

РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ  
ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ им. А. И. ГЕРЦЕНА



ГЕРЦЕНОВСКИЕ ЧТЕНИЯ:  
РОССИЯ–2021.  
АКТУАЛЬНЫЕ ВОПРОСЫ  
ПОЛИТИЧЕСКОГО ЗНАНИЯ

Сборник материалов  
научно-практической конференции  
(23 апреля 2021 г.)

Санкт-Петербург  
Издательство РГПУ им. А. И. Герцена  
2021

ББК 66.2  
Г41

Под общей редакцией доктора политических наук  
заведующей кафедрой политологии  
*Л. А. Гайнутдиновой*

Редколлегия:

канд. полит. наук, доцент *С. В. Смаль*  
ст. преподаватель *М. С. Русских*

Организационно-техническая редакция:  
канд. полит. наук, мл. научный сотрудник *С. Ю. Зайцев*

Ответственный составитель:  
канд. полит. наук, мл. научный сотрудник *С. Ю. Зайцев*

Г41 **Герценовские чтения: Россия–2021.** Актуальные вопросы политического знания. Сборник материалов научно-практической конференции (23 апреля 2021 г.) / под общ. ред. Л. А. Гайнутдиновой. — Санкт-Петербург : Изд-во РГПУ им. А. И. Герцена, 2021. — 200 с.  
ISBN 978-5-8064-3130-2

Ежегодный сборник «Герценовские чтения: Россия–2021. Актуальные вопросы политического знания» посвящен ключевым аспектам современной политической повестки дня и включает в себя материалы ежегодной межвузовской научно-практической конференции, которая состоялась 23 апреля 2021 г. на базе РГПУ им. А. И. Герцена.

**ББК 66.2**

ISBN 978-5-8064-3130-2

© Авторы статей, 2021  
© С. В. Лебединский, оформление обложки, 2021  
© Издательство РГПУ им. А. И. Герцена, 2021

# СОДЕРЖАНИЕ

## РАЗДЕЛ I. ПЛЕНАРНОЕ ЗАСЕДАНИЕ

<i>Гайнутдинова Л. А.</i> Россия в поисках ответов на глобальные и региональные вызовы (политологический дискурс) . . . . .	6
<i>Грибанова Г. И.</i> Россия и Китай в глобальной политике: диалектика сотрудничества и конкуренции (на примере Арктического региона) . .	12
<i>Онопко О. В.</i> Российское направление современной украинской внешнеполитической экспертизы: основные институты и акценты в исследованиях . . . . .	17
<i>Гавриков А. В.</i> Политическая трансформация белорусского общества: феномен белорусского протеста (социально-политический аспект) . .	26

## РАЗДЕЛ II. РОССИЯ И МИР: 2021

<i>Вульфович Р. М.</i> Вакцина как элемент «мягкой силы»: место России в мире во время и после пандемии . . . . .	33
<i>Сирота Н. М.</i> «Новая нормальность» глобальной миросистемы: особенности и перспективы . . . . .	38
<i>Клещенко Л. Л.</i> Образ России в Латинской Америке в период пандемии COVID-19 . . . . .	43
<i>Близнецкая Е. А.</i> Влияние пандемии COVID-19 на глобальную экологическую повестку дня: перспективы для внешней и внутренней политики России . . . . .	49
<i>Невзоров М. В.</i> К программе исследования случаев участия России в миротворческих операциях . . . . .	54
<i>Фролова Ю. Н.</i> Возможности теории драмы при анализе этнополитических конфликтов: пример Страны Басков . . . . .	59
<i>Осинов В. А.</i> Оцифровывая Левиафана: о некоторых случаях виртуальных и кибергосударств . . . . .	64
<i>Гладченко И. А.</i> О роли символов в цифровизации политических процессов . . . . .	68
<i>Балаян А. А., Томин Л. В.</i> Политические эффекты цифровой трансформации городского управления (на примере Москвы) . . . . .	74

**РАЗДЕЛ III. ВЫБОРЫ В РОССИИ 2021 ГОДА:  
контекст, анализ, технологии**

<i>Скоробогатько А. В.</i> Новая социальность в постковидном мире . . . . .	82
<i>Рябов О. В., Рябова Т. Б.</i> Негативная легитимация власти как прием символической политики . . . . .	86
<i>Морозова О. С.</i> Внедрение альтернативных практик голосования: оценка рисков международными организациями в сфере наблюдения на выборах . . . . .	92
<i>Зайцев С. Ю.</i> Направления деятельности оппозиционных движений Санкт-Петербурга в преддверии выборов 2021 года . . . . .	97
<i>Паиковский Е. А.</i> Место внешней политики в предвыборных программах парламентских политических партий России и Польши . . . . .	101
<i>Кандыба Р. А.</i> Кампания по выборам депутатов Государственной Думы-2021 в контексте требований современности . . . . .	106
<i>Крылова М. А.</i> Культурологические аспекты функционирования идеологий политических партий на выборах 2021 г. . . . .	111
<i>Кетов А. Р.</i> Актуальные проблемы демократического транзита в современной России . . . . .	115
<i>Смаль С. В.</i> Социальная политика в программах политических партий России на выборах 2021 года . . . . .	119
<i>Камари Д. М.</i> Цифровизация и политические партии: новый вектор развития . . . . .	126

**РАЗДЕЛ IV. ТРИБУНА МОЛОДЫХ УЧЕНЫХ**

<i>Романова И. О.</i> Ответ России на глобальные вирусологические угрозы: опыт борьбы с COVID-19 . . . . .	132
<i>Шевцов А. Н.</i> Цифровые государственные услуги в современной России: проблемное поле развития . . . . .	138
<i>Ташкенова Д. Ш.</i> Трансформация электронного правительства в цифровое государство: вызовы и решения . . . . .	141
<i>Гусаров А. В.</i> Роль цифровой дипломатии в борьбе с дезинформацией и пропагандой . . . . .	144
<i>Поджидаева А. Ю.</i> Цифровизация политики как новый инструмент общественного взаимодействия . . . . .	148
<i>Ребриков Д. Д., Посредник А. В.</i> Проблемы и перспективы правового регулирования электронного голосования в России . . . . .	151
<i>Меркулова К. О.</i> Проблема ограничения представительного характера Государственной Думы Российской Федерации: о самовыдвижении . . . . .	154

<i>Артюнов А. Г., Корниевский А. А.</i> «Единая Россия» в преддверии выборов 2021: динамика результатов партии на региональных выборах 2018–2020 .....	158
<i>Лукушин В. А.</i> Цифровые аудитории российских политических партий: результаты социально-медийного анализа .....	163
<i>Ангаев М. В.</i> Реформа институтов развития 2020 г. ВЭБ.РФ как инструмент реализации национальных целей .....	167
<i>Крюкова А. С.</i> Роль инфраструктурных проектов в государственной антикризисной политике .....	170
<i>Буздыханова С. Ю.</i> Политический региональный лидер: ожидания и предпочтения граждан на основе социологических исследований (ФОМ, ВЦИОМ, Левада-Центр) .....	174

## **V. УЧЕБНО-МЕТОДИЧЕСКИЙ РАЗДЕЛ**

<i>Невзоров М. В., Фролова Ю. Н.</i> Структура и содержание рабочей программы дисциплины «Организационная культура политических акторов» .....	179
Abstracts and keywords .....	186
Сведения об авторах .....	196

7. *Cohen A.* The politics of elite culture: explorations in the dramaturgy of power in a modern African society. Berkeley: Univ. of California press, 1981. 262 p.
8. *Карасик В. И.* Языковые ключи. М.: Гнозис, 2009. 406 с.
9. *Попова З. Д., Стернин И. А.* Семантико-когнитивный анализ языка: научное издание. Воронеж: ИСТОКИ, 2007. 250 с.

*Балаян А. А., Томин А. В.*

## ПОЛИТИЧЕСКИЕ ЭФФЕКТЫ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ГОРОДСКОГО УПРАВЛЕНИЯ (НА ПРИМЕРЕ МОСКВЫ)

*Аннотация.* В последние годы возникла и стала распространяться по миру новая социотехническая модель управления — цифровая автократия. Возникновение цифровых автократий не было результатом изначального плана правящего класса по политическому использованию интернета. Это констелляция множества факторов, сложившихся в процессе адаптации политических режимов в ряде стран к внешним (глобальная экономическая конкуренция, внешнеполитические конфликты) и внутренним (политическая дестабилизация) вызовам. Работа посвящена исследованию места и роли «умных городов» в социотехнической модели управления цифровых автократий на примере процессов, которые происходят в Москве. Отдельно рассмотрены проблемы, связанные с использованием данных в городском управлении: избыточный сбор данных и непрозрачность государственных информационных систем.

*Ключевые слова:* цифровизация сверху, городское управление, умный город, автократия, большие данные.

Одним из эффектов политики правительств по контролю над перемещением населения в условиях пандемии коронавируса, стало осознание многими гражданами механизмов мониторинга и контроля повседневной жизни посредством цифровой инфраструктуры. В последние годы вышло множество работ, посвященных различным негативным эффектам цифровизации: усиливающемуся государственному и корпоративному контролю над жизнью граждан [1], растущему экономическому неравенству [2] и непрозрачности цифровых алгоритмов управления [3]. Большинство подобных исследований посвящено государствам, которые в различных индексах относят к демократиям.

Существуют работы, посвященные китайской системе социального кредита, но пока недостаточно концептуально осмыслен сам феномен

использования цифровых технологий различными автократиями (однопартийными, электоральными). Ряд уже имеющихся работ демонстрирует, что цифровизация дает автократиям новые техники управления и социального контроля [4]. В последние годы появляются эмпирические исследования механизмов функционирования цифровых автократий, осуществленные на примерах ряда стран [5]. Политологи для именованной этой новой модели используют различные названия: «цифровой авторитаризм», «сетевой авторитаризм» [6]. Проблема «возвышения цифровых автократий» отмечена как главная в ежегодном докладе организации Freedom House, посвященном свободе интернета (2018 г.) [7]. События последних лет демонстрируют, что одним из механизмов стабилизации и легитимации режима правящие элиты автократий выбрали управляемую и контролируруемую сверху цифровизацию.

**Подъём цифровых автократий.** В 1990-е — начале 2000-х — начале обсуждения цифровизации и влияния интернета доминировала оптимистическая точка зрения. Интернет описывался как децентрализованная система, формирующая новую прогрессивную модель экономики (открытая, коллаборативная, экологичная) и политики (сетевые модели управления, возрождение прямой демократии) [8]. Автократиям с их системами цензуры в этом цифровом мире не было места, считалось, что они не смогут выжить в условиях свободно циркулирующих информационных потоков. В тот период лишь отдельные исследователи отмечали амбивалентную роль интернета в процессах демократизации. 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» [9].

Появление цифровых автократий не было результатом изначального плана правящего класса по политическому использованию интернета. Это констелляция множества факторов, связанных с трансформацией неолиберализма и адаптации к этому стран в различных регионах, технологическим развитием экономики больших данных. Прежде чем перейти к анализу цифровых автократий необходимо описать экономические изменения, сформировавшие цифровую инфраструктуру для экономики

больших данных. В качестве методологической основы для исследования трансформации неолиберализма, формирования платформенной экономики мы используем концепции: «капитализма платформ» Н. Срничека [10] и «надзорного капитализма» Дж. Б. Фостера, Р. МакЧесни [11]. Основа бизнес-модели «капитализма платформ» («надзорного капитализма») — 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 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 — это т. н. «умный дом» или интегрированные экосистемы интернета вещей. Верхний уровень включен в существующие отдельные элементы системы «умных городов» (камеры видеонаблюдения, Wi-Fi, система датчиков).

В условиях цифровой автократии как специфического ассамбляжа (или исторической констелляции) 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. 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).

В американском контексте процессы цифровизации и проекты «умных городов» во многом инициированы крупнейшими IT-компаниями, поскольку именно платформы контролируют цифровую инфраструктуру. Для них это инструмент доминирования на рынке, их рыночная и политическая сила основана на сетевых эффектах от цифровой инфраструктуры. В институциональном ландшафте автократий трансформируется роль и функции «умного города», он отчасти сохраняет логику бизнес-модели платформенных компаний, но его функциональность интегрируется в контролируемую государством и аффилированными с ним компа-

ниями социотехническую модель социального контроля. Цифровая автократия собирает и анализирует данные граждан и на этой основе формирует систему «перевернутой подотчетности». Цифровизация сверху усиливает информационную асимметрию, поскольку делает более прозрачной не правительство, а общество. Городское управление, основанное на больших данных, в условиях автократии реально не ограничено в использовании собранной информации. Информационные системы в цифровых автократиях собирают избыточное, с точки зрения нужд управления, количество данных. Кроме того, непрозрачны сами государственные информационные системы, граждане не знают кем и как их данные используются.

Главным примером политического использования автократиями цифровой инфраструктуры в национальном масштабе является система фильтрации интернет-контента «Великий китайский файрвол». Изначально она позволяла 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 контроля над интернетом стал запрет и блокировка зарубежных социальных сетей и сервисов (Facebook, Instagram, Twitter), поисковиков (Google), видеохостингов (YouTube). Блокировка данных сервисов сопровождалась развитием китайских альтернативных продуктов, технологически и юридически встроенных в национальную систему управления интернетом (Renren, Baidu, Sina Weibo, Youku).

Развитие цифровой инфраструктуры создало условия появления системы социального кредита — 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). Система социального кредита разработана на основе продукта компании Alibaba (Sesame Credit). В системе социального кредита центральным элементом сотрудничества государства и частных IT-компаний является программа развития «умных городов». Она охватила 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. Протесты в Гонконге, начавшиеся в 2019 году, продемонстрировали новые модели протеста граждан в условиях цифровых автократий. Протестующие в Гонконге понимали, что цифровая инфраструктура, например уличные камеры, оснащенные

технологией распознавания лиц, — это репрессивный инструмент, используемый полицией.

Модель цифровой автократии или ее отдельные элементы в последние годы начали распространяться по миру. В докладе о свободе интернета за 2018 год 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. Тридцати восьми странам поставляется цифровая инфраструктура, восемнадцати — интегрированные системы камер с технологией распознавания лиц и в тридцати шести проводятся тренинги официальных лиц и журналистов [7].

***Роль цифровой инфраструктуры в Москве.*** В исследованиях и различных индексах измерения демократии политический режим, существующий в Российской Федерации, характеризуется как автократический или гибридный [12]. Так, один из разработчиков концепции электорального авторитаризма А. Шедлер определял его как режим, не являющийся демократией, но который не использует репрессивные практики регулярно [13]. По ряду признаков видно, что в качестве успешных моделей и примеров цифровизации сверху, российские власти выбрали КНР и Сингапур. Столица страны — Москва — стала лабораторией, где подобная система «умного города» выстроена. В дальнейшем планируется копировать данную модель в других крупных городах.

Сергей Собянин с 2008 года занимал должность главы аппарата правительства РФ и курировал программу по цифровизации государственных услуг («Информационное общество»). Став мэром Москвы, он с 2012 года инициировал программу формирования модели «умного города», основанного на интегрированной цифровой инфраструктуре и системе сбора и анализа данных («Информационный город»). Процесс формирования цифровой инфраструктуры и пула данных начался с государственных услуг и сервисов и создания интеллектуальной транспортной системы управления трафиком. Цифровая инфраструктура позволила извлекать данные постоянно и почти из всех действий горожан.

Общий пул данных, собираемый мэрией о горожанах, можно разделить на несколько потоков:

1. Геоаналитические данные операторов сотовой связи. С 2015 года 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 («Безопас-

ный 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 бесплатного публичного wi-fi. По соглашению с пользователем при входе в wi-fi, оператор использует технологию Deep Packet Inspection 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 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).

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.

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) [14]. По контракту они могут быть расшифрованы и переданы в виде обычного номера телефона. Одним из наиболее важных элементов цифровой инфраструктуры Москвы как «умного города» являются камеры видеонаблюдения, оснащенные функцией распознавания лиц. Все они интегрированы в единую систему хранения и обработки данных (ЕЦХД). Камеры расположены на улицах, в метро, в государственных учреждениях, во дворах и подъездах домов, больницах, школах. Важно отметить, что в период пандемии контроль над перемещением граждан получил новый импульс. Например, данные геолокации телефона и система камер наблюдения

с функцией распознавания лиц использовались для наказания нарушителей режима карантина.

27 июля и 3 августа 2019 перед выборами в Мосгордуму проходили акции протеста, связанные с отказом в регистрации многим оппозиционным кандидатам. В эти дни в местах проведения митингов зафиксировано отключение мобильного интернета и wi-fi-сетей кафе и других заведений, находящихся поблизости от мест проведения митинга. Согласно закону «О связи» по требованию организаций, осуществляющих оперативно-розыскную деятельность или обеспечение безопасности операторы должны приостановить оказание услуг связи юридическим и физическим лицам. Лаборатория NetBlocks выяснила, 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» [15]. В их докладе отмечается, что измерения с приложения Android Network Cell Info Lite показали — часть станций операторов мобильной связи работали в режиме GSM-only. Локальное отключение мобильного интернета произошло в северной части центрального округа Москвы, именно там проходил митинг. 23 и 31 января 2021 года в тех частях Москвы, где проходили акции в поддержку А. Навального, NetBlocks зафиксировала аналогичное отключение интернета. Кроме того, полиция подтвердила, что в метро задерживали участников несанкционированных акций используя систему камер с технологией распознавания лиц [16].

Глядя на современную Россию, мы наблюдаем попытку авторитарного режима укрепиться, используя цифровые технологии, которые массово трансплантируются из других регионов мира, прежде всего, из Сингапура и Китая. В силу социально-экономического дисбаланса тестовым городом выступает Москва, где создана специфическая модель «умного города», а администрация полностью контролирует цифровую инфраструктуру. Система слежения, построенная в Москве, в условиях непрозрачности и отсутствия реальных инструментов контроля за решениями властей дополнительно усиливает информационную асимметрию и политическую нестабильность. Проблемным здесь выступает то, что в отличие от Китая или Сингапура, в стране, помимо политических, отсутствуют современные экономические институты и господствует сырьевая модель экономики. В такой ситуации, построение цифрового авторитаризма связано с целым рядом издержек и будет постоянно нуждаться в ужесточении, что мы и наблюдаем в последние несколько лет. Это значит, что от условно «мягкой» сингапурской модели страна будет постепенно переходить к «жесткой» китайской.

## Литература

1. *Zuboff S.* The age of surveillance capitalism: the fight for a human future at the new frontier of power. Public Affairs, 2019. 704 p.
2. *Eubanks V.* Automating inequality. How high-tech tools profile, police, and punish the poor. St. Martin's Press. 2018. 288 p.
3. *Pasquale F.* The black box society. The secret algorithms that control money and information. Harvard University Press. 2015. 320 p.
4. *Morozov E.* The net delusion: The dark side of internet freedom. Public Affairs, 2011. 432 p.
5. *Burgers T., Robinson D.* Networked authoritarianism is on the rise // Security and Peace. 2016. Vol. 34. № 4. P. 248–252.
6. *Pearce K., Kendzior S.* Networked authoritarianism and social media in Azerbaijan // Journal of Communications. 2012. Vol. 62. Issue 2. P. 248–252.
7. 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: 15.03.2021).
8. *Bory P.* The Internet Myth: From the Internet Imaginary to Network Ideologies. University of Westminster Press. 2020. 168 p.
9. *Kalathil S., Boas T.* Open networks, closed regimes. The impact of the internet on authoritarian rule. Carnegie Endowment for International Peace. 2003. 218 p.
10. *Srnicek N.* Platform capitalism. Polity, 2016. 120 p.
11. *Foster J. B., McChesney R.* Surveillance capitalism. Monthly Review. 01.07.2014. URL: <https://monthlyreview.org/2014/07/01/surveillance-capitalism/> (дата обращения: 15.03.2021).
12. Polity IV Project. URL: <https://www.systemicpeace.org/polity/polity4.htm> (дата обращения: 15.03.2021).
13. *Schedler A.* The Menu of Manipulation // Journal of Democracy. 2002. Vol. 13. Issue 2. P. 36–50.
14. *Захаров А.* «Умный город» или «Старший брат»? Как мэрия научилась знать о москвичах всё. Русская служба ВВС. 10.04.2020. URL: <https://www.bbc.com/russian/features-52219260> (дата обращения: 15.03.2021).
15. Evidence of internet disruptions in Russia during Moscow opposition protests. NetBlocks. 03.08.2019. URL: <https://netblocks.org/reports/evidence-of-internet-disruptions-in-russia-during-moscow-opposition-protests-XADErzBg> (дата обращения: 15.03.2021).
16. *Камалетдинов Д.* Система распознавания лиц в Москве теперь ищет протестующих. Как она устроена и что сделать для защиты. Tjournal. 04.02.2021. URL: <https://tjournal.ru/tech/333457-sistema-raspoznavaniya-lic-v-moskve-teper-ishchet-protetstuyushchih-kak-ona-ustroena-i-chto-sdelat-dlya-zashchity> (дата обращения: 15.03.2021).