АКТУАЛЬНЫЕ ВОПРОСЫ УПРАВЛЕНИЯ

УДК 324

DOI 10.26425/1816-4277-2019-11-5-11

Ерохина Оксана Валерьевна
Научный сотрудник, Центр изучения трансформации общественно-политических отношений Финансового университета при Правительстве Российской Федерации, г. Москва, Российская Федерация
ORCID: *0000-0002-5453-4118*
e-mail: *o.v.erokhina@gmail.com*

ТЕХНОЛОГИИ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ В РОССИИ

Аннотация. *Следуя общемировой тенденции, связанной с применением цифровых технологий в политическом процессе, в России активно внедряют технологии электронного голосования. Их применение обеспечивает ряд преимуществ в организации и проведении выборов, но также сопровождается рисками, которые требуют дополнительного изучения. Важным положительным эффектом внедрения интернет-технологий выступает повышение информированности граждан о выборах и их участниках, а также сокращение финансовых расходов на проведение голосования и быстрая обработка его результатов. Основные риски применения технологий электронного голосования связаны с угрозами снижения легитимности выборов и проблемами защиты информации: абсолютную конфиденциальность персональных данных в рамках цифровых избирательных технологий обеспечить невозможно, что непосредственно связано с техническими особенностями электронного голосования.*

Ключевые слова: *цифровые технологии, электронное голосование, выборы, блокчейн, тайна голосования, защита информации.*

Цитирование: Ерохина О.В. Технологии электронного голосования в России//Вестник университета. 2019. № 11. С 5-11.

Erokhina Oksana
Research assistant, Centre for the Study of the Transformation of Social and Political Relations of the Financial University under the Government of the Russian Federation, Moscow, Russia
ORCID: *0000-0002-5453-4118*
e-mail: *o.v.erokhina@gmail.com*

ELECTRONIC VOTING TECHNOLOGIES IN RUSSIA

Abstract. *Following the global trend related to the use of digital technologies in the political process, Russia is actively introducing electronic voting technologies. Their application provides a number of advantages in the organization and conduct of elections, but also comes with risks, that require further study. An important positive effect of the introduction of Internet technologies is to increase the awareness of citizens about the elections and their participants, as well as to reduce the financial costs of voting and fast processing of its results. The main risks of the use of electronic voting technologies are associated with threats to reduce the legitimacy of elections and problems of information protection: absolute confidentiality of personal data in the framework of digital election technologies cannot be ensured, which is directly related to the technical features of electronic voting.*

Keywords: *digital technologies, electronic voting, elections, blockchain, secrecy of voting, information protection.*

For citation: Erokhina O.V. Electronic voting technologies in Russia (2019) Vestnik universiteta, I. 11, pp. 5-11. doi: 10.26425/1816-4277-2019-11-5-11

Внедрение информационных технологий в политические процессы происходит стремительно: расширяется перечень технических средств и программного обеспечения для проведения различных видов электронного голосования, активно обсуждаются возможности внедрения новых «умных» сервисов, связанных с предоставлением гражданам более качественных и разнообразных государственных услуг, в том числе связанных

Благодарности. Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финансовому университету при Правительстве РФ.

Acknowledgements. The article has been prepared on the results of research, carried out at the expense of budgetary funds on the state assignment to the Financial University under the Government of the Russian Federation.

с реализацией политических прав. В этом контексте особую актуальность приобретает вопрос о перспективе применения в России технологий электронного голосования.

В статье проводится анализ практики применения цифровых технологий в российском избирательном процессе, выявляются преимущества новых решений и издержки их применения, ставится вопрос о необходимости взвешенного подхода к внедрению популярной в настоящее время технологии блокчейн, намечаются перспективы для дальнейших исследований в области обеспечения защиты информации в ходе использования электронных технологий в политическом процессе.

Понятие электронного голосования в общем виде определяет процедуру волеизъявления избирателей, подсчета голосов и подведения итогов голосования с помощью специальных электронных технических средств [1]. Технологии проведения электронного голосования различны, однако их можно классифицировать по принципу взаимодействия избирателей со специальными техническими средствами: дистанционное голосование не предполагает личного присутствия граждан в определенном месте использования новых технологий, тогда как стационарное голосование связано с необходимостью посещать оборудованные необходимым программным обеспечением места. На практике дистанционное голосование проводилось в трех избирательных округах Москвы на выборах 8 сентября 2019 г., примером же стационарного электронного голосования выступает многолетнее применение Государственной автоматизированной системы Российской Федерации «Выборы» (далее – ГАС «Выборы») на федеральном и региональном уровнях. С нормативной точки зрения именно использование этой системы выступает одной из гарантий реализации прав граждан Российской Федерации (далее – РФ) посредством обеспечения гласности, достоверности, оперативности и полноты информации о выборах и референдуме, тогда как дистанционное электронное голосование на данном этапе носит лишь экспериментальный характер [2].

Изначально основной задачей ГАС «Выборы» была автоматизация процесса подсчета голосов, и ее решение происходило в несколько этапов. Первые сканеры избирательных бюллетеней были созданы еще в 1996 г., однако широкое применение получили позднее их усовершенствованные модели. До 2003 г. (появление первых комплексов обработки избирательных бюллетеней (далее – КОИБ)), автоматизация не затрагивала «низовой» уровень участковых избирательных комиссий, где бюллетени по-прежнему подсчитывали вручную, а на уровне территориальных комиссий полученные результаты загружались в автоматизированную систему и передавались далее в избирательные комиссии вышестоящих уровней. Таким образом, на уровне участковых избирательных комиссий сохранялась техническая возможность «вброса» бюллетеней, и оппозиционные кандидаты не раз сообщали о подобных фактах (далеко не всегда подтверждаемых проверками). В КОИБ процесс подсчета бюллетеней автоматизирован, как и учет волеизъявления избирателей: благодаря технологии оптического сканирования и распознавания комплекс «считывает» проставленные избирателями знаки в бюллетенях [5]. По мере распространения КОИБ процесс голосования был в большей степени автоматизирован: начиная с 2010 г. значительная часть избирательных участков по всей территории РФ была оснащена новыми сканерами, а также системами видеонаблюдения. В 2011 г. начался последний к настоящему времени этап технической модернизации избирательной системы РФ, результатом которой стало введение в эксплуатацию усовершенствованных моделей КОИБ и комплексов электронного голосования (далее – КЭГ), предполагающих использование специальных карт и сенсорной технологии [3]. КЭГ включают сенсорный экран, микроконтроллеры и специальные файлы данных.

С технологической точки зрения именно КЭГ соответствуют критериям стационарного электронного голосования, так как КОИБ лишь обрабатывают бумажные бюллетени автоматическим образом (технологии оптического сканирования и распознавания). КЭГ выполняют подсчет голосов, поданных с помощью сенсорных карт и специальных кодов доступа, и не имеют ни функций компьютера (операционной системы), ни доступа к сети «Интернет» (далее – Интернет), при этом сетевой контроллер собирает информацию со всех подключенных к КЭГ устройств для голосования и управляет создаваемой базой данных. КЭГ предусматривают возможность распечатать итоговые результаты, голосования, а проверка соотношения числа выданных бюллетеней с числом зарегистрированных/пришедших на участки избирателей производится после ввода дополнительных показателей в ручном режиме (в КОИБ встроена эта функция).

Основным преимуществом использования КОИБ является сокращение времени на обработку результатов голосования за счет автоматизации (протокол избирательной комиссии может быть распечатан с подключенного к автоматизированной системе принтера) и то, что при его использовании вероятность искажения

результатов выборов значительно снижается благодаря устранению человеческого фактора. Интересно отметить, что в случае необходимости по решению комиссии может быть осуществлен ручной пересчет голосов для перепроверки данных КОИБ, однако на практике это происходит редко [4]. Еще одна важная функция автоматизированной системы связана с созданием, поддержанием и актуализацией базы данных об избирателях, а также с обеспечением обмена информацией между избирательными комиссиями разных уровней. Наконец, нужно отметить расширение возможностей для участия в голосовании лиц с ограниченными возможностями здоровья: предусмотрен аудиосервис для слабовидящих и иные специальные возможности, облегчающие реализацию избирательных прав этой категории граждан.

Внедрение ГАС «Выборы» изначально было направлено на повышение «прозрачности» электорального процесса и, как следствие, уровня доверия избирателей к процедуре голосования и ее потенциальным результатам. Руководство Центральной избирательной комиссии Российской Федерации (далее – ЦИК России) уже признало эту цель достигнутой, отмечая, что факты расхождения результатов ручного и автоматизированного подсчета голосов единичны [8, с. 6]. Подобная позиция политически закономерна и выражает лояльность руководству государства, тем более что именно президент и правительство изначально выступали инициаторами цифровых преобразований как в экономике и государственном управлении, так и в организации избирательного процесса. Однако с точки зрения технологии обработки информации выявляются риски безопасности, что позволяет говорить об уязвимости ГАС «Выборы» и отсутствии гарантий достоверности обрабатываемой системой информации.

Будучи масштабной, замкнутой и при этом автономной системой, ГАС «Выборы» достаточно хорошо защищена от внешних воздействий: принцип действия КОИБ исключает возможность «вбрасывания» бюллетеней, а отсутствие интернет-подключений в КОИБ и КЭГ само по себе является лучшей защитой от хакерских атак. Однако нужно учитывать, что КОИБ, в отличие от КЭГ, не обеспечивает эффективной системы идентификации избирателей и не исключает возможности применения широко известной технологии «карусели», предполагающей противоречащее закону неоднократное голосование одних и тех же лиц. Еще более важно то, что применение ГАС «Выборы» сокращает, но не исключает негативное действие человеческого фактора. Архитектура ГАС «Выборы» включает три иерархически расположенных уровня: (нижний – уровень территориальных избирательных комиссий, средний – уровень избирательных комиссий субъектов РФ, высший уровень – ЦИК России), но не включает подчиняющиеся территориальным избирательным комиссиям участковые избирательные комиссии, которые с помощью автоматизированных средств собирают данные о результатах голосования на местах. Далее информация передается через программно-аппаратные комплексы, которые функционируют на каждом из описанных уровней ГАС «Выборы» и образуют сеть с использованием государственных и частных каналов связи. Протоколы участковых избирательных комиссий переносятся в базу данных системным администратором, что не исключает возможности искажения информации.

Таким образом, анализ технологий стационарного электронного голосования на примере ГАС «Выборы» показывает, что вероятность действия человеческого фактора, который может негативно повлиять на «прозрачность» традиционной процедуры голосования и достоверность ее результатов, значительно уменьшается, но не исчезает. Описанная система замкнута, изолирована от сетей общего доступа, однако администрируется из единого центра, а значит, полноценной защиты информации обеспечить не может. В этом контексте дистанционные технологии электронного голосования выглядят, на первый взгляд, более совершенно. Однако при ближайшем рассмотрении в процессе их использования выявляются те же угрозы информационной безопасности.

Эксперимент по проведению дистанционного электронного голосования 8 сентября 2019 г. прошел в трех избирательных округах Москвы (№ 1, № 10 и № 30) и предоставил возможность электоральной поддержки кандидатов через Интернет более чем 11,2 тыс. избирателей, большая часть из которых ею воспользовалась (явка составила 92,3 %, что значительно выше средней по городу). Таким образом, одна из важных политических задач властей была решена: мэрия столицы во главе с Сергеем Собяниным позиционирует Москву как наиболее быстро развивающееся пространство для внедрения умных технологий в сфере госуслуг, социальных сервисов, местного самоуправления и обеспечения политических прав граждан. Однако, важно заметить терминологическую неточность, допущенную при PR-продвижении новой технологии голосования: представители правительства Москвы неоднократно называли процедуру электронного голосования блокчейном, подчеркивая ее высокую надежность и невозможность искажения данных, однако в действительности

применяемая технология к решениям в указанной области не относится. Вероятно, неточность в терминологии в данном случае обусловлена стремлением руководства Москвы «встроиться» в одно из ключевых направлений политической повестки, связанное с развитием цифровых технологий. Возможности применения решений в области блокчейна активно изучают различные органы власти в рамках реализации национальной программы «Цифровая экономика», однако их применение далеко не всегда выглядит целесообразным [6].

Рассмотрим важнейшие технологические новации, примененные в ходе проведения дистанционного электронного голосования в Москве. Начало применению электронных форм голосования было положено в 2014 г., когда правительство Москвы в лице Департамента информационных технологий представило проект «Активный гражданин» – интернет-площадку для проведения референдумов по актуальным вопросам городского управления. По официальным данным, в 2017 г. в рамках реализации этого проекта начали применять технологию блокчейн, то есть создание распределенного реестра данных [12].

Основное преимущество технологии блокчейн, которое стремится использовать руководство Москвы, состоит в возможности формирования единого источника достоверной информации о гражданах и их запросах/предпочтениях в сфере городского управления (в случае с проектом «Активный гражданин»), а также о ходе политических процессов, в том числе голосования (в случае с экспериментом по проведению «электронных» выборов 8 сентября 2019 г.). Речь идет о формировании базы данных, которая может быть использована в самых широких сферах государственного управления, в процессе взаимодействия органов власти между собой и с общественными организациями, при этом информация должна оперативно собираться и обновляться, а изменения должны быть защищены как от неправомерного изменения, так и от несанкционированного доступа. Сказанное обусловливает повышенный интерес к решениям на основе блокчейна со стороны общественных организаций: одним из ожидаемых положительных эффектов от применения этой технологии выступает повышение эффективности управления и снижение уровня коррупции.

При проведении электронного голосования преимуществом технологии блокчейн считается высокая степень защищенности данных, а значит, обеспечение нового, более высокого уровня «честности» и «прозрачности» избирательного процесса, большее соответствие теоретическим представлениям о демократии [7]. Действительно, внутри цепочки транзакций информация, например, о результатах голосования, остается неизменной, однако механизм идентификации пользователей вызывает сомнения с точки зрения гарантий важнейшего принципа волеизъявления – тайны голосования. С нормативной точки зрения несоблюдение этого принципа ставит под сомнение проведение выборов и не только легитимность, но и легальность их результатов, так как принцип тайного голосования входит в число конституционных гарантий (ч. 1 ст. 81 Конституции РФ) [9]. В этом контексте вновь возникает вопрос о целесообразности применения технологии блокчейн в политической сфере, особенно в государственном масштабе.

Стоит обратить внимание на то, что технология, предлагаемая при развитии проекта «Активный гражданин», не содержит механизма защиты от манипуляций со стороны внешнего источника, например, от создания дублирующих аккаунтов для голосования. Закономерно, что вопрос обеспечения защиты информации стал одним из ключевых при подготовке эксперимента по проведению дистанционного электронного голосования на выборах в Москве. Так, использовалась новая программа обеспечения тайны голосования – анонимизатор [11]. Основной смысл ее запуска состоял в том, чтобы создать автономную систему, не контролируемую Правительством Москвы и, в частности, его «профильным» подразделением в лице Департамента информационных технологий города Москвы. Анонимизатор обезличивает данные о голосовании и включает несколько систем их шифрования, что теоретически обеспечивает и тайну голосования, и защиту данных от искажения. Личный кабинет пользователя «привязан» к номеру телефона, что позволяет идентифицировать избирателя и предотвратить повторное голосование, однако говорить о полной анонимности не приходится (аналогично ГАС «Выборы», при использовании которой человек регистрируется на участке с помощью паспортных данных). Защита информации и в этом случае односторонняя: будучи независимой от органов исполнительной власти, система администрируется специалистами Московской городской избирательной комиссии, а значит, полностью защищенной от вмешательства не является. Речь идет лишь об отсутствии теоретической возможности для влияния на процедуру выборов со стороны Департамента информационных технологий Москвы. При этом изначально предполагалась возможность контроля за ходом голосования со стороны общественных организаций, которым передавались бы данные для защиты информации (разделенный на части ключ-пароль).

Введение многоступенчатой системы шифрования способно обеспечить конфиденциальность передаваемой в ходе электронного голосования информации на промежуточных этапах (до подведения итогов), хотя нужно обратить внимание на то, что даже в теории наличие нескольких шифров не повышает общий уровень защищенности системы по сравнению с использованием однократного шифрования. Тем не менее, при наличии одного центра администрирования системы техническая возможность влияния на результаты голосования сохраняется и обеспечить абсолютную неуязвимость системы электронного голосования технически не представляется возможным. Кроме того, любая связанная с интернет-технологиями система потенциально уязвима для целенаправленных негативных воздействий, для распределенных сетевых атак (DDoS-атаки) и иных проявлений хакерства. В случае с электронным голосованием взлом, приводящий даже к кратковременному сбою, может существенно исказить итоги голосования.

Преодолеть уязвимость информационных систем, предполагающих администрирование из единого центра, призвано использование технологии блокчейн. Под блокчейном понимают выстроенную по определенным правилам непрерывную последовательную цепочку информационных блоков (транзакций), связь между которыми и безопасность цепочки в целом обеспечивается криптографическими средствами, а именно применением хэш-функции и криптографической подписи [10]. В отличие от большинства технологий интернет-голосования, которые лишь частично поддаются верификации со стороны независимого внешнего источника, создание распределенной базы данных без подключения к общему серверу обеспечивает прозрачность и контроль транзакций со стороны участников системы. Однако на первый план выходит проблема использования алгоритмов шифрования данных, обеспечивающих безопасность и конфиденциальность данных. Помимо несовершенства законодательной базы, нужно учесть, что применение иностранных протоколов шифрования в РФ невозможно, так как они не сертифицированы соответствующими специальными службами, а разработка собственных систем шифрования направлена, преимущественно, на решение задач государственной безопасности и сохранения государственной тайны, и применение их в процессе обеспечения электронного голосования в обозримом будущем не соответствует приоритетам силовых структур. В связи с этим полноценное применение технологии блокчейн для проведения электронного голосования в РФ выглядит сомнительно.

Анализ современного опыта электронного голосования показывает, что применение новых технологических решений способно значительно сократить издержки, однако зачастую требует законодательных изменений в сфере гарантий основных избирательных прав граждан, а также имеет существенные ограничения, затрагивающие проблемы информационной безопасности. Основные преимущества электронного голосования можно обобщить следующим образом: упрощение процедуры и более привлекательные решения для избирателя, а значит, больше возможностей для роста участия; новое качество информирования избирателей и, как следствие, повышение «прозрачности» избирательного процесса, снижение бюджетных расходов на организацию и проведение голосования и, как следствие, рост эффективности управления государственными финансами. Недостатки или потенциальные издержки технологий электронного голосования связаны с возникающим «цифровым неравенством» граждан, то есть неравномерностью доступа к современным технологиям передачи и хранения информации, угрозами легитимности принимаемых в ходе прямого голосования решений, недостаточным доверием избирателей к электронным формам демократии, возможностью нарушения тайны голосования и проблемами идентификации участников цифрового избирательного процесса.

Библиографический список

1. Федеральный закон «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» от 12.06.2002 № 67-ФЗ (ред. от 29.05.2019) // СПС «Консультант Плюс» [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_37119 (дата обращения: 20.09.2019).
2. Федеральный закон «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва» от 29.05.2019 № 103-ФЗ // СПС «Консультант Плюс» [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_325552 (дата обращения: 20.09.2019).
3. Федеральный закон «О проведении эксперимента по голосованию на цифровых избирательных участках, образованных в городе федерального значения Москве, на дополнительных выборах депутатов Государственной Думы Федерального

Собрания Российской Федерации седьмого созыва и выборах высших должностных лиц субъектов Российской Федерации (руководителей высших исполнительных органов государственной власти субъектов Российской Федерации), проводимых 8 сентября 2019 года» от 29.05.2019 № 102-ФЗ // СПС «Консультант Плюс» [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_ 325553 (дата обращения: 20.09.2019).

4. Постановление о завершении Программы ускоренного технического переоснащения избирательной системы Российской Федерации, утвержденной постановлением Центральной избирательной комиссии Российской Федерации «О новой редакции Программы ускоренного технического переоснащения избирательной системы Российской Федерации» от 22 ноября 2013 года № 205/1378-6 [Электронный ресурс]. – Режим доступа: http://www.cikrf.ru/activity/docs/postanovleniya/27797/ (дата обращения: 20.09.2019).
5. Инструкция о порядке использования комплексов обработки избирательных бюллетеней на выборах и референдумах, проводимых на территории Российской Федерации [Электронный ресурс]. – Режим доступа: http://www.cikrf.ru/upload/decree-of-cec/31-218-5-pril.php (дата обращения: 20.09.2019).
6. Программа «Цифровая экономика». Утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р [Электронный ресурс]. – Режим доступа: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения: 20.09.2019).
7. Даль, Р. (2000) О демократии / Пер. с англ. А. С. Богдановского. – М.: Аспект Пресс, 2000. – 204 с.
8. КОИБ: история создания и применения: сб. материалов / Под общ. ред. В. Е. Чурова, В. А. Крюкова. – М.: Центральная избирательная комиссия Российской Федерации, 2014. – 176 с.
9. Матренина, К. Ю. (2014) Принцип тайного голосования при использовании современных информационных технологий// Вестник Тюменского государственного унверситета. – 2014. – № 3. – С. 206-211.
10. Панков, К. Н. (2018) Использование криптографических средств для сквозных цифровых технологий на примере систем распределенного реестра // Технологии информационного общества: материалы XII Международной отраслевой научно-технической конференции. Москва, 14-15 марта 2018 г. – М.: Издательский дом Медиа паблишер, 2018. – С. 365-366.
11. Ключ шифрования и анонимизатор: как защитят результаты электронного голосования [Электронный ресурс]. – Режим доступа: https://www.mos.ru/news/item/58384073/ (дата обращения: 20.09.2019).
12. Технология блокчейна сделает проект «Активный гражданин» более открытым [Электронный ресурс]. – Режим доступа: https://www.mos.ru/news/item/33560073/ (дата обращения: 20.09.2019).

References

1. Federal`nyi zakon (red. ot 29.05.2019) “Ob osnovnykh garantiyakh izbiratel`nykh prav i prava na uchastie v referendume grazhdan Rossiiskoi Federatsi” ot 12.06.2002 № 67-FZ [*Federal Law* “*On the basic guarantees of electoral rights and the right to participate in the referendum of citizens of the Russian Federation*” *dated June 12, 2002 № 67-FZ*], SPS “Konsultant Plyus” [*Legal reference system* “*Consultant Plus*”]. Available at: https://www.consultant.ru/document/cons_doc_LAW_37119 (accessed 20.09.2019).
2. Federal`nyi zakon “O provedenii eksperimenta po organizatsii i osushchestvleniyu distantsionnogo elektronnogo golosovaniya na vyborakh deputatov Moskovskoi gorodskoi Dumy sed`mogo sozyva” ot 29.05.2019 № 103-FZ [*Federal Law of May 29, 2019 “On carrying out experiment on the organization and implementation of remote electronic voting at elections of deputies of the Moscow City Duma of the Seventh Convocation*], SPS “Konsultant Plyus” [*Legal reference system* “*Consultant Plus*”]. Available at: https://www.consultant.ru/document/cons_doc_LAW_ 325552 (accessed 20.09.2019).
3. Federal`nyi zakon “O provedenii eksperimenta po golosovaniyu na tsifrovykh izbiratel`nykh uchastkakh, obrazovannykh v gorode federal`nogo znacheniya Moskve, na dopolnitel`nykh vyborakh deputatov Gosudarstvennoi Dumy Federal`nogo Sobraniya Rossiiskoi Federatsii sed`mogo sozyva i vyborakh vysshikh dolzhnostnykh lits sub``ektov Rossiiskoi Federatsii (rukovoditelei vysshikh ispolnitel`nykh organov gosudarstvennoi vlasti Rossiiskoi Federatsii), provodimykh 8 sentyabrya 2019 goda” ot 29.05.2019 № 102-FZ [*Federal Law “On carrying out experiment on voting at the digital polling stations formed in the City of Federal Value Moscow, on additional elections of deputies of the State Duma of Federal Assembly of the Russian Federation of the Seventh Convocation and elections of the highest officials of Subjects of the Russian Federation (heads of the highest Executive bodies of the State Power of Subjects of the Russian Federation) held on September 8, 2019” dated May 29, 2019 №102-FZ*], SPS “Konsultant Plyus” [*Legal reference system* “*Consultant Plus*”]. Available at: https://www.consultant.ru/document/cons_doc_LAW_ 325553 (accessed: 20.09.2019).
4. Postanovlenie o zavershenii Programmy uskorennogo tekhnicheskogo pereosnashcheniya izbiratel`noi sistemy Rossiiskoi Federatsii, utverzhdennoi postanovleniem Tsentral`noi Izbiratel`noi Komissii Rossiiskoi Federatsii ot 22.11.2013 g. № 205/1378-6 “O novoi redaktsii Programmy uskorennogo tekhnicheskogo pereosnashcheniya izbiratel`noi sistemy Rossiiskoi Federatsii”

[*Resolution resolution on completion of the Program of the accelerated technical re-equipment of the electoral system of the Russian Federation, approved by decision of the Central Election Commission of the Russian Federation dated November 22, 2013 № 205/1378-6 "On new edition of the Program for accelerating the technological re-equipment of the electoral system of the Russian Federation"*]. Available at: http://www.cikrf.ru/activity/docs/postanovleniya/27797/ (accessed 20.09.2019).

5. Instruktsiya o poryadke ispol`zovaniya kompleksov obrabotki izbiratel`nykh byulletenei na vyborakh i referendumakh, provodimykh na territorii Rossiiskoi Federatsii [*Regulation on the procedure for the use of voting papers processing complexes in elections and referendums held in the territory of the Russian Federation*]. Available at: http://www.cikrf.ru/upload/decree-of-cec/31-218-5-pril.php (accessed 20.09.2019).
6. Programma "Tsifrovaya Ekonomika". Utverzhdena rasporyazheniem Pravitel`stva Rossiiskoi Federatsii ot 28 iyulya 2017 g. № 1632-r [*Program "Digital economy" Was approved by the Order of the Government of the Russian Federation dated July 28, 2017 № 1632-r*]. Available at: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (accessed 20.09.2019).
7. Dahl R. O demokratii [*About democracy*], Per. s angl. A. S. Bogdanovskogo, Moscow, Aspekt Press, 2000, 204 p.
8. KOIB: istoriya sozdania i primenenia: sb. materialov [*KOIB: the story of creation and application: collection of materials*], Pod obsh. red. V. E. Churova, B. A. Krykova, Moscow, Tsentral'naya izbiratel'naya komissiya Rossiiskoi Rederatsii, 2014, 176 p.
9. Matrenina K.Yu. Printsip tainogo golosovania pri ispolzovanii sovremennykh informatsionnykh tekhnologii [*The principle of secret voting in the use of modern information technologies*], Vestnik Tyumenskogo gosudarstvennogo universiteta [*Tyumen State University Herald*], 2014, I. 3, pp. 206-211.
10. Pankov K. N. Ispol`zovanie kriptograficheskikh sredstv dlya skvoznykh tsifrovykh tekhnologii na primere system raspredelennogo reestra [*Using of cryptographic tools for end-to-end digital technologies on the example of distributed registry systems*], Tekhnologii informatsionnogo obshchestva: materialy XII Mezdunarodnoi otraslevoi nauchno-tekhnicheskoi konferentsii, Moskva, 14-15 marta 2018 g. [*Collection of Articles. Information Society Technologies. Proceedings of XII International Branch Scientific and Technical Conference, Moscow, March 14-15, 2018*], Moscow, Izdatel'skii dom Media publisher, 2018, pp. 365-366.
11. Kluch shifrovania i anonimizator: kak zashchityat rezultaty elektronnogo golosovania [*Encryption key and anonymizer: how to protect the results of electronic voting*]. Available at: https://www.mos.ru/news/item/58384073/ / (accessed 20.09.2019).
12. Tekhnologiya blokcheina sdelaet proekt "Aktivnyi grazhdanin" bolee otkrytym [*Blockchain technology will make project "Active citizen" more open*]. Available at: https://www.mos.ru/news/item/33560073/ (accessed: 20.09.2019).