

Научная статья
УДК 342.8
doi: 10.17223/15617793/518/23

Дистанционное электронное голосование (ДЭГ): актуальные проблемы доверия и перспективы развития

Елена Александровна Масуфранова¹, Никита Сергеевич Дубровский²,
Константин Геннадьевич Балашов³

¹ Юго-Западный государственный университет, Курск, Россия, a25021985@yandex.ru

² Управление Министерства юстиции Российской Федерации по Курской области, Курск, Россия, KeIIIycTuk@yandex.ru

³ Адвокатская контора Красноперкопского района г. Ярославля (Ярославская областная коллегия адвокатов),
Ярославль, Россия, balashoffkonstantin@yandex.ru

Аннотация. Революционные технологические достижения неизбежно вплетаются во всевозможные общественные отношения. Информационные технологии оказали беспрецедентное влияние на избирательные правоотношения, благодаря которым и появился институт дистанционного электронного голосования (ДЭГ). Авторами проводится подробный анализ особенностей ДЭГ, уровня доверия граждан к нему, а также анализируются история и практика его применения. По результатам работы авторами формулируется обоснованный вывод, способный оказать благоприятное влияние на правоприменительную практику ДЭГ.

Ключевые слова: дистанционное электронное голосование, выборы, голосование, доверие, явка, избирательное право, технологии

Для цитирования: Масуфранова Е.А., Дубровский Н.С., Балашов К.Г. Дистанционное электронное голосование (ДЭГ): актуальные проблемы доверия и перспективы развития // Вестник Томского государственного университета. 2025. № 518. С. 202–210. doi: 10.17223/15617793/518/23

Original article
doi: 10.17223/15617793/518/23

Remote electronic voting (REV): Problems of trust and prospects for development

Elena A. Masufranov¹, Nikita S. Dubrovsky², Konstantin G. Balashov³

¹ Southwest State University, Kursk, Russian Federation, a25021985@yandex.ru

² Administration of the Ministry of Justice of the Russian Federation for Kursk Oblast, Kursk, Russian Federation, KeIIIycTuk@yandex.ru

³ Law Office of Krasnoperekopsky District of Yaroslavl, Yaroslavl, Russian Federation, balashoffkonstantin@yandex.ru

Abstract. A key focus of this research is examining the need to enhance public trust in the use of the Remote Electronic Voting (REV) system. It is noteworthy that, to date, most constituent entities of the Russian Federation are characterized by low voter turnout in government elections. At the same time, it must be acknowledged that the number of citizens voting via the REV system has increased with each electoral campaign, despite calls from some political forces to abandon this modern remote voting method. Clearly, the use of remote voting today represents the most convenient and straightforward electoral procedure. However, unfortunately, not all members of the electorate are fully informed about the modern capabilities and methods available for casting their vote "from the comfort of their own home." Consequently, the aim of this study is to identify current issues of trust in REV within the context of applying blockchain technology, and to find ways to overcome them. To achieve this aim, the authors have set the following objectives: (1) to identify the conceptual problems of REV as an element of the modern information and telecommunication environment of the Russian Federation; (2) to analyze the overall experience with remote electronic voting in the Russian Federation; (3) to test the research through sociological surveys within the stated research directions; (4) to determine current solutions and identify viable opportunities for overcoming the problem of trust in REV within the framework of applying blockchain technology. In preparing this research, the authors employed methods of observation, comparison, analysis, synthesis, deduction, as well as sociological survey. The object of the study is Remote Electronic Voting (REV). The focus of the study is on the problems of public trust in the institution of remote electronic voting within the context of applying blockchain technology and methods for increasing the level of trust in it. The main sources on which the research relies are: normative legal acts; normative acts containing clarifications of legislation; leading doctrinal positions on the issue under consideration; and current data from the latest sociological studies. In conclusion, the finding is formulated that REV is progressive; experiments with its use in the regions (in Moscow, Kursk, Yaroslavl, and Rostov oblasts) have, in most cases, shown a fairly high level of citizen interest. The conducted surveys confirm a gradual formation of trust in the system among the population. However, some problems were also identified, the qualitative resolution of which is the key to the effective development of remote electronic voting in the Russian Federation.

Keywords: remote electronic voting, elections, voting, trust, turnout, suffrage, technology

For citation: Masufranova, E.A., Dubrovsky, N.S. & Balashov, K.G. (2025) Remote electronic voting (REV): Problems of trust and prospects for development. *Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal*. 518. pp. 202–210. (In Russian). doi: 10.17223/15617793/518/23

Абсолютное большинство проводимых за последнее время публичных мероприятий, посвященных экономическим, социальным, технологическим вопросам, не проходят стороной тематику развития и внедрения технологии блокчейн. На сегодняшний день данный вопрос является краеугольным камнем не только у ведущих производственных площадок, бизнесменов и предприятий, но и у государств. Не безызвестно, что в Российской Федерации в течение длительного времени в ходе электоральных процессов активно применяется технология блокчейн.

Фундаментальными национальными стратегическими документами делается акцент на необходимости устойчивого развития российской инфраструктуры на новой технологической и информационной основах. В сегодняшних условиях с каждым днем все больше актуализируются вопросы, связанные с повсеместным внедрением новейших технологий во все сферы жизнедеятельности нашего общества. В современных условиях в эпицентре всеобщего внимания находятся возможности аппаратно-программных комплексов и различных систем, которые способны упростить не только профессиональную жизнедеятельность, но и способствовать улучшению организационных основ избирательных процессов.

Выступающими с высоких трибун все чаще констатируется, что современное общество переступило порог четвертой промышленной революции. Уже никого не удивить способностями голосовых помощников, возможностями умного дома, а также беспилотными автомобилями и летательными аппаратами. Безусловно, подобные технологии существенно упрощают нашу жизнь и делают ее более упрощенной и комфортной. Все современные государства стремятся максимально быстро и одновременно безопасно внедрять технологические достижения в правоприменительную деятельность. Практика применения технологии блокчейна на выборах разных уровней и ступеней власти в Российской Федерации позволяет констатировать, что дистанционное электронное голосование их год за год набирает популярность среди граждан.

Однозначно можно заключить, что внедряемые, в том числе в избирательные правоотношения, цифровые технологии порождают новые проблемы и риски, на решение и снижение которых должно быть сфокусировано акцентированное внимание государства. Под воздействием новых технологий зачастую меняется и сущность некоторых урегулированных нормами права общественных отношений. Данные тенденции вызывают к необходимости определения и изучения этих изменений, а также поиска оптимальных способов взаимодействия правовых норм и цифровых технологий. Это поможет решить проблему между правовым регулированием и современными цифровыми технологиями, которая проявляется в их разнонаправленном влиянии на общественные отношения и может иметь деструктивные последствия для общества в целом,

например, способствуя разрушению правового сознания. Хотя говорить о новых формах реализации права, связанных с цифровыми информационными технологиями, пока рано, в некоторых случаях они значительно изменяют традиционные формы, придавая им новые особенности и порождая новые правовые проблемы. К таким технологиям относятся, например, интеллектуальные программные агенты и смарт-контракты. Использование таких информационных технологий связано с фактической передачей части полномочий лица программным средствам, которые начинают действовать и имеют юридические последствия для этого лица независимо от его воли, а иногда и вопреки ей. И это лишь в очередной раз доказывает серьезность вопроса о правовой природе таких объектов и систем, а также о юридическом значении действий, осуществляемых с их использованием и применением.

Очевидно, что не только социальные потрясения и революции могут вызвать изменения в праве. Развитие информационных цифровых технологий в XXI веке уже привело к эволюции права, включая появление новых объектов, форм и способов реализации права. Сейчас многие ученые указывают на то, что право продолжает трансформироваться под влиянием цифровых технологий. Например, В.Н. Синюков считает, что «в России происходят фундаментальные изменения в правовой системе, которые можно охарактеризовать как процессы этапной трансформации» [1. С. 13]. Развитие новых технологий вытесняет традиционное правовое регулирование и опережает его методологически. Классические формы процессуальной деятельности становятся препятствиями для инноваций во многих областях. А.А. Карцхия подчеркивает, что «технологические платформы, такие как блокчейн, Интернет вещей, искусственный интеллект, облачные сервисы, аналитика больших данных и другие, создают новые условия и базу для изменения традиционных правовых институтов» [2. С. 43]. Так, О.В. Танимов указывает на «трансформацию права и правоотношений в условиях цифровизации, где появляются новые объекты и субъекты, а также изменяется содержание правоотношений, например, с появлением цифровых платформ» [3. С. 14]. Известные ученые Т.Я. Хабриева и Н.Н. Черногора считают, что «право не только является средством, обеспечивающим цифровизацию экономики и управления, но и становится объектом воздействия цифровизации, претерпевая изменения в форме, содержании, системе, структуре и механизмах действия» [4. С. 85]. И хотя эти изменения в правовой системе являются важными, они скорее относятся к эволюции права, вместо того чтобы быть революционными. Однако существуют предпосылки к трансформации права под влиянием цифровых технологий. Например, если основным источником права станет цифровой код, применяемый к общественным отношениям и обеспечиваемый правилами информационных систем, а не традиционными формами права и силой государства.

Конституция РФ определяет Россию как демократическое правовое государство и гарантирует гражданам право на участие в управлении государственными делами. Это право реализуется через другие конституционные права и свободы, включая право на избрание и быть избранным в органы государственной власти и местного самоуправления. В последние годы в политическом процессе и избирательной системе активно обсуждается тема цифровизации [5. С. 13]. Развитие электронных технологий для определения и учета мнений избирателей, включая процесс голосования, вызывает интерес к ретроспективному анализу мнений и объективной оценке перспектив и рисков. Федеральным законом «О внесении изменений в отдельные законодательные акты Российской Федерации» от 23.05.2020 года № 154-ФЗ в российский избирательный процесс было введено понятие «дистанционное электронное голосование», которое для федерального правоприменения стало весьма серьезным прорывным, открывающим возможность дистанционного электронного голосования на общегосударственном уровне, без использования бумажных бюллетеней, а с использованием специального программного обеспечения. Некоторые существенные преимущества такого голосования включают улучшение безопасности избирательных процессов, более оперативное проведение выборов и подсчет голосов, привлечение большего числа избирателей, особенно молодежи, и экономию ресурсов при большом охвате избирателей.

В контексте внедрения в правоприменительную деятельность возможностей информационно-телекоммуникационных инструментов возникает немало теоретических и практических вопросов. Стоит сказать о том, насколько важно, чтобы дистанционное электронное голосование соответствовало основным принципам избирательного права, таким как всеобщность, тайность и равенство.

Говоря о вышеуказанных принципах в контексте применения дистанционного электронного голосования, необходимо учитывать, что государство, внедряя данный институт в избирательный процесс, должно сформировать весомые гарантии того, что каждый гражданин, независимо от пола, возраста, имущественного и социального положения, должен иметь беспрепятственную возможность отдать свой голос с помощью электронных технологий. Стоит сказать, что принять участие в дистанционном электронном голосовании можно посредством персонального компьютера, смартфона или планшета. Однако, исходя из достоверных результатов социологических исследований, 15% россиян не имеют смартфоны. Кроме того, анализируя социологические исследования можно сделать вывод о том, что в некоторых регионах Российской Федерации, персональными компьютерами владеют менее половины семей, такая ситуация наблюдается, например, в Еврейской автономной области [6]. Приведенная статистика говорит о том, что если бы дистанционное электронное голосование было единственным способом участия в выборах, то невозможно было бы следовать соблюдению рассматриваемых принципов изби-

рательного процесса. Напротив, рассматриваемая статистика подтверждает тезис о том, что дистанционное электронное голосование как факультативный способ голосования идеально подходит для абсолютного большинства граждан нашей страны, которые являются активными пользователями Интернета с различных технических устройств. Таким образом, внедряя дистанционное электронное голосование, государство упрощает процедуру избирательного процесса, в целях создания большего удобства для граждан, при этом, не пренебрегая основными принципами избирательного процесса.

В сегодняшних условиях стремительного роста высокотехнологичных сфер жизнедеятельности зачастую правовое регулирование не успевает за этими процессами. Все достижения информатизации, цифровизации и компьютеризации направлены на создание более комфортных условий проживания людей. В этой связи уместным будет упомянуть про недавно созданный революционный вид денег – криптовалюта, функционирование которой, как и дистанционного электронного голосования, основано на блокчейне. Проводя аналогию с постепенным внедрением дистанционного электронного голосования, стоит сказать, что первые годы своего существования криптовалюта не вызвала доверия у большинства граждан. Сегодня же ситуация коренным образом поменялась: число инвесторов в криптовалюту в России растет с каждым годом. Так, в 2023 г. в Российской Федерации открыто более 13 миллионов кошельков – и это только те кошельки, создание и функционирование которых могут наблюдать государственные органы посредством централизованных бирж [7]. Несмотря на возрастающую популярность криптовалют в настоящее время правовое регулирование данной сферы во многих странах, как и в Российской Федерации не системно и фрагментарно, что порождает большое количество правовых коллизий в правоприменительной практике. Стоит отметить, что в Российской Федерации на сегодняшний день также отсутствует специальное системное законодательство, направленное на регулирование общественных отношений, связанных с оборотом криптовалют.

В сфере электронного голосования разработаны схожие с криптовалютой соответствующие протоколы и алгоритмы. Кроме того, во многих государствах уже имеется успешный опыт внедрения дистанционного электронного голосования. Например, электронное голосование через Интернет используется в Швейцарии, Великобритании и Канаде [8. С. 22]. В Эстонии общенациональные выборы с использованием дистанционного голосования проводятся с 2005 г.

Успешность внедрения системы дистанционного электронного голосования зависит от ряда аспектов: повсеместности перехода на электронное голосование; возможности контроля результатов голосования; разнообразия форм доступа к информационной системе.

Для наглядного подтверждения актуальности первого аспекта достаточно обратить внимание на количество регионов Российской Федерации, в которых применяется дистанционное электронное голосование на

федеральной платформе дистанционного электронного голосования. По данным Центральной избирательной комиссии Российской Федерации в 2023 г. ДЭГ внедрено лишь в 24 регионах (Московская область, Республика Крым, Липецкая область, Курская область, Воронежская область, Республика Карелия, Алтайский край и т.д.) [9. С. 114]. Вместе с тем надо понимать, что именно повсеместное применение дистанционного электронного голосования, иначе говоря, охват всех субъектов, способен оказать влияние на качество его внедрения, так как рост числа проголосовавших с помощью платформы дистанционного электронного голосования позволяет выявить различные проблемы технического и организационного характера, которые могли оставаться вне поля зрения разработчиков и законодателя. Кроме того, представляется, что такое расширение в масштабах всего государства поспособствует более быстрому восприятию дистанционного электронного голосования гражданами и, соответственно, формированию у них положительного, доверительного отношения к нему, осознанию его преимуществ в сравнении с традиционным способом голосования на бумажном бюллетене. Вполне естественно, что не менее значимым фактором здесь выступает целенаправленная работа представителей избирательных комиссий всех уровней с населением, направленная на разъяснение механизмов дистанционного электронного голосования, ее преимуществ, особенностей, специфики защиты данных, возможности контроля за «прозрачностью» подсчета голосов и результатов голосования.

В подтверждение второго аспекта справедливым будет заметить, что всеми экспертами и специалистами активно пропагандируется основное преимущество дистанционного электронного голосования, заключающееся в том, что он функционирует на блокчейне. В общепотребительной терминологии блокчейн – это цепочка блоков данных, которая известна своей децентрализацией и функционированием исключительно по заданному программному коду. Стоит заметить, что в отличие от знакомых многим криптовалют (например Bitcoin или Ethereum), которые функционируют распределенно на децентрализованном блокчейне, в ДЭГ используется централизованный приватный блокчейн [10]. Возможность контроля подсчета голосов и результатов голосования – база для формирования доверительного отношения граждан к дистанционному электронному голосованию, и без него об эффективности внедрения и применения такого голосования невозможно и говорить. Этот контроль также можно назвать аудируемостью – независимой проверкой законности и корректности подведения итогов голосования.

В подтверждение же третьего аспекта целесообразным будет обратиться к демографической линии проблемы. Так, на выборах в 2023 г. средний возраст избирателя в системе дистанционного электронного голосования составил 35–50 лет. Это демографические категории населения, которые способны путем использования современных средств информационно-телекоммуникационной связи участвовать в дистанционном голосовании. Однако по данным Федеральной

службы государственной статистики Российской Федерации каждый четвертый житель страны – в пенсионном возрасте. Более того, в 71 субъекте Российской Федерации наблюдается превышение численности людей старшего возраста. В то же время, исходя из недавних социологических исследований Института статистических исследований и экономики знаний (ИСИЭЗ) НИУ ВШЭ, большинство россиян, не пользующихся Интернетом, – это люди старше 55 лет [11. С. 470]. Вдобавок ко всему приведенному, этим же исследованием было установлено, что в России год от года растет число населения, которое не желает подключаться к сети Интернет (данная проблема характерна, например, для республик Марий Эл и Мордовия). Таким образом, есть проблема, заключающаяся в том, что некоторые категории населения остаются непричастными к рассматриваемому способу голосования в силу различных объективных и субъективных причин.

Организация и проведение голосования граждан в электронной форме с использованием различных информационных технологий так или иначе связаны с определенными рисками. Одним из самых важных таких рисков является подверженность подобных информационных систем уязвимостям, связанным с необходимостью передавать трафик через Интернет. Использование информационных систем, которые не обеспечивают должного уровня безопасности данных и могут быть изменены извне техническими или другими способами, может вызвать сомнения в результате выборов и дискредитировать саму идею дистанционного электронного голосования в целом.

Такие процессы уже происходили в некоторых странах. Например, из-за сложностей с протоколами электронного голосования, потенциальными компьютерными ошибками и хакерскими атаками избирательные комиссии в Казахстане (2011) и Нидерландах (2008, 2017) вернулись к традиционным бумажным бюллетеням, урнам и ручному подсчету голосов [12. С. 48]. Аналогичные события произошли в США, где еще в 2004 г. была попытка создать высокотехнологичную систему Интернет-голосования. Однако система электронного голосования подверглась жесткой критике из-за обнаруженных уязвимостей в системе безопасности. В связи с этим на общегосударственном уровне в США вопросы внедрения и развития электронного голосования практически не рассматриваются, за исключением некоторых штатов, где продолжают эксперименты по этому вопросу.

Таким образом, можно сказать, что вопрос безопасности проведения дистанционного электронного голосования является весьма важным и актуальным на сегодняшний день. Однако интерес к дистанционному электронному голосованию не сможет возрасти, если граждане будут относиться с большим недоверием к ДЭГ [13. С. 30]. Стоит отметить, что недоверие граждан раскрывается в двух формах – объективной и субъективной. Объективная форма подразумевает, например, ситуации, при которых благодаря совокупности собственных знаний граждане имеют недостаточно правильное представление о пробелах в процедуре дистанционного электронного голосования.

Субъективная же форма предполагает, например, ситуации, когда гражданин скептически относится к любым общественным отношениям, которые так или иначе связаны с информационно-телекоммуникационной средой. Субъективная форма является, по мнению авторов, наиболее преобладающей в связи с тем, что число преступлений, совершенных дистанционными способами, то есть, как правило, с применением современных вычислительных средств, растет буквально в геометрической прогрессии. Так, из доклада Генерального прокурора Российской Федерации за 8 месяцев 2023 г. следует, что было совершено почти 230 тыс. дистанционных мошенничеств, а это на 40% выше показателей за аналогичный период прошлого года. Складывающаяся ситуация неизбежно формирует концептуальный неверный подход у отдельно взятого гражданина, считающего, что большая часть его личных персональных данных должным образом не охраняется государством, а информационные технологии в такой ситуации ничего хорошего преподнести не могут [14].

Результаты всевозможных социологических опросов, доступные для публичного обозрения, позволили выявить следующее: в целом граждане доверяют системе дистанционного электронного голосования, однако опасения вызывают возможность внешнего вмешательства в систему ДЭГ со стороны недружественных государств и хакерских атак. В связи с чем, нами было принято решение выявить основные проблемы, стоящие на пути доверия к дистанционному электронному голосованию, а также определить возможные пути их преодоления и оптимизации нормативно-правовой базы в рамках указанных направлений исследования.

Для начала определим понятийно-категориальный аппарат проблемной сферы. Легальной дефиниции технологии «блокчейн» до сих пор не существует. Мнения научного сообщества на это весьма различны. Мы считаем, что более удачное определение технологии даёт Д.В. Балдов, определяя блокчейн как новый способ хранения информации, только электронный [15. С. 29].

Стоит сказать, что необходимость создания нового способа хранения информации вызвана тем, что привычный способ стал слишком уязвим для несанкционированного воздействия на вычислительную технику с целью нарушения работы системы хранения информации или получения секретной информации. В связи с тем, что цифровизация проходит почти повсеместно, масштаб уязвимости информационных ресурсов приобретает глобальный характер.

Однако заметим, что финансирование процедуры избирательного процесса и предоставляемого материально-технического обеспечения находится на должном уровне, позволяющем отразить внешние атаки.

Ещё одним положительным и весьма очень важным аспектом применения технологии блокчейна в избирательном процессе является то, что при подтверждении личности человеком его персональные данные будут зашифрованы, а доступ к ним закрыт. Все это можно

объяснить тем, что после процедуры голосования информация поступает в систему, где пользователь сети подтверждает действие, а майнер (человек, который отвечает за работу сети блокчейна и проверку транзакций) сети добавляет блок в блокчейн.

На официальном портале mos.ru в результате таких действий любой пользователь может увидеть в открытом доступе следующую информацию: за кого он отдал голос, время голосования и время учёта голоса. Причем не только свой, но и всех избирателей по всем кандидатам. Считаем целесообразным разрабатывать аналогичные способы наблюдения и для федерального дистанционного электронного голосования, где будут отображаться: передача голоса, время голосования и время учёта голоса.

Благодаря способности эллиптической криптографии обмен ключами способствует защите информации даже через незащищенные каналы связи. Нельзя не отметить, что безопасный обмен секретными ключами является весьма востребованным в наше время.

В 2020 г. ключ шифрования для онлайн голосования на выборах был разбит на 5 частей, в 2021 г. – на 8 частей, в 2022 г. – на 5 частей. В 2023 г. при проведении дистанционного электронного голосования ключ шифрования был разбит на 7 частей, при соединении 5 из которых означало, что итоги выборов признавались действительными [16. С. 6]. То есть повышением доверия к институту дистанционного электронного голосования служит то, что возможность расшифровать результаты выборов будет возможна даже в том случае, если несколько частей будут уничтожены. В 2024 г. на прошедших мартовских и сентябрьских выборах использовалось, по информации от IT-эксперта и лидера «Партии прямой демократии» Олега Артамонова, 7 частей ключа шифрования с возможностью восстановления через 5 частей.

Последние выборы наглядно продемонстрировали демократичность избирательного процесса в рамках рассматриваемой избирательной технологии, так как задействованы в сохранении ключа шифрования были не только провластные партии и политические деятели, что положительно сказалось на легитимности результатов выборов и уровне доверия граждан к дистанционному электронному голосованию.

Оптимизация нормативно-правовой базы по регулированию как самого блокчейна, так и технологий ему сопутствующих, сейчас требует восполнения значительных пробелов.

Технология блокчейна на территории Российской Федерации регулируется Федеральным законом «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 № 259-ФЗ, Федеральным законом «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» от 12.06.2002 № 67-ФЗ и Постановлением ЦИК России от 08.06.2022 № 86/716-8 «О Порядке дистанционного электронного голосования с использованием федеральных государственных информационных систем», однако прямого и деталь-

ного регулирования с учетом специфики всех технических аспектов сейчас не имеется. Учитывая объективно присущую специфику технической сферы, не лишено здравого смысла предложение о разработке обособленного закона «О правовом регулировании технологии блокчейн на территории Российской Федерации».

В настоящее время всесторонне проявляется ряд факторов, препятствующих конструированию действенного механизма внедрения новой технологии блокчейна в российскую правовую действительность.

Как отмечал исследователь Н.С. Чимаров, правовое регулирование внедрения блокчейна должно базироваться на основе закреплённых принципов избирательного права как в международных договорах, так и в системе национального законодательства [17. С. 144].

Так, никто не может гарантировать, что на избирателя в условиях процедуры голосования дома не будет оказываться давление и он примет решение не в соответствии со своими соображениями, а под воздействием чужого влияния, поэтому в таких условиях под угрозу ставится тайна голосования. Однако тут можно поспорить с тем, что давление может оказываться на избирателя и при стандартной процедуре до его явки на выборы (в семейном кругу, среди друзей, профессиональном коллективе и т.д.).

Стоит сказать, что большинство граждан ставит под сомнение при проведении дистанционного электронного голосования соблюдение принципа гласности и открытости. Мы полностью с этим несогласны, в связи с тем, что Общественной Палатой Российской Федерации (далее – ОП РФ) был разработан так называемый «Золотой стандарт» наблюдения за дистанционным электронным голосованием, который содержит в своем содержании 45 пунктов [18. С. 25]. «Золотой стандарт» наблюдения за дистанционным электронным голосованием позволяет контролировать процесс процедуры голосования с самого начала и до момента его завершения. Дополнительно ОП РФ готова обсудить каждый из этих пунктов и принять во внимание любое предложение. В связи с чем мы предлагаем дополнить их пунктом следующего содержания: «одна из частей зашифрованного ключа может передаваться по запросу (который рассматривается ТИК ДЭГ) оппозиционно-настроенным политическим деятелям или лидерам партий».

Кроме того, в рамках повышения уровня доверия граждан к ДЭГу избирательным комиссиям всех уровней следует увеличить интенсивность проводимой агитационной и разъяснительной работы с населением. Для этого необходимо в избирательных комиссиях всех уровней поднимать вопрос о повышении уровня квалификации действующих сотрудников в психологическом направлении или же организовать привлечение для работы граждан, уже имеющих психологическое образование. Так как мало понимать нормативно-правовую основу функционирования избирательного процесса, нужно уметь донести данную информацию до населения. Также положительным моментом повышения квалификации в области психологии является тот факт, что сотрудники избирательных комиссий

смогут более эффективно решать возникающие во время проведения избирательных процедур конфликтные ситуации.

В связи с тем, что в настоящее время отсутствует руководство гражданам в случае возникновения нестандартных ситуаций при голосовании посредством сервиса Портала государственных услуг Российской Федерации, выявляющих нарушения при проведении дистанционного электронного голосования, в рамках наблюдения. Мы решили дополнить основной алгоритм поведения граждан в случае возникновения нестандартных ситуаций при голосовании посредством Портала государственных услуг Российской Федерации, разработанный в рамках создания Золотого стандарта, следующими положениями:

1. При наблюдении за дистанционным электронным голосованием следует анализировать отображающиеся данные как по абсолютным, так и по относительным показателям. При проведении статистического наблюдения измерение абсолютных величин играет важную роль в оценке характеристик изучаемых данных голосования, относительные же показатели позволяют измерить соотношение между двумя сопоставляемыми величинами (графики разных кандидатов).

2. Следует через систему Портала наблюдения за ДЭГ отслеживать голосование по всем округам для обнаружения одинакового паттерна (повторяющиеся способы действий и реакций на события) поведения избирателей.

При выявлении любой нестабильности или подозрительных изменений, указанных в пунктах выше, требуется незамедлительно обратиться к представителям избирательных комиссий или по телефону горячей линии ЦИК РФ: 8 (800) 200-00-20, а также в правоохранительные органы (номера телефонов индивидуально по субъектам).

Помимо этого, считаем, что система контроля наблюдения за ДЭГ должна состоять из двух уровней:

1. Обычные наблюдатели, не имеющие специального технического образования (например представители партий, общественных организаций и т.д.).

2. Профессиональные специалисты, имеющие образование в технической сфере и представители научного сообщества.

Формирование системы контроля наблюдения за ДЭГ с помощью этих двух уровней будет способствовать обеспечению повышения доверия граждан к ДЭГу и нивелированию их уверенности в возможность внешнего вмешательства процедуры выборов.

Особого внимания стоит уделить тестированию системы ГАС «Выборы» 2.0, ЦИК РФ планирует получить около 1,5 миллионов заявок от граждан, желающих принять тестирование системы голосования, отметим, что такой подход не является совсем верным, так как система не получает максимальной пиковой нагрузки, которая будет реализована при настоящих выборах, соответственно для выявления нестабильных мест и технических ошибок следует увеличивать при тестировании системы количество заявок от избирателей, желающих принять участие в апробировании системы.

Помимо всего вышеперечисленного, считаем, что сейчас остро назревает необходимость привлечения специалистов в области наблюдения за дистанционным электронным голосованием для работы в избирательных комиссиях. Привлечь их можно путем проведения агитационных мероприятий на выпускных курсах ведущих высших учебных заведений нашей страны. Но главный ориентир здесь должен быть направлен не только на выпускников, обучающихся в сфере информационной безопасности, но и на студентов 2–3-х курсов, с целью проявления интереса к будущей работе в рамках проведения дистанционного электронного голосования, а также к проведению научных разработок, способствующих повышению эффективности ДЭГа в Российской Федерации.

Подводя итог вышесказанному, отметим, что доверие граждан – достаточно важный фактор при проведении любых выборов, так как только при объективном доверии обеспечивается их легитимность. Полученные в данной работе выводы могут найти свое применение в рамках дальнейшего совершенствования дистанционного электронного голосования на территории Российской Федерации.

В результате проведенного исследования, посвященного актуальным проблемам доверия граждан к дистанционному электронному голосованию в рамках применения технологии блокчейна, можно сделать следующие выводы и обобщения.

Современные информационные технологии, также известные как цифровые технологии, оказывают влияние на все сферы общественной жизни. Появление этих технологий приводит к изменению традиционных общественных отношений и появлению новых отношений, которые определяются возможностями цифровых технологий, что требует разработки новых правовых норм, институтов и даже подотраслей права.

Указанные обстоятельства требуют определения и изучения этих изменений, а также разработки качественного правового регулирования цифровых технологий и отношений по поводу их применения.

Весьма важным является вопрос безопасности дистанционного электронного голосования и возможности внешнего вмешательства в него. В нем, как показывают проведенные опросы, и заключается одна из основных проблем формирования доверительного отношения граждан к дистанционному голосованию.

Стоит отметить, что недоверие граждан раскрывается в двух формах – объективной и субъективной. Объективная подразумевает, например, ситуации, при которых из-за совокупности собственных знаний избиратели или участники референдума имеют недостаточно правильное или вовсе ошибочное представление

о процедуре дистанционного электронного голосования. Субъективная же форма предполагает, например, ситуации, когда гражданин скептически относится к любым общественным отношениям, которые так или иначе связаны с информационно-телекоммуникационной средой и необходимостью предоставления персональных данных. Важно уточнить, что в основном недоверие выражает старшее поколение (в возрасте от сорока лет).

С другой стороны, молодые люди в возрасте от 18 до 35 лет, что также наглядно демонстрируют данные из опросов, проявляют интерес к дистанционному электронному голосованию как наиболее удобной форме выражения воли в избирательном процессе или при проведении референдумов в связи с отсутствием необходимости выделения времени для посещения избирательных участков. Превалирующее большинство респондентов ответили, что ДЭГ обеспечивает конфиденциальность данных, а результаты голосования на федеральной и региональной платформах дистанционного электронного голосования являются достоверными.

Возникающие проблемы обусловлены объективными факторами технического и правового характера. Представляется, что формирование положительного отношения граждан к ДЭГ достижимо при ряде необходимых условий:

- 1) совершенствование законодательства в области использования дистанционного электронного голосования;
- 2) работа по совершенствованию технической, программной частей и своевременного исправления выявленных ошибок и сбоев;
- 3) распространение его использования в выборах на все регионы Российской Федерации;
- 4) повсеместная работа представителей избирательных комиссий всех уровней с населением по поводу разъяснения им механизмов дистанционного электронного голосования, способов обеспечения защиты персональных данных, особенностей шифрования, анонимизации результатов.

Таким образом, можно заключить, что дистанционное электронное голосование прогрессивно; эксперименты с его использованием в регионах в большинстве случаев (в Москве, Курской, Ярославской, Ростовской областях) показали достаточно высокую заинтересованность в нем граждан, а проведенные опросы подтвердили постепенное формирование доверительного отношения к нему среди населения, но также были выявлены некоторые проблемы, качественное решение которых – залог эффективного развития дистанционного электронного голосования в Российской Федерации.

Список источников

1. Синюков В.Н. Право XXI века: сущность и новизна // Право и общество в эпоху социально-экономических преобразований XXI века: опыт России, ЕС, США и Китая : коллективная монография к 90-летию Университета имени О.Е. Кутафина (МГЮА) / под общ. ред. В.В. Блажеева, М.А. Егоровой. М. : Проспект, 2021. С. 12–29.
2. Карцхия А.А. Цифровые права и правоприменение // Мониторинг правоприменения. 2019. № 2 (31). С. 43–46.
3. Танимов О.В. Трансформация правоотношений в условиях цифровизации // Актуальные проблемы российского права. 2020. Т. 15, № 2 (111). С. 11–18.
4. Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1 (253). С. 85–102.
5. Рыбаков А.В. Избирательное право и избирательные системы // Социально-политический журнал. 1998. № 2. С. 113–122.

6. Исследование: почти 70% россиян используют смартфон для выхода в интернет // Информационное агентство ТАСС. URL: <https://tass.ru/obschestvo/9508331/amp> (дата обращения: 22.10.2024).
7. Антон Ткачев: Из-за санкций россияне активно используют криптовалюту // Парламентская газета. URL: <https://www.pnp.ru/economics/anton-tkachev-iz-za-sankciy-rossiyane-aktivno-ispolzuutkriptovalyutu.html> (дата обращения: 28.10.2024).
8. Антонов Я.В. Электронное голосование в системе электронной демократии: конституционно-правовое исследование : автореф. дис. ... канд. юрид. наук. М., 2015.
9. Яркова О.Н., Осипова А.А. Защищенная система электронного голосования на основе криптографических алгоритмов // Вестник УрФО. Безопасность в информационной сфере. 2014. № 2 (12). С. 9–15.
10. Дистанционное электронное голосование: официальный сайт Центральной избирательной комиссии Российской Федерации // Центральная Избирательная Комиссия Российской Федерации. URL: <http://www.cikrf.ru/analog/ediny-den-golosovaniya-2023/distantionnoe-elektronnoe-golosovanie/>.
11. Трофимова И.Н. Доступность и использование сети Интернет: проблема цифрового неравенства // Россия: Тенденции и перспективы развития: Ежегодник. Материалы XIII Международной научно-практической конференции, Курск, 03–04 июня 2022 года / отв. ред. В.И. Герасимов. Вып. 17, ч. 2. М. : Институт научной информации по общественным наукам РАН, 2022. С. 468–471.
12. Овчинников В.А., Антонов Я.В. Основы обеспечения безопасности информации в рамках систем электронного голосования // Российская юстиция. 2013. № 3. С. 46–48.
13. Чаннов С.Е. Использование блокчейн-технологий для ведения реестров в сфере государственного управления // Административное право и процесс. 2019. № 12. С. 29–34.
14. Генпрокуратура сообщила о росте числа дистанционных мошенничеств на 40% // Информационное агентство ТАСС. URL: <https://tass.ru/obschestvo/18957905> (дата обращения: 29.10.2023).
15. Балдов Д.В., Петрова С.Ю., Лебедев А.А. Использование технологии блокчейн для защиты данных // International Journal of Open Information Technologies. 2021. Т. 9, № 9. С. 27–34.
16. Ерохина О.В. Технологии электронного голосования в России // Вестник университета. 2019. № 11. С. 5–11.
17. Былинкина Е.В. Блокчейн: правовое регулирование и стандартизация // Право и политика. 2020. № 9. С. 143–155.
18. Чимаров Н.С., Сергиенко А.М. Правовые основы дистанционного электронного голосования в контексте развития электронной демократии // Вестник Санкт-Петербургской юридической академии. 2021. № 3 (52). С. 23–26.

References

1. Sinyukov, V.N. (2021) Pravo XXI veka: sushchnost' i novizna [Law of the 21st century: essence and novelty]. In: Blazheev, V.V. & Egorova, M.A. (eds) *Pravo i obshchestvo v epokhu sotsial'no-ekonomicheskikh preobrazovaniy XXI veka* [Law and Society in the Era of Socioeconomic Transformations of the 21st Century]. Moscow: Prospekt. pp. 12–29.
2. Kartskhiya, A.A. (2019) Tsifrovye prava i pravoprimeneniye [Digital rights and law enforcement]. *Monitoring pravoprimeneniya*. 2 (31). pp. 43–46.
3. Tanimov, O.V. (2020) Transformatsiya pravootnosheniy v usloviyakh tsifrovizatsii [Transformation of legal relations in the context of digitalization]. *Aktual'nye problemy rossiyskogo prava*. 2-15 (111). pp. 11–18.
4. Khabrieva, T.Ya. & Chernogor, N.N. (2018) Pravo v usloviyakh tsifrovoy real'nosti [Law in the conditions of digital reality]. *Zhurnal rossiyskogo prava*. 1 (253). pp. 85–102.
5. Rybakov, A.V. (1998) Izbiratel'noye pravo i izbiratel'nye sistemy [Electoral law and electoral systems]. *Sotsial'no-politicheskiy zhurnal*. 2. pp. 113–122.
6. TASS. (2024) Issledovaniye: pochtu 70% rossiyan ispol'zuyut smartfon dlya vykhoda v internet" [Research: Almost 70% of Russians Use Smartphones to Access Internet]. TASS. 21 September. [Online] Available from: <https://tass.ru/obschestvo/9508331/amp> (Accessed: 22.10.2024).
7. Tkachyov, A. (2023) Iz-za sanktsiy rossiyan aktivno ispol'zuyut kriptovalutu [Due to sanctions Russians actively use cryptocurrency]. *Parlament-skaya gazeta*. 30 October. [Online] Available from: <https://www.pnp.ru/economics/anton-tkachev-iz-za-sankciy-rossiyane-aktivno-ispolzuutkriptovalyutu.html> (Accessed: 28.10.2024).
8. Antonov, Ya.V. (2015) *Elektronnoye goslovaniye v sisteme elektronnoy demokratii: konstitutsionno-pravovoye issledovaniye* [Electronic voting in the e-democracy system: constitutional and legal study]. Abstract of Law Cand. Diss. Moscow.
9. Yarkova, O.N. & Osipova, A.A. (2014) Zashchishchennaya sistema elektronnoy goslovaniya na osnove kriptograficheskikh algoritmov [Secure electronic voting system based on cryptographic algorithms]. *Vestnik UrFO. Bezopasnost' v informatsionnoy sfere*. 2 (12). pp. 9–15.
10. Tsentral'naya izbiratel'naya komissiya Rossiyskoy Federatsii [Central Election Commission of the Russian Federation]. (2023) *Distantionnoye elektronnoye goslovaniye* [Remote Electronic Voting]. [Online] Available from: <http://www.cikrf.ru/analog/ediny-den-golosovaniya-2023/distantionnoe-elektronnoe-golosovanie/>
11. Trofimova, I.N. (2022) [Accessibility and Internet use: the problem of digital inequality]. *Rossiya: Tendentsii i perspektivy razvitiya* [Russia: Development Trends and Prospects]. Proceedings of the 13th International Conference. Vol. 17. Part 2. Kursk. 3–4 June 2022. Moscow: Institute of Scientific Information for Social Sciences RAS. pp. 468–471. (In Russian).
12. Ovchinnikov, V.A. & Antonov, Ya.V. (2013) Osnovy obespecheniya bezopasnosti informatsii v ramkakh sistem elektronnoy goslovaniya [Fundamentals of information security in electronic voting systems]. *Rossiyskaya yustitsiya*. 3. pp. 46–48.
13. Channov, S.E. (2019) Ispol'zovaniye blokcheyn-tekhnologiy dlya vedeniya reestrov v sfere gosudarstvennogo upravleniya [Use of blockchain technologies for registry maintenance in public administration]. *Administrativnoye pravo i protsess*. 12. pp. 29–34.
14. TASS. (2023) Genprokuratura soobshchila o roste chisla distantionnykh moshennichestv na 40% [General Prosecutor's Office Reported a 40% Increase in Remote Frauds]. TASS. 10 October. [Online] Available from: <https://tass.ru/obschestvo/18957905> (Accessed: 29.10.2023).
15. Baldov, D.V., Petrova, S.Yu. & Lebedev, A.A. (2021) Ispol'zovaniye tekhnologii blokcheyn dlya zashchity dannykh [Use of blockchain technology for data protection]. *International Journal of Open Information Technologies*. 9 (9). pp. 27–34.
16. Erokhina, O.V. (2019) Tekhnologii elektronnoy goslovaniya v Rossii [Electronic voting technologies in Russia]. *Vestnik universiteta*. 11. pp. 5–11.
17. Bylinkina, E.V. (2020) Blokcheyn: pravovoye regulirovaniye i standartizatsiya [Blockchain: legal regulation and standardization]. *Pravo i politika*. 9. pp. 143–155.
18. Chimarov, N.S. & Sergienko, A.M. (2021) Pravovyye osnovy distantionnoy elektronnoy goslovaniya v kontekste razvitiya elektronnoy demokratii [Legal foundations of remote electronic voting in the context of e-democracy development]. *Vestnik Sankt-Peterburgskoy yurydicheskoy akademii*. 3 (52). pp. 23–26.

Информация об авторах:

Масуфранова Е.А. – канд. ист. наук, доцент кафедры конституционного права Юго-Западного государственного университета (Курск, Россия). E-mail: a25021985@yandex.ru

Дубровский Н.С. – специалист Управления Министерства юстиции Российской Федерации по Курской области (Курск, Россия). E-mail: KeShucTuk@yandex.ru

Балашов К.Г. – помощник адвоката Адвокатской конторы Красноперекопского района г. Ярославля (Ярославская областная коллегия адвокатов) (Ярославль, Россия). E-mail: balashoffkonstantin@yandex.ru

Авторы заявляют об отсутствии конфликта интересов.

Information about the authors:

E.A. Masufranova, Cand. Sci. (History), associate professor, Southwest State University (Kursk, Russian Federation). E-mail: a25021985@yandex.ru

N.S. Dubrovsky, specialist, Administration of the Ministry of Justice of the Russian Federation for Kursk Oblast (Kursk, Russian Federation). E-mail: KeIIIycTuk@yandex.ru

K.G. Balashov, lawyer's assistant, Law Office of Krasnoperekopsky District of Yaroslavl (Yaroslavl, Russian Federation). E-mail: balashoffkonstantin@yandex.ru

The authors declare no conflicts of interests.

*Статья поступила в редакцию 27.11.2024;
одобрена после рецензирования 17.09.2025; принята к публикации 30.09.2025.*

*The article was submitted 27.11.2024;
approved after reviewing 17.09.2025; accepted for publication 30.09.2025.*