle of the Internet of Things. Strelka Press, 2014.
29. *Zuboff S.* The age of surveillance capitalism: the fight for a human future at the new frontier of power. PublicAffairs, 2019.

Об авторах:

Балаян Александр Александрович, доцент департамента политологии и международных отношений Национального исследовательского университета «Высшая школа экономики» — Санкт-Петербург (Санкт-Петербург, Российская Федерация), кандидат политических наук; alexandr1138@mail.ru

Томин Леонид Владимирович, доцент кафедры политического управления Санкт-Петербургского государственного университета (Санкт-Петербург, Российская Федерация), кандидат политических наук; leopolit@yandex.ru

References

1. Agamben G. Homo sacer. State of exeption. M. : Europe, 2011. (In rus).
2. Balayan A. A., Tomin L. V. Digital autocracy. Institutional specifics of relations between the state and IT companies // Public policy [Publichnaya politika]. 2020. Vol. 4. N 2. P. 101–115. (In rus).
3. Bykov I. A. De-politicization of socially significant problems in digital platforms of public administration // Media in the modern world. 60th St. Petersburg Readings: procedings of the International Scientific Forum. In 2 vol. SPb.: Mediapapir, 2021. P. 192–193. (In rus).
4. Gel'man V.Y. The rise and fall of electoral authoritarianism in Russia // Center for Modernization Research [Electronic source]. URL: https://eusp.org/sites/default/files/archive/M_center/Electoral_Authoritarianism_in_Russia.pdf (accessed: 20.07.2021) (In rus).
5. Gel'man V.Y. Digitalization in Russia: (semi)transparency without accountability // Riddle [Electronic source]. URL: https://www.ridl.io/ru/cifrovizacija-v-rossii-polu-prozrachnost-bez-podotchetnosti/ (accessed: 20.07.2021) (In rus).
6. Golosov G. V. Electoral authoritarianism in Russia // Pro et Contra. 2008. N 1. P. 22–35. (In rus).
7. Deleuze G. Negotiations. SPb. : Science, 2004. (In rus).
8. Levitsky S., Way L. The rise of competitive authoritarianism // NZ. Debates on politics and culture [Neprikosnovenny`j zapas. Debaty` o politike i kul`ture]. 2018. N 5. P. 29–47. (In rus).
9. Polorotov A. A month after the rally in support of Navalny, law enforcement agencies drew up protocols for 289 people // Seldon News [Electronic source]. URL: https://news.myseldon.com/ru/news/index/251176822 (accessed 20.07.2021) (In rus).
10. Scott J. Good intentions of the state. M. : University book, 2005. (In rus).

11. Smorgunov L. V. Internet Public Administration Institutions: Comparative Analysis of Russia, Belarus and Kazakhstan // Administrative Consulting [Upravlencheskoe konsul`tirovanie]. 2020. N 12. P. 24–39. (In rus).
12. China's digital transformation. Experience of transforming the infrastructure of the national economy. M. : Alpina Publisher. 2019 (In rus).
13. Bischoff P. Data privacy laws and government surveillance by country: Which countries best protect their citizens? // Comparitech [Electronic source]. URL: https://www.comparitech.com/blog/vpn-privacy/surveillance-states/ (accessed: 21.07.2021).
14. Bischoff P. Surveillance camera statistics: which cities have the most CCTV cameras? // Comparitech [Electronic resource]. URL: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/ (accessed: 22.07.2021).
15. Bory P. The Internet Myth: From the Internet Imaginary to Network Ideologies. University of Westminster Press, 2020.
16. Burgers T., Robinson D. Networked authoritarianism is on the rise // Security and Peace. 2016. Vol. 34. N 4. P. 248–252.
17. Collier D., Levitsky S. Democracy with Adjectives: Conceptual Innovation in Comparative Research // World Politics. 1997. Vol. 49. N 3. P. 430–451.
18. Electoral Authoritarianism: The Dynamics of Unfree Competition, Boulder. Lynne Rienner, 2006.
19. Foster J. B., McChesney R. Surveillance capitalism // Monthly Review [Electronic source]. URL: https://monthlyreview.org/2014/07/01/surveillance-capitalism/ (accessed: 20.07.2021).
20. Greene S., Robertson G. Affect and Autocracy: Emotions and Attitudes in Russia after Crimea // Perspectives on Politics, 2020. First view. P. 1–15.
21. Guriev S., Treisman D. A theory of informational autocracy // Journal of Public Economics. 2020. Vol. 186.
22. Howard P. The Digital origins of dictatorship and democracy. Information technology and political Islam. Oxford University Press, 2011.
23. Kendall-Taylor A., Frantz E., Wright J. The Digital Dictators. How Technology Strengthens Autocracy // Foreign Affairs [Electronic source]. URL: https://www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators (accessed: 20.07.2021).
24. Krivy M. Towards a critique of cybernetic urbanism: the smart city and the society of control // Planning theory. 2016. N 17 (1). P. 8–30.
25. Levitsky S., Way L. Competitive Authoritarianism. Hybrid regimes after the Cold War. Cambridge University Press, 2010.
26. Melgaço L., Van Brakel R. Smart Cities as Surveillance Theatre // Surveillance & Society. 2021. N 19 (2) P. 244–249.
27. Polyakova A., Meserole C. Exporting digital authoritarianism // The Brookings Institution [Electronic source]. URL: https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190826_digital_authoritarianism_polyakova_meserole.pdf (accessed: 20.07.2021).
28. Sterling B. The Epic Struggle of the Internet of Things. Strelka Press, 2014.
29. Zuboff S. The age of surveillance capitalism: the fight for a human future at the new frontier of power. PublicAffairs, 2019.

About the authors:

Alexandr A. Balayan, Associate Professor of Department of Political Science and International Affairs, HSE Campus in St. Petersburg (Saint-Petersburg, Russian Federation), Candidate of Political Science; alexandr1138@mail.ru

Leonid V. Tomin, Associate Professor Department of Political Governance, Saint-Petersburg State University (St. Petersburg, Russian Federation), Candidate of Political Science; leopolit@yandex.ru