ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/2226-7867-2021-11-3-55-61
УДК 32(045)

Электронное голосование в России: технологический и политический аспекты

О.В. Ерохина
Финансовый университет, Москва, Россия
https://orcid.org/0000-0002-5453-4118

АННОТАЦИЯ

Основные направления применения цифровых технологий в российском политическом процессе связаны с проведением электронного голосования, а также использованием интернет-сервисов для развития новых форм политического участия, как на общегосударственном уровне, так и в сфере местного самоуправления. Рост числа интернет-пользователей, ставший устойчивой тенденцией последних 20 лет, создает новые условия для взаимодействия властных структур и общества. Они включают как новые риски дестабилизации, связанные с повышением требований к государственным институтам и снижением доверия к власти, так и новые возможности для взаимодействия государства и общественности в социально значимых сферах госуправления. Реализация на практике курса, обозначенного программой «Цифровая экономика» и призванного обеспечить конкурентные преимущества России с учетом глобальных тенденций ожидания либо наступления (по разным оценкам) четвертой промышленной революции, создает новый контекст для развития политических процессов. В этих условиях электронные технологии голосования рассматриваются как неотъемлемая часть развития современного государства, и этот взгляд характерен, в том числе, для значительной части политических элит.

Ключевые слова: электронное голосование; доверие власти; электоральные процессы; технология блокчейн

Для цитирования: **Ерохина О.В. Электронное голосование в России: технологический и политический аспекты.** ***Гуманитарные науки. Вестник Финансового университета.*** **2021;11(3):55-61. DOI: 10.26794/2226-7867-2021-11-3-55-61**

ORIGINAL PAPER

Prospects of Electronic Voting in Russia: Technological and Political Aspects

O.V. Erokhina
Financial University, Moscow, Russia
https://orcid.org/0000-0002-5453-4118

ABSTRACT

The main areas of application of digital technologies in the Russian political process are related to the conduct of electronic voting and the use of Internet services for the development of new forms of political participation both at the national level and in the field of local self-government. The growth in the number of Internet users, which has become a steady trend over the past 20 years, creates new conditions for interaction between government structures and society. They include both unknown risks of destabilization associated with increased demands on state institutions and reduced confidence in the government, as well as new opportunities for interaction between the state and the public in socially significant areas of public administration. The implementation in practice of the course outlined by the Digital Economy program and designed to ensure Russia's competitive advantages, taking into account the global trends of the expectation or the onset (according to various estimates) of the fourth industrial revolution, creates a new context for the development of political processes. In these conditions, the author considered electronic voting technologies an integral part of the development of the modern state, and this view is typical, including for a significant part of the political elites.

Keywords: electronic voting; trust in the authorities; electoral processes; blockchain technology

For citation: **Erokhina O.V. Prospects of electronic voting in Russia: Technological and political aspects.** ***Gumanitarnye Nauki. Vestnik Finasovogo Universiteta = Humanities and Social Sciences. Bulletin of the Financial University.*** **2021;11(3):55-61. (In Russ.). DOI: 10.26794/2226-7867-2021-11-3-55-61**

ВВЕДЕНИЕ

Прежде чем рассматривать подробнее практику применения технологий электронного голосования в России, необходимо уточнить используемую для их анализа терминологию. Так, различают стационарное и дистанционное голосование: оба способа волеизъявления граждан предполагают возможность использования «цифровых» решений, однако дистанционное голосование осуществляется при отсутствии избирателей на участке или в ином специально оборудованном месте, а стационарное — только при условии личного присутствия избирателя. «Электронным» голосованием считают процедуру волеизъявления избирателей, подсчета голосов и подведения итогов голосования с помощью специальных электронных технических средств [1]. Кроме того, анализ нормативно-правовой базы позволяет акцентировать внимание на отсутствии применения бумажных бюллетеней при проведении электронного голосования [2].

Дистанционное голосование проводится в РФ с 2019 г. в виде эксперимента разной степени масштабности и предполагает использование специальных цифровых платформ, двухступенчатой системы шифрования данных для соблюдения анонимности волеизъявления и принципов блокчейн для обеспечения достоверности результатов голосования и обеспечения информационной безопасности. Можно прогнозировать, что границы применения технологий голосования через интернет будут существенно расширены уже в ближайшем будущем.

По предварительным данным, дистанционное электронное голосование пройдет в 10 субъектах федерации (в том числе, в Москве) во время «единого дня голосования» в сентябре 2021 г., однако список может быть дополнен после рассмотрения Центризбиркомом соответствующих заявок от администраций субъектов федерации. На данном этапе, кроме столицы, к проведению электронных выборов готовятся Ярославская, Курская, Нижегородская, Вологодская, Мурманская, Рязанская области, республики Северная Осетия и Бурятия, а также Севастополь, однако окончательный список субъектов, переходящих на цифровую форму голосования, еще не утвержден.

Обобщая заявления руководства Центризбиркома, можно сформулировать ряд критериев отбора региональных заявок. Во-первых, учитываются технические требования. Среди них: широкое использование интернет-технологий населением, достаточное число совершеннолетних пользователей электронных госуслуг. Также необходим реестр актуальных данных о гражданах, имеющих право голоса и зарегистрированных на Едином портале госуслуг, который используется для авторизации при получении бюллетеня. При этом указанные сведения должны соответствовать данным автоматизированной системы «Выборы» (ГАС «Выборы»). Во-вторых, отметим политический аспект готовности к внедрению электронного голосования, включающий как наличие квалифицированных кадров и возможности для обучения членов региональных избирательных комиссий, так и целенаправленную PR-поддержку и разъяснительную работу среди населения, которое в целом пока настороженно относится к электронному голосованию. Возможность наблюдения за ходом выборов со стороны региональных общественных палат и иных общественных организаций вряд ли может кардинально повлиять на общественное мнение, так как уровень доверия этим структурам также невысок.

Проиллюстрируем неоднозначное отношение граждан к электронному голосованию данными социологических исследований. Как показал опрос ВЦИОМ в 2020 г.,[1] при возможности выбора способа голосования 23% россиян предпочли бы проголосовать с помощью электронных технологий, хотя в целом возможность использования электронного голосования допускают 51% опрошенных; 69% высказались за использование традиционной электоральной процедуры на избирательных участках с бумажными бюллетенями (в случае выбора из нескольких альтернатив). Основные причины настороженного отношения к электронному голосованию связаны с недостаточным материально-техническим обеспечением избирателей, а также с опасениями насчет возможных фальсификаций, нарушения тайны голосования и т.д. Немаловажен низкий уровень информированности населения о новых технологиях волеизъявления: общая доля тех, кто ничего не знает об электронном голосовании или плохо информирован, в мае 2020 г. составила 86%. Также можно отметить рост положительных оценок электоральной процедуры, хотя сформированные еще в 1990-е гг. представления о широко распространенных нарушениях в ходе проведения голосования сохраняют свою значимость. Так, по исследованиям ВЦИОМ, в 2007–

[1] Электронное голосование: новые технологии меняют электоральные привычки. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/elektronnoe-golosovanie-novye-tekhnologii-menyayut-elektoralnye-privychki.

2011 гг. доля граждан, уверенных в достоверности результатов выборов, колебалась от 21 до 45% [3], а в марте 2021 г. более половины (57%) опрошенных оценили подсчет голосов на известных им выборах как «скорее честный» и заслуживающий доверия, но при этом 42% указали, что «слышали о нарушениях», хотя и не сталкивались с ними лично, а 48% не сталкивались с фальсификациями[2]. В описанной ситуации, учитывая курс на внедрение цифровых инструментов и сервисов в сферу политических процессов и госуправления, целесообразной выглядит разработка властными структурами мер информационного характера, направленных на преодоление стереотипов и формирование положительного отношения к интернет-решениям в избирательном процессе. Ниже будут рассмотрены особенности технологии электронного голосования с точки зрения обеспечения честности и «прозрачности» электоральной процедуры, а также показано значение фактора доверия общества новым институтам.

БЛОКЧЕЙН ДЛЯ ПРОВЕДЕНИЯ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Ключевые особенности применяемых в России технологий дистанционного электронного голосования связаны с использованием технологии блокчейн — созданием распределенного реестра данных по тому же принципу, что применяется в децентрализованной среде Ethereum. В результате реализации решений блокчейн формируется выстроенная по определенным правилам непрерывная последовательная цепочка информационных блоков (транзакций), связь между которыми и безопасность цепочки в целом обеспечивается криптографическими методами. В рассматриваемом примере транзакции — это акты голосования. К достоинствам технологии блокчейн, особенно востребованным в политическом процессе, можно отнести отсутствие необходимости в участии третьей доверенной стороны. На каждом из компьютеров пользователей цепочки транзакций хранится полная, обновляемая с каждой транзакцией копия данных всего блокчейна. Пока функционирует хоть одно устройство хранения данных любого пользователя, сведения в блокчейне существуют. Однажды внесенная в распределенный реестр запись уже не может быть изменена или стерта, однако возможно внесение корректировок путем проведения новых транзакций, и после того, как информация о каждой из них станет частью нового блока, обновленные данные появятся у каждого участника сети. В настоящее время сформированы две платформы для обеспечения реализации избирательных прав граждан в режиме онлайн. Первая, разработанная Правительством (Департаментом информационных технологий) Москвы функционирует в столичном регионе, вторая, основанная на решениях компании «Ростелеком», имеет общефедеральный «радиус распространения». В основе обеих платформ лежат сходные принципы доступности для широкого круга пользователей, обеспечения анонимности голосования и безопасности передачи данных.

Указанные особенности позволяют рассматривать решения блокчейн как наиболее востребованный в настоящее время способ обеспечения «прозрачности» хода голосования и подсчета его результатов. Вместе с тем задача обеспечения анонимности волеизъявления вряд ли может быть решена полностью. Это актуализирует вопрос о целесообразности применения технологии блокчейн в политических процессах. Технологически подобные решения обеспечивают высокий уровень сохранности данных и защиты от вмешательств (внешних воздействий), однако основополагающие принципы (в случае электоральных процедур — это соблюдение тайны голосования и честность подсчета результатов) будут работать только в том случае, если общество характеризуется высоким уровнем доверия к властным структурам/государству.

Технологические изменения нередко сопровождаются обратным эффектом снижения поддержки властей и ростом угроз безопасности, связанных со сбором и использованием «больших данных» [4]. Исследования рисков, связанных с внедрением цифровых технологий, отмечают в числе негативных факторов применение инноваций в интересах государства в ущерб общественным инициативам, рост административных барьеров, а также расширение сферы для манипуляций и негативную реакцию потенциальных избирателей [5]. Вопрос о мерах для снижения политических рисков внедрения цифровых технологий заслуживает особого внимания. Так или иначе, даже при благоприятном сценарии технологических изменений позиционировать решения на основе блокчейн как автоматизированную гарантию честности и «прозрачности» избира-

[2] Выборы в российских регионах: легитимность, доверие, нарушения. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/vybory-v-rossiiskikh-regionakh-legitimnost-doverie-narushenija.

тельного процесса (в противовес ассоциируемому со злоупотреблениями «человеческому фактору») нецелесообразно. При всех преимуществах технологии создания распределенного реестра данных технически невозможно ни гарантировать отсутствие «утечек» информации в результате хакерских атак, ни полностью исключить возможность неправомерной интерпретации результатов голосования. Рассмотрим особенности применения решений блокчейн на примере технологии электронного голосования, используемой в российских регионах на основе решения компании «Ростелеком».

ПЛАТФОРМА «РОСТЕЛЕКОМ» ДЛЯ ОБЩЕРОССИЙСКОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

После экспериментальных выборов, проведенных в Москве в 2019–2020 гг., дальнейшим развитием опыта электронного голосования в России стала разработанная по заказу ЦИК РФ интернет-система дистанционного волеизъявления «Ростелеком». Компания распространяет на специализированных ресурсах большое количество материалов, свидетельствующих об успешном прохождении мониторинга системы, надежности применяемых протоколов шифрования данных, а также высокой степени ее защищенности от угроз информационной безопасности. Открытых данных об особенностях функционирования платформы, разработанной «Ростелекомом», больше, чем сведений о технологиях организации электронного голосования в Москве, и они отличаются последовательностью и системным подходом к описанию технических параметров. Таким образом, можно говорить о целенаправленном PR-продвижении системы электронного дистанционного голосования еще до начала ее применения в общегосударственном масштабе. Это в полной мере соответствует курсу, предполагающему расширенное применение цифровых технологий в сфере политических процессов.

Общая конфигурация системы дистанционного электронного голосования, применение которой в общероссийском масштабе ожидается уже в сентябре 2021 г., представлена на *рисунке*.

Общероссийская платформа «Ростелекома» изначально позиционируется как сложная система, использующая как технологию блокчейн, так и иные способы организации взаимодействия между условными избирателями, наблюдателями и уполномоченными органами власти в лице избирательных комиссий. Основные цели ее работы предсказуемо связываются с требованиями федерального законодательства о гарантиях избирательных прав граждан[3], среди которых тайна голосования и неизменность волеизъявления, открытость и публичность процесса голосования, отсутствие возможности подсчитать результат голосования до окончательного завершения электоральной процедуры и пр.

Необходимым условием реализации избирательного права в рассматриваемой системе выступает прохождение идентификации личности с помощью портала государственных услуг. За составление актуального списка избирателей отвечает такой компонент системы, как «Список избирателей», с ним же связан процесс создания идентификаторов в системе блокчейн для присвоения уникального номера каждому лицу, имеющему право на участие в голосовании. Отметим, что доступ к списку избирателей имеют как члены избирательной комиссии, так и наблюдатели, и в этом смысле электронная система мало отличается от традиционной.

После прохождения идентификации избирателя решается одна из ключевых задач системы электронного голосования, связанная с анонимизацией пользователей. Голосование происходит с использованием личного цифрового устройства, и в это время пользователь уже «невидим» для системы: анонимный голос зашифровывается и передается в «хранилище» голосов, созданное по технологии распределенного реестра данных. Одновременное установление личности и шифрование данных возможно путем применения «слепой электронной подписи». Это широко известный криптографический алгоритм [6], работа которого в рамках системы электронного голосования связана с другими алгоритмами, обеспечивающими шифрование данных.

Вопрос обеспечения тайны голосования проработан в системе электронного голосования от «Ростелеком» весьма подробно и с технической точки зрения сомнений не вызывает. В ходе голосования используется алгоритм выдачи и проверки слепой подписи на базе алгоритма шифрования RSA, далее происходит создание общего открытого ключа шифрования (на основе криптографических алгоритмов, подразумевающих создание распределенного реестра для выработки ключа

[3] Федеральный закон от 12.06.2002 № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_37119/.

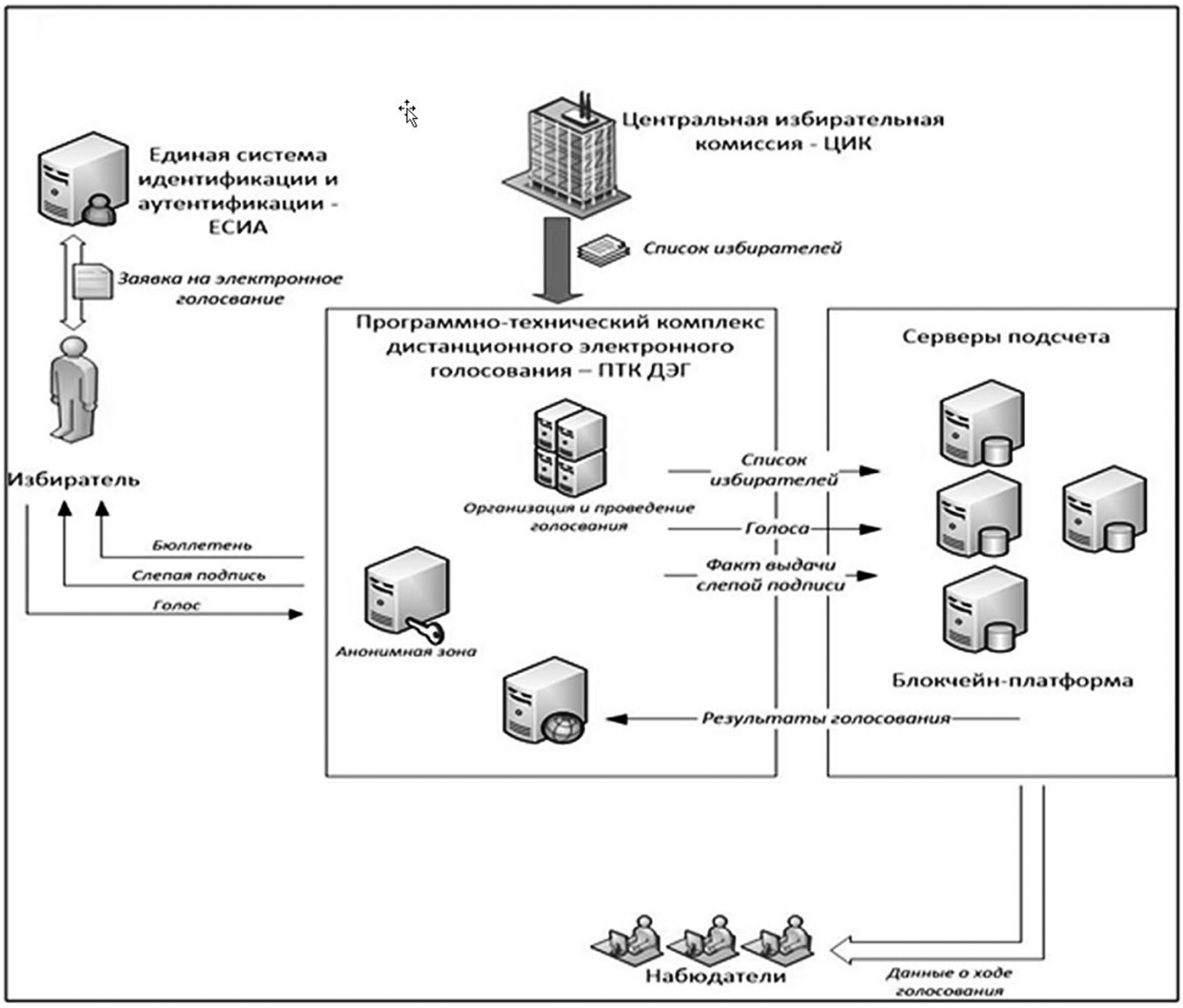

Рис. / Fig. **Основные элементы системы дистанционного электронного голосования / The main elements of the remote electronic voting system**

Источник / Source: составлено автором по данным открытых источников / Compiled by the author according to open sources.

и дальнейшее его разделение программными методами). Сложная двухступенчатая система призвана гарантировать безопасность передачи данных. Как и в других системах электронного голосования, для получения бюллетеня используется технология электронной подписи по стандарту ГОСТ Р 34.10–2012, а для шифрования каждого голоса и дешифрования общих результатов голосования используется протокол по схеме Эль-Гамаля на эллиптических кривых и доказательство с нулевым разглашением Disjunctive Chaum-Pedersen range proof. Список используемых в рассматриваемой системе голосования криптографических протоколов далеко не полон, важно учитывать, что платформа «Ростелекома», как и другие подобные системы, предусматривает возможность замены алгоритмов шифрования в случае возникновения угроз безопасности либо некорректного функционирования системы. Сложность изучения механизмов шифрования данных в системах электронного голосования состоит в том, что процесс решения задачи анонимизации голоса избирателя специальными техническими средствами, как правило, не освещается в открытых источниках, тем более, крайне сложно найти информацию о проблемах применения того или иного алгоритма криптографии.

ВЫВОДЫ

В настоящее время властные структуры ведут информационную кампанию в поддержку новых цифровых решений с тем, чтобы повысить уровень доверия широких слоев потенциальных избирателей к процедуре онлайн-голосования и предотвратить возможные спекуляции на тему нарушения государством принципов неразглаше-

ния персональных данных и иных угроз, связанных с избыточным контролем и ограничением гражданских свобод. По официальным данным руководства ЦИК, основная цель модернизации избирательной системы в виде снижения числа злоупотреблений и усиления контроля за соблюдением законодательства в сфере реализации избирательных прав граждан, уже достигнута [7]. Однако эта публичная позиция не отменяет необходимости дальнейшего расширения применения цифровых технологий в электоральном процессе.

В результате анализа технологических особенностей применяемой в РФ системы электронного голосования можно констатировать, что при ее разработке выполняющая госзаказ компания «Ростелеком» опиралась на общепризнанные требования к организации и функционированию подобных систем. Среди важнейших из них — тайна голосования, легитимность всех участников, невозможность изменения результатов после завершения голосования [8]. Отметим, что приоритетом государства, как и в случае с другими системами дистанционного электронного голосования, выступает обеспечение надежной защиты от внешних воздействий, а не выстраивание наиболее эффективных взаимодействий в процессе сбора и передачи данных о голосовании. Об этом, в частности, свидетельствует подключение созданной «Ростелекомом» платформы к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)[4], которая включает иерархически организованный комплекс информационных центров, распределенных по территории страны. Основная задача ГосСОПКА — сбор информации об угрозах информационной безопасности для выработки мер превентивной защиты. Аппаратно-программный комплекс электронного голосования считается объектом критической информационной инфраструктуры, вследствие чего включается в общегосударственную систему обмена информацией об угрозах безопасности и кибератаках. В рассматриваемом примере безопасность данных находится в сфере ответственности ПАО «Ростелеком»: центры обработки данных компании обеспечивают размещение и функционирование создаваемого распределенного реестра, хотя к этому процессу в любой момент могут подключиться и другие участники (например, общественные организации в статусе наблюдателей). Однако возможность контроля за хранением данных либо частичного дешифрования итогового бюллетеня с помощью отдельных частей закрытого ключа не означает доступа к механизмам обеспечения информационной безопасности, которые остаются под контролем специалистов «Ростелеком».

В связи с технологическими особенностями системы электронного голосования вопрос легитимности власти и доверия властным институтам со стороны общества приобретает новую актуальность. Абсолютная «прозрачность» электоральной процедуры, как и анонимность пользователей, недостижимы при использовании решений на основе технологии блокчейн в политическом процессе. Это не отменяет возможности применения электронного голосования и не обесценивает его преимущества, однако ставит вопрос о необходимости эффективного взаимодействия между государством и обществом, о поддержании «обратной связи», позволяющей учитывать восприятие новых технологий при принятии политических решений. В случае низкого уровня доверия власти технически невозможная «открытость» алгоритмов управления данными о голосовании может стать основанием для снижения легитимности всей электоральной процедуры (например, на основании теоретически возможных воздействий на процесс шифрования политических предпочтений). В этом случае применение более совершенных, чем «бумажное» голосование, решений на основе блокчейн может иметь деструктивные политические эффекты.

[4] Деятельность ГосСОПКА регулируется Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

СПИСОК ИСТОЧНИКОВ

1. Матренина К.Ю. Электронное голосование: понятие и виды. *Государство и право*. 2015(2):120–123. Matrenina K. Yu. Electronic voting: the concept and types. *State and Law.* 2015;(2):120–123.
2. Fedorov V. Presidential Elections in Russia 2018 and Electronic Voting. 2020. URL: https://www.researchgate.net/publication/346259619_Presidential_Elections_in_Russia_2018_and_Electronic_Voting.
3. Киселев В.О. Доверие к политическим институтам в России: опыт социологического мониторинга. Мониторинг. URL: https://cyberleninka.ru/article/n/doverie-k-politicheskim-institutam-v-rossii-opyt-sotsiologicheskogo-monitoringa.

Kiselev V. O. Trust in political institutions in Russia: experience of sociological monitoring. *Monitoring*. 2014;6(124). URL: https://cyberleninka.ru/article/n/doverie-k-politicheskim-institutam-v-rossii-opyt-sotsiologicheskogo-monitoringa (accessed on 01.05.2021).
4. Li G., Hou Y. & Wu A. Fourth Industrial Revolution: Technological drivers, impacts and coping methods. *Chinese Geographical Science*. 2017;27(4):626–637.
5. Мухаметов Д.Р. Технологии big data в политических процессах: риски и ограничения. *Гуманитарные науки. Вестник Финансового университета.* 2019;9(6):143–149.
   Mukhametov D.R. Big Data technologies in political processes: risks and opportunities. Gumanitarnye Nauki. *Vestnik Finasovogo Universiteta = Humanities and Social Sciences. Bulletin of the Financial University.* 2019;9(6):143–149. (In Russ.).
6. Стопинге В. Криптография и защита сетей. Принципы и практика. М.: Вильямс; 2001. 672 с.
   Stopinge V. Cryptography and network protection. Principles and practice. Moscow: Williams; 2001. 672 p. (In Russ.).
7. Чурова В.И., ред. КОИБ: история создания и применения: сб. материалов. М.: ЦИК Российской Федерации; 2014. (In Russ.).
   Churov V.I., ed. KOIB: history of creation and application: collection of materials, Moscow, 2014. (In Russ.).
8. Nurmi H., Salomaa A. Conducting secret ballot elections in computer networks: Problems and solutions. *Ann Oper Res.* 1994:(51):185–194. URL: https://doi.org/10.1007/BF02032763.

REFERENCES

1. Matrenina K. Yu. Electronic voting: the concept and types. *Gosudarstvo i pravo*. 2015(2):120–123. (In Russ.).
2. Fedorov V. Presidential Elections in Russia 2018 and Electronic Voting. 2020. URL: https://www.researchgate.net/publication/346259619_Presidential_Elections_in_Russia_2018_and_Electronic_Voting.
3. Kiselev V. O. Trust in political institutions in Russia: experience of sociological monitoring. 2014. URL: https://cyberleninka.ru/article/n/doverie-k-politicheskim-institutam-v-rossii-opyt-sotsiologicheskogo-monitoringa. (In Russ.).
4. Li G., Hou Y., Wu A. Fourth Industrial Revolution: Technological drivers, impacts and coping methods. *Chinese Geographical Science*. 2017;27(4):626–637.
5. Mukhametov D.R. Big Data technologies in political processes: risks and opportunities. *Gumanitarnye Nauki. Vestnik Finasovogo Universiteta = Humanities and Social Sciences. Bulletin of the Financial University*. 2019;9(6):143–149. (In Russ.).
6. Stopinge V. Cryptography and network protection. Principles and practice. Moscow: Williams; 2001. 672 p. (In Russ.).
7. Churov V.I., ed. KOIB: history of creation and application: a collection of materials. Moscow; 2014. (In Russ.).
8. Nurmi H., Salomaa A. Conducting secret ballot elections in computer networks: Problems and solutions. *Ann Oper Res.* 1994:(51):185–194. URL: https://doi.org/10.1007/BF02032763.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Оксана Валерьевна Ерохина — кандидат политических наук, доцент Департамента политологии и массовых коммуникаций, Финансовый университет, Москва, Россия
o.v.erokhina@gmail.com

ABOUT THE AUTHOR

Oksana V. Erokhina — Cand. Sci. (Political Science), Associate Professor, Financial University, Moscow, Russia
o.v.erokhina@gmail.com

Статья поступила 10.04.2021; принята к публикации 30.04.2021.
Автор прочитала и одобрила окончательный вариант рукописи.
The article received on 10.04.2021; accepted for publication on 30.04.2021.
The author read and approved the final version of the manuscript.