

ЗАЩИТА РЕЗУЛЬТАТОВ ВОЛЕИЗЪЯВЛЕНИЯ ИЗБИРАТЕЛЕЙ ПРИ ДИСТАНЦИОННОМ ЭЛЕКТРОННОМ ГОЛОСОВАНИИ

Аннотация. В статье рассматриваются тенденции регулирования и применения дистанционного электронного голосования (ДЭГ) в зарубежных странах и в России. Исследуется история внедрения ДЭГ на выборах в нашей стране. Предлагается классификация форм голосования: его основная и производные формы. ДЭГ отнесено к производной форме голосования. Дается определение фальсификации и предлагается оценка ее риска в зависимости от форм голосования. Основная форма голосования оценивается как наименее рискованная в аспекте фальсификации результатов волеизъявления избирателей. ДЭГ квалифицируется как наиболее рискованная и нуждающаяся в дополнительных мерах правовой защиты волеизъявления избирателей. Анализируются существующие средства защиты результатов волеизъявления избирателей в ДЭГ и выдвигаются предложения по их совершенствованию и дополнению. Основной вывод заключается в том, что ДЭГ, как новая форма голосования, требует дополнительных средств защиты результатов голосования. Среди этих средств акцент делается на совершенствовании наблюдения за ДЭГ.

Ключевые слова: выборы, формы голосования, дистанционное электронное голосование, ДЭГ, наблюдение, результаты волеизъявления избирателей, правовая защита.

PROTECTION OF THE RESULTS OF THE WILL OF THE VOTERS WITH REMOTE ELECTRONIC VOTING

Abstract. The article discusses the trends in the regulation and use of remote electronic voting (REV) in foreign countries and in Russia. The history of the implementation of the REV in the elections in Russia is studied. A classification of voting forms is proposed: basic and derived forms. The REV is classified as a derivative form of voting. A definition of falsification is given and an assessment of its risk is proposed depending on the forms of voting. The main form of voting is assessed as the least risky in terms of falsification of the results of the will of voters. The REV is qualified as the riskiest and in need of additional measures of legal protection of the voter's will. The existing means of protecting the results of the expression of the voter's will in the REV are analyzed and proposals are put forward for their improvement and addition. The main conclusion is that the REV, as a new form of voting, requires additional means of protecting the voting results. Among these tools, emphasis is placed on improving REV surveillance.

Keywords: *elections, forms of voting, remote electronic voting, REV, observation, results of the voter's will, legal protection.*

Исследования доступности Интернета показывают, что в России около 80 процентов населения систематически пользуются Всемирной сетью¹. Бурное развитие цифровизации породило новое социально-правовое явление — электронную демократию, которая является предметом пристального исследования ученых-юристов [1, с. 45–57; 2, с. 38–49]. Одним из проявлений электронной демократии выступает дистанционное электронное голосование, которое также нередко именуется интернет-голосованием.

К преимуществам дистанционного электронного голосования (ДЭГ), способствующим его распространению в будущем, исследователи относят удобство и доступность [3, с. 218–222], экологичность (не требует тиражей бумажных бюллетеней) и экономичность [4, с. 37–47], повышение явки [1], защищенность голосования и быстрота подведения его итогов [5], привлекательность для молодых избирателей [6, р. 53–62].

На протяжении последних двух десятилетий разные страны экспериментировали с интернет-голосованием. В 2000 году Швейцария запустила проект «Электронное голосование». В 2008 году Норвегия провела тестирование интернет-голосования и несколько испытаний во время муниципальных выборов 2011 года и парламентских выборов 2013 года. В Канаде интернет-голосование доступно в провинциях Онтарио и Новая Шотландия с 2003 года. Пожалуй, наиболее успешный эксперимент был проведен в Эстонии, где обсуждение интернет-голосования началось в 2001 году, а с 2005 года оно стало юридически обязательной формой голосования [7]. По данным портала e-voting [8] в 2015 году интернет-голосование применялось в четырех странах: Канаде, Швейцарии, Эстонии, Индии. В четырех странах велись дискуссии в связи с проведенными экспериментами по применению интернет-голосования: Исландии, Великобритании, Литве и Финляндии. В Норвегии, Австрии, Германии, Ирландии, Казахстане после проведения экспериментов по разным причинам отказались от электронного голосования. Еще в 40 странах Европы, Южной Америки, Африки и Азии велись теоретические дискуссии относительно возможного использования ДЭГ на выборах.

Таким образом, ДЭГ, с одной стороны, пока не слишком широко распространено в качестве устоявшейся формы голосования, с другой, — его преимущества стимулируют избирательные органы многих стран проводить эксперименты по его внедрению, результаты которых оцениваются неоднозначно.

¹ Internet Stats and Facebook Usage in Europe 2021 Mid-Year Statistics [Электронный ресурс] // <https://www.internetworldstats.com/europa2.htm#ru> (дата обращения: 10.01.2022).

В России ДЭГ длительное время обсуждалось теоретически, с ним проводились осторожные эксперименты и, наконец, пандемия подтолкнула власти к его широкому применению.

В отечественной истории интернет-голосования можно выделить четыре этапа становления, как правового института в избирательном праве: первый этап — теоретические исследования ДЭГ и проведение экспериментов [9; 10, с. 5–13; 11, с. 237–247], не имеющих юридических последствий, — 2006–2018 годах; второй этап — эксперимент² на выборах депутатов Московской городской думы в 2019 году, имеющий обязательные правовые последствия; третий этап — при сохранении экспериментального режима распространение ДЭГ на разные уровни выборов и голосований³ [12] — 2020 год (в октябре 2008 года был проведен первый эксперимент: голосование через Интернет было протестировано во время выборов в местные органы власти в городе Новомосковске Тульской области); четвертый этап — стабилизация ДЭГ как устойчивого института избирательного права, научный поиск разрешения выявленных практикой проблем [13, с. 25–30 и др.]⁴ — 2021–2022 годы.

На первых этапах введение ДЭГ в электоральную практику не сопровождалось всплеском судебных споров. Впрочем, в ходе московского эксперимента в 2019 году интересны два дела. Так, один из кандидатов оспорил утвержденный Московской городской избирательной комиссией порядок ДЭГ, полагая, что он не предусматривает удостоверение личности избирателя, не дает гарантий тайны голосования, а «зашифровывание» данных не способно обеспечить эту тайну. Однако суд отказал⁵ в иске, указав, в частности, что процедура шифрования волеизъявления специальным программным обеспечением гарантирует тайну голосования.

² Федеральный закон от 29.05.2019 № 103-ФЗ «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва» // *Собрание законодательства РФ*. 03.06.2019. № 22. ст. 2659; Закон г. Москвы от 22.05.2019 № 18 «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва» // *Вестник Мэра и Правительства Москвы*. № 30. 30.05.2019.

³ Закон Российской Федерации о поправке к Конституции Российской Федерации от 14.03.2020 № 1-ФКЗ «О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти» // «Собрание законодательства РФ», 16.03.2020, № 11, ст. 1416; Федеральный закон от 23.05.2020 № 152-ФЗ «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования в городе федерального значения Москве» // *Собрание законодательства РФ*. 25.05.2020. № 21. ст. 3231.

⁴ Федеральный закон от 23.05.2020 № 154-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // «Собрание законодательства РФ», 25.05.2020, № 21, ст. 3233; Федеральный закон от 14.03.2022 № 60-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // *Собрание законодательства РФ*. 21.03.2022. № 12. ст. 1787.

⁵ Решение Московского городского суда от 26.07.2019 по делу № За-4301/2019; Апелляционное определение Судебной коллегии по административным делам Верховного Суда Российской Федерации от 06.08.2019 № 5-АПА19–93 // СПС «Консультант плюс».

Другое дело касалось осуществления волеизъявления в ДЭГ. Истец в обоснование иска указал, что в день голосования происходили сбои в работе системы ДЭГ (под системой ДЭГ в целях исследования понимаются программно-аппаратный комплекс, обеспечивающий голосование, а также средства сетевой коммуникации между участником и организатором голосования), что привело к потере 148 голосов (избиратели получали доступ к бюллетеню, но из-за сбоев на сайте не смогли отдать свои голоса). Следует отметить, что разрыв в голосах между истцом и победителем в этом округе составил около 100 голосов. Суд отклонил иск⁶, придя к выводу, что произошедший сбой не мог повлиять на волеизъявление избирателей, так как после восстановления работы системы ДЭГ голосование продолжилось, и все избиратели смогли принять участие в голосовании.

Следующий этап охарактеризовался, пожалуй, наибольшей спорностью применения ДЭГ. Все дела были связаны с голосованием в Москве на выборах депутатов Государственной Думы, депутатов Московской городской думы и депутатов одного из муниципальных округов. Доводы истцов в целом сводились к тому, что использованная 17–19.09.2021 система ДЭГ была небезопасна; не была избавлена от сбоев в работе, которые приводили к потере голосов избирателей; позволяла внести в список избирателей любое лицо, в том числе вымышленное; была непрозрачна и допускала нарушения в осуществлении наблюдения за ходом голосования и подсчетом голосов; по странному совпадению привела во всех округах к выигрышу определенной группы кандидатов исключительно благодаря победе на «цифровых» участках; допускала процедуру переголосования, при которой голоса индивидуализировались и связывались с подавшими их избирателями; позволила исказить волеизъявление избирателей и привела к недостоверным итогам.

Суды отказали⁷ во всех исках, сделав вывод, что процедура анонимизации и шифрования поданного голоса обеспечивала тайну голосования; процедуры аутентификации и идентификации обеспечивали установление личности избирателя; вмешательство оператора в расшифрование голосов и подсчет голосов не доказано. Суды посчитали, что публикации⁸ со стати-

⁶ Решение Чертановского районного суда от 30.10.2019 по делу № 02а-0296/2019 // <https://mosgorsud.ru/ts/chertanovskij/services/cases/kas/details/e91b1c8d-cde5-49e6-91a8-9d2dce486da7> (дата обращения: 11.01.2022).

⁷ См., например, решение Пресненского районного суда по делу № 02а-0670/2021 Лобанов М.С. к УИК № 5013, решение Тушинского районного суда по делу № 02а-0810/2021 Абушаев Т.Р. к УИК № 5020 и др.

⁸ А. Заякин. Боты с правом решающего голоса. Сайт «Новой газеты» [Электронный ресурс] // <https://novayagazeta.ru/articles/2021/09/27/boty-s-pravom-reshaiushchego-golosa> (дата обращения: 11.01.2022); А. Лобанов, Н. Колосов, И. Сухоруков. Настоящие голоса попали в черный ящик. Сайт «Новой газеты» [Электронный ресурс] // <https://novayagazeta.ru/articles/2021/09/28/nastoiashchie-golosa-popali-v-chernyi-iashchik> (дата обращения: 11.01.2022); М. Гонгальский, И. Снимщиков, Я. Соболев. Мандаты пользуются вбросом. Сайт «Новой газеты» [Электронный ресурс] // <https://novayagazeta.ru/articles/2021/09/30/mandaty-polzuiutsia-vbrosom> (дата обращения: 11.01.2022);

стическими выкладками аномалий на «цифровых» участках, на которые ссылались истцы, не являются достаточными доказательствами, чтобы установить нарушения в ходе ДЭГ.

Таким образом, судебные споры высветили ряд правовых рисков в электронно-цифровой форме голосования {согласно ГОСТу (ГОСТ Р 51897–2011 / Руководство ИСО 73:2009. Национальный стандарт Российской Федерации. Менеджмент риска. Термины и определения. — М.: Стандартиформ, 2012), «Риск — это следствие влияния неопределенности на достижение поставленных целей. Под следствием влияния неопределенности необходимо понимать отклонение от ожидаемого результата. Риск часто характеризуют путем описания возможного события и его последствий или их сочетания, также его часто представляют в виде вероятности. Неопределенность — это состояние полного или частичного отсутствия информации, необходимой для понимания события, его последствий и их вероятностей». Для целей настоящей статьи риск рассматривается как вероятность негативных последствий дистанционного электронного голосования в отношении сохранности и неизменности волеизъявления избирателя (его голоса) и достоверного его учета при подсчете голосов}.

* * *

Чтобы определить перспективы ДЭГ в российской избирательной системе, оценить его потенциальные риски и предложить способы их снижения, следует определить его особенности как формы голосования на выборах.

Свободные выборы в конечном счете материализуются в результатах волеизъявления избирателей, которые должны быть достоверными. Достоверность их достигается в том случае, когда действительная воля избирателей совпадает с их волеизъявлением. По смыслу пунктов 1 и 2 статьи 3 Федерального закона № 67-ФЗ⁹ волеизъявление избирателей реализуется в процессе тайного голосования. Статьи 64–66 этого же закона регулируют процедуры голосования в различных его формах. Анализ этих положений позволяет сделать вывод, что форма голосования на выборах — это совокупность норм избирательного права процедурного характера, гарантирующих реализацию свободного волеизъявления избирателей и его достоверный учет.

Д. Нестеров, Е. Федин, Д. Кузнецов. Соль процентов. Сайт «Новой газеты» [Электронный ресурс] // <https://novayagazeta.ru/articles/2021/10/01/sol-protsentov> (дата обращения: 11.01.2022); А. Заякин. Пошли на крайние химеры. Сайт «Новой газеты» [Электронный ресурс] // <https://novayagazeta.ru/articles/2021/10/17/poshli-na-krainie-khimery> (дата обращения: 11.01.2022).

⁹ Федеральный закон от 12.06.2002 № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» // Собрание законодательства РФ. 17.06.2002. № 24. ст. 2253.

Традиционно основной формой голосования считается голосование избирателей на участках в помещении для голосования в течение одного дня путем личной явки, заполнения бюллетеня и опускания его в стационарный ящик для голосования. Другие формы голосования, в том числе ДЭГ, определяются как производные. Их производность заключается в том, что они возникли исторически позже основной формы, но имеют с ней тесную связь. Эти формы голосования направлены на то, чтобы привлечь к участию в выборах тех, кто по тем или иным причинам не может или не хочет прийти на участок.

Дистанционное голосование — это процесс принятия решения путем голосования с применением специальных электронных средств голосования и подсчета голосов [14]. А.В. Павлушкин и А.Е. Постников предложили рассматривать ДЭГ как разновидность электронного голосования [10, с. 8]. Электронное голосование, включая дистанционное, может осуществляться в контролируемой среде, то есть в присутствии официальных лиц, и в неконтролируемой среде [15]. В законодательстве¹⁰ дистанционное электронное голосование определяется как голосование без изготовления бюллетеня на бумажном носителе с использованием программно-технического комплекса, доступ к которому участнику ДЭГ предоставляется на портале, размещенном в Интернете.

То есть, основными признаками российской модели ДЭГ являются: 1) электронный способ голосования; 2) применение избирателем персонального «гаджета» (мобильного или стационарного компьютерного устройства); 3) отсутствие бумажного бюллетеня; 4) наличие программно-аппаратного комплекса; 5) коммуникация избирателя с организатором выборов через Интернет; 6) голосование в неконтролируемой среде; 7) голосование в произвольном месте, 8) использование организатором выборов специального сайта (портала), имеющего связь со Всемирной сетью.

Совокупность перечисленных признаков ДЭГ дает основание утверждать, что это новая и высокотехнологичная форма голосования, которую необходимо проанализировать на наличие в ней риска для достоверного волеизъявления избирателей, который связывается с таким понятием, как фальсификация. О.А. Кравченко понимает под фальсификацией любое искажение волеизъявления избирателей [16, с. 82–91]. По мнению Д.О. Парамонова

¹⁰ Федеральный закон от 29.05.2019 № 103-ФЗ «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва» // Собрание законодательства РФ. 03.06.2019. № 22. ст. 2659; Закон г. Москвы от 22.05.2019 № 18 «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва» // Вестник Мэра и Правительства Москвы». № 30. 30.05.2019; Федеральный закон от 23.05.2020 № 154-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ. 25.05.2020. № 21. ст. 3233.

и В.В. Кириченко, фальсификация — это преднамеренное искажение результатов голосования путем манипуляции с избирательными документами, удостоверяющими волеизъявление граждан, либо путем преднамеренного изменения свободного волеизъявления граждан [17, с. 12]. Ж.Б. Скрипкина делает акцент на преднамеренности фальсификаций [18, с. 168].

Соглашаясь с перечисленными мнениями исследователей и обобщая их, можно дать следующее определение фальсификации: это — подмена подлинного волеизъявления избирателей. Фальсификация разрушает саму суть свободных выборов как конституционной ценности, и ей следует противопоставить надежный правовой механизм противодействия.

С точки зрения риска фальсификаций наименее рискованной является основная форма голосования. Возможность подмены подлинного волеизъявления избирателей при голосовании на участке снижается наблюдением. Конкурирующие силы на выборах направляют на участки своих наблюдателей, которые следят за соблюдением процедуры голосования и сохранностью голосов и противодействуют заинтересованным в искажении результатов голосования лицам. Контроль также осуществляется независимыми наблюдателями и журналистами. На участке наблюдение сфокусировано в одном месте и в ограниченное время, а потому риск при этой форме голосования надо оценить, как наименьший.

Исследование научных источников, а также изучение судебной практики выявили ряд проблем ДЭГ, сопряженных с рисками для подлинного волеизъявления избирателей.

На первом этапе в процедуре ДЭГ осуществляется идентификация лица, как избирателя. Исследователи [см., например, 19, с. 59–63] единодушны в том, что имеется проблема удостоверения личности лица, которое запрашивает доступ к участию в ДЭГ. Эта проблема влечет риск включения в список для голосования не-избирателей. Кроме того, совмещение в системе ДЭГ процедур идентификации избирателя, голосования и сохранения его голоса до начала подсчета влечет риск установления связи между личностью избирателя и его волеизъявлением (особенно актуален этот риск для процедуры переголосования — неоднократного голосования на протяжении некоторого промежутка времени, когда учету подлежит только последний голос).

Исследователи ДЭГ [20, с. 106–108; 21, с. 16–23] не менее единодушно отмечают проблему сохранения тайны голосования как основную, на нее же обращают пристальное внимание и международные институты [22]. Поскольку заполнение электронного бюллетеня происходит вне контроля со стороны избирательной комиссии и наблюдателей, нельзя исключить так называемое семейное голосование, когда избиратель голосует в кругу близких или под влиянием иных посторонних лиц. Эта проблема влечет риск

покупки голосов или иного воздействия на волеизъявление избирателей в момент его совершения.

Ученые сходятся на том, что система ДЭГ является «черным ящиком» для абсолютного большинства граждан [23, с. 80–83]. В силу физической природы процессов, происходящих в компьютерном оборудовании, судить о них можно лишь опосредованно с помощью программного обеспечения и средств визуализации. Для глубокого понимания этих процессов необходимы специальные знания, которые есть лишь у немногих экспертов. Сама по себе сложность устройства системы ДЭГ создает риск того, что внутри этого «черного ящика» заинтересованными лицами (экспертами) с применением высокотехнологичных средств могут осуществляться манипуляции с голосами и недостоверный их подсчет. Проблема «черного ящика» влечет риск утраты контроля за честностью голосования.

В ряде исследований [см., например, 24, с. 345–350] авторы обращают внимание на то, что компьютерная малограмотность избирателей старшего возраста, отсутствие у малообеспеченных групп населения нужных для ДЭГ «гаджетов» и доступа в Интернет порождает риск «цифрового разрыва» (неравенство непродвинутых и продвинутых избирателей). Упомянутые выше судебные споры выявили, что сбои в системе ДЭГ — не редкость, и они влекут риск потери голосов избирателей, на что указывают и ученые-юристы [см., например, 25, с. 41–49]. Другие исследователи [26, с. 302–314 и др.] обращают внимание на то, что намеренное и непреднамеренное вмешательство в систему ДЭГ влечет риск неправильного учета и подсчета голосов. Все вместе эти проблемы создают в совокупности недоверие к ДЭГ у граждан, на что справедливо указывает А.Ю. Цаплин [24]. В связи с этим ДЭГ должно быть отнесено к рискованной форме голосования, и каждый из выявленных рисков требует соответствующих мер правовой защиты.

Исторический и сравнительный анализ регулирования ДЭГ показывает, что законодатель и Центральная избирательная комиссия Российской Федерации предусмотрели ряд правовых средств, направленных на защиту результатов волеизъявления избирателей от указанных выше рисков. Действующий порядок ДЭГ¹¹ решает проблему идентификации посредством учетной записи (аккаунта) на портале государственных услуг (ПГУ) и процедуры подтверждения личности избирателя. Чтобы зарегистрировать аккаунт на ПГУ, гражданину необходимо верифицировать себя в официальном порядке. Тем самым гарантируется, что в ДЭГ участвует гражданин, удостоверивший у официального лица свою личность. Доступ к аккаунту становится возможен, если пользователь верно указал свой логин и пароль.

¹¹ В силу ограниченного объема настоящего исследования в нем сделан акцент на анализ мер административной защиты, предусмотренных в Постановлении ЦИК России от 20.07.2021 № 26/225-8 (далее — порядок ДЭГ).

Доступ же к бюллетеню можно получить путем ввода кода подтверждения, который высылается пользователю аккаунта на номер его мобильного телефона. Таким образом, создается «цепочка доверия», которая построена на крайне малой вероятности того, что случайное лицо одновременно имеет логин и пароль к чужому аккаунту и чужой мобильный телефон. Исследователи [6] справедливо ссылаются на широкое применение «цепочек доверия» в интернет-банкинге¹², операции в котором крайне редко фальсифицируются.

* * *

Надо признать, что в ДЭГ наверняка нельзя утверждать, что доступ к голосованию получает именно избиратель, а не кто-то еще, и радикальным решением этой проблемы является отказ от голосования в неконтролируемой среде. Однако такой подход стирает все выгоды интернет-голосования. Сохраняя возможность голосования в неконтролируемой среде, следует предусмотреть ответственность избирателя за передачу своего доступа к аккаунту для участия в ДЭГ постороннему лицу, а также ответственность оператора ДЭГ за недобросовестные манипуляции с аккаунтами. Кроме того, идентификацию в ДЭГ можно было бы усложнить, введя дополнительные звенья в «цепочки доверия», как это было сделано в московском порядке ДЭГ¹³ на выборах депутатов Московской городской Думы в 2019 году, когда Московская городская избирательная комиссия требовала, чтобы избиратель до получения доступа к голосованию заполнял в соответствующем поле экранной формы свой адрес. Также надо иметь в виду, что доверие к идентификации может быть повышено при использовании биометрических данных (отпечатка пальца, радужной оболочки глаза и т.д.). Возможна имплементация швейцарского опыта («В кантоне Женева после каждого голосования ответственные государственные служащие опрашивают по телефону два процента избирателей, проголосовавших по почте, чтобы убедиться, что они голосовали самостоятельно и свободно» [27]), который предусматривает выборочный опрос 2 процентов проголосовавших в ДЭГ по телефону с тем, чтоб убедиться в их реальности.

Рискованность ДЭГ в наибольшей степени проявляется в проблеме сохранения тайны голосования. При ее решении нужно учитывать принцип приоритета тайны голосования, — удобство использования ДЭГ не должно преобладать над необходимостью высокого уровня его безопасности. Для соблюдения тайны голосования нынешний порядок ДЭГ предусматривает,

¹² Статья «Интернет-банкинг». Википедия [Электронный ресурс] // <https://ru.wikipedia.org/wiki/Интернет-банкинг> (дата обращения: 24.09.2021).

¹³ Решение Мосгоризбиркома от 18.07.2019 № 102/3 2 «Об утверждении Положения о порядке дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва» // Вестник Московской городской избирательной комиссии. № 4. 05.08.2019.

что перед получением доступа к бюллетеню запускается процедура анонимизации, которая создает эффект виртуальной «кабинки», тем самым избиратель уединяется от постороннего виртуального «взгляда». Однако в реальности избиратель может использовать свой гаджет в момент голосования в людном месте. Поэтому риск нарушения тайны голосования хотя и снижается в виртуальном мире, но остается в реальном.

Для устранения этого риска ЦИК России непосредственно накануне выборов в Москве в 2021 году ввела процедуру переголосования: избиратель (проголосовавший, например, под «административным» давлением) в любое время из трех дней проведения ДЭГ мог вернуться к виртуальной «урне», найти в ней свой (специально индивидуализированный для такого случая) бюллетень и изменить голос. Однако проведенное IT-специалистами исследование¹⁴ статистики переголосований показало, что парадоксальным образом избиратели переголосовывали в пользу определенных кандидатов. Это вызвало подозрения в том, что оператор ДЭГ использовал процедуру переголосования для «перекладки» голосов из «стопки» за оппозицию в «стопку» ее соперников.

С учетом московского опыта целесообразно было бы в дальнейшем отказаться от процедуры переголосования. Если же законодатель сохранит данную процедуру, то связь между избирателем и его голосом, необходимая для обработки нескольких голосов (один голос стирает другой и учитывается только последний), должна разрываться на заранее определенной стадии хранения голосов до начала их подсчета.

Никакая остаточная информация¹⁵, относящаяся к решению избирателя, не должна отображаться в системе ДЭГ после того, как голос был подан. Оператор системы обязан принять все меры для удаления следов такой информации. Избиратель же должен быть поставлен в известность о возможных рисках сохранения ее следов и о способах их снижения.

Порядком ДЭГ¹⁶ предусмотрены гарантии гласности: присутствие наблюдателей при формировании ключей шифрования, а также в помещении участковой комиссии (УИК) ДЭГ, наличие «ноды наблюдателя» (компьютера, который визуализирует происходящее в блокчейне системы ДЭГ), кроме того, на сайте избирательной комиссии в режиме реального времени публикуются данные о ходе голосования. Однако, как верно заметил

¹⁴ М. Гонгальский, И. Снимщиков, Я. Соболев. Указ. соч.

¹⁵ Под «остаточной информацией» в рекомендации СМ/Рес (2017)5 подразумевается информация, которая остается доступной в различных источниках (в памяти персонального компьютера, кэше браузера, видеопамати, файлах подкачки, временных файлах и т.д.) после голосования и может раскрыть решение избирателя.

¹⁶ Постановление ЦИК России от 20.07.2021 № 26/225-8 «О Порядке дистанционного электронного голосования на выборах, назначенных на 19 сентября 2021 года» // Вестник ЦИК России. № 13. 2021.

Е.И. Колюшин [12, с. 29], в настоящее время механизмы контроля за ДЭГ позволяют лишь наблюдать на экранах за внешними проявлениями работы программных продуктов без правовых возможностей убедиться в ее адекватности подлинному волеизъявлению.

Прозрачность ДЭГ надо рассматривать в нескольких аспектах.

Во-первых, оно обеспечивается сложным программно-аппаратным комплексом. Его сложность создает ранее выявленный риск «черного ящика». Абсолютное большинство избирателей не разбирается в нем и вынуждено просто верить в честность разработчиков и оператора данной системы. Такое положение видится чреватом потенциальными нарушениями подлинного волеизъявления в «черном ящике». Поэтому возникает необходимость пролить свет на устройство «черного ящика» ДЭГ.

Следуя международным рекомендациям, необходимо нормативно предусмотреть, чтоб Общественная палата, представители политических партий и другие имели возможность провести аудит этой системы. На избирательную комиссию, организующую выборы, следует законодательно возложить обязанность заблаговременно публиковать исходный код программного обеспечения ДЭГ для такого аудита. Публикация должна также раскрывать конфигурацию системы, ее аппаратные и программные компоненты.

Во-вторых, со стороны избирательной комиссии должен осуществляться эффективный контроль за функционированием системы ДЭГ. Непосредственно перед началом работы организующая выборы комиссия с участием наблюдателей должна убедиться в аутентичности системы и корректности ее работы. Должны быть регламентированы изменение программного обеспечения ДЭГ и модернизация его аппаратной структуры. Кроме того, системные администраторы системы ДЭГ должны назначаться организующей выборы избирательной комиссией или с ее санкции. Все их действия в системе необходимо автоматически протоколировать. Доступ к этой информации должен быть открыт для наблюдателей.

В-третьих, в порядке ДЭГ необходимо предусмотреть расширение контроля за ним. Учитывая огромный объем информации, поступающий в блокчейн в ходе голосования, следует предусмотреть увеличение числа наблюдателей, которых кандидат может назначить в УИК ДЭГ. Следует также предусмотреть обязательную визуальную фиксацию всех событий, которые транслируются из блокчейна на «ноду наблюдателя» с возможностью просмотра записи после подведения итогов голосования.

Ситуацию сбоя работы системы ДЭГ действующее регулирование решает не до конца последовательно. Допускается неоднократное повторение ввода кода подтверждения для доступа к бюллетеню, поэтому если сбой имеет краткосрочный характер, то избиратель, не получивший доступ к бюллетеню, может попробовать получить его позднее. Однако, если сбой имеет

долгосрочный характер, то избиратель вовсе может лишиться своего голоса, поскольку законодательством предусмотрено, что внесенный в список ДЭГ избиратель не вправе проголосовать на «обычном» участке.

Во избежание потери голосов следует предусмотреть, что при длительной неработоспособности системы организующая выборы избирательная комиссия может принять решение о прекращении приема голосов в ДЭГ и о голосовании исключительно на «обычных» участках, — это открывает для избирателей, которые не успели к этому моменту подать голос в ДЭГ, возможность проголосовать на «обычном» участке.

Проблема неправильного учета голоса и подсчета голосов порядком ДЭГ решается неоднозначно. В отношении ДЭГ, осуществляемом за пределами Москвы, какое-либо подтверждение учета голоса не предусмотрено. Порядок ДЭГ, касающийся выборов в Москве, предусматривает правило «бумажного следа»: при получении доступа к бюллетеню аппаратными средствами ДЭГ происходит распечатывание информации об этом в помещении УИК ДЭГ, информация также отображается на «ноде наблюдателя»; после подачи голоса происходит распечатка зашифрованной информации об анонимизированном волеизъявлении.

Согласно международным стандартам честных выборов, подсчет голосов должен быть воспроизводимым. В нормативном регулировании необходимо предусмотреть возможность получить убедительные доказательства того, что процедура подсчета была проведена честно, в том числе посредством независимого пересчета. Поэтому правило «бумажного следа» нужно сделать обязательным. В ином случае проверить правильность учета и подсчета голосов в системе ДЭГ путем ручного пересчета невозможно.

Кроме того, в порядке ДЭГ можно было бы предусмотреть, что в момент подачи зашифрованного голоса избиратель получает от системы ДЭГ подтверждение (например, в виде хеш-суммы¹⁷), которое содержит информацию о том, что зашифрованный голос попал в блокчейн системы ДЭГ и остается там в неизменном виде. В дальнейшем связь между этим «электронным следом» и аккаунтом избирателя сохраняется до начала подсчета голосов. И если голос подвергся изменению (а в этом случае изменяется хеш-сумма), то избиратель незамедлительно ставится об этом в известность.

Согласно международным актам по наблюдению за ДЭГ, система электронного голосования может быть введена только в том случае, если избиратели доверяют своей избирательной системе в целом. Как отмечалось ранее, все проблемы и вытекающие из них риски в совокупности создают проблему недоверия избирателей к ДЭГ, соответственно, успехи по системному решению всех поставленных проблем и снижение их рисков будет

¹⁷ Статья «Хэш-сумма». Википедия // <https://ru.wikipedia.org/wiki/Хэш-сумма> (дата обращения: 11.01.2022).

способствовать повышению доверия избирателей к данной системе. Одной из важных мер в этом направлении является просвещение избирателей относительно того, как устроена система ДЭГ и как она функционирует. Надо позитивно оценить усилия ЦИК России, которая на своем сайте¹⁸ опубликовала обучающие видеоролики об устройстве системы ДЭГ, об алгоритме голосования и так далее.

* * *

Таким образом, у российской системы ДЭГ есть большой потенциал для завоевания доверия у россиян. Выявленные в исследовании преимущества ДЭГ (удобство и доступность, экономичность и быстрота получения результатов, рост явки и привлечение молодых избирателей) стимулируют избирательные органы разных стран, включая Россию, внедрять эту форму голосования в практику выборов. В то же время, применяя ДЭГ, необходимо учитывать связанные с ним риски для достоверного волеизъявления избирателей. Ряд предложений по снижению вероятности фальсификаций изложен в настоящем исследовании. Некоторые из них дискуссионны и требуют дополнительного осмысления. Вместе с тем, исследование показало необходимость принятия системных законодательных мер по совершенствованию правовой защиты результатов волеизъявления избирателей при применении ДЭГ, которые наряду с мерами, уже предпринятыми законодателем и Центральной избирательной комиссией Российской Федерации, будут способствовать повышению доверия граждан к этому развивающемуся институту избирательного права.

Список литературы

1. Григорьев А.В. Реализация конституционного права граждан на управление делами государства в условиях цифровизации // Журнал российского права. 2020. № 2.
2. Постников А.Е. Конституционная модель политической системы России в условиях развития «цифрового общества» // Журнал российского права. 2020. № 5.
3. Мостовая М.Ю. Электронная демократия в избирательной системе Украины: долгожданная реальность или утопия? // Вісник Маріупольського Державного Університету, серія: Право. 2013. Вип. 5.
4. Турищева Н.Ю. Активное избирательное право: развитие форм реализации // Журнал российского права. 2021. № 6.
5. Худолей Д.М. Электронное голосование — необходимость для цифровизации избирательного процесса Российской Федерации // <https://cyberleninka>.

¹⁸ Дистанционное электронное голосование. Сайт ЦИК [Электронный ресурс] // <http://www.cikrf.ru/analogue/ediny-den-golosovaniya-2021/distantcionnoe-elektronnoe-golosovanie/> (дата обращения: 11.01.2022).

- ru/article/n/elektronnoe-golosovanie-neobhodimost-dlya-tsifrovizatsii-izbiratel'nogo-protssessa-rossiyskoy-federatsii (дата обращения: 03.12.2021).
6. Босова Е.Н., Реут Д.А. Дистанционное электронное голосование: поиск законодательного оформления // *Law Enforcement Review* 2019, vol. 3, no. 3.
 7. Совместный отчет Венецианской Комиссии и Дирекции по информационному обществу и противодействию преступности Генеральной Дирекции по правам человека и верховенству права (DGI) «О цифровых технологиях и выборах» (одобрен Советом по демократическим выборам на 65-м заседании, Венеция, 20.06.2019, Венецианской комиссией на 119-й пленарной сессии, Венеция, 21–22.06.2019) // [https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD\(2019\)016-e](https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2019)016-e) (дата обращения: 11.01.2022).
 8. E-Voting Map 2015 (Атлас электронного голосования в 2015 году – перевод автора) [Электронный ресурс] // https://www.e-voting.cc/wp-content/uploads/2012/03/e-voting_worldmap_2015.pdf (дата обращения: 11.01.2022).
 9. Красинский В.В. О проблемах почтового голосования на выборах в зарубежных странах // *Журнал российского права*. 2008. № 12.
 10. Павлушкин А.В., Постников А.Е. Правовой механизм дистанционного электронного голосования (анализ возможной модели) // *Журнал российского права*. 2009. № 11.
 11. Пескова О.Ю., Половко И.Ю., Фатеева С.В. Обзор подходов к организации электронного голосования // *Научно-технический и прикладной журнал «Известия ЮФУ. Технические науки»*. 2014. № 2.
 12. Колюшин Е.И. Избирательная реформа 2020 года в свете принципов избирательного права // *Конституционное и муниципальное право*. 2020. № 12.
 13. Колюшин Е.И. Правовые проблемы дистанционного электронного голосования избирателей // *Конституционное и муниципальное право*. 2020. № 2.
 14. Фирсова С.А., Вдовин П.С., Карпушкина И.С. Применение технологии блокчейн для дистанционного голосования // <https://cyberleninka.ru/article/n/primenenie-tehnologii-blokcheyn-dlya-distantsionnogo-golosovaniya> (дата обращения: 24.09.2021).
 15. Отчет Европейской Комиссии за демократию через право (Венецианская Комиссия) «О совместимости удаленного голосования и электронного голосования с стандартами Совета Европы» (принят Венецианской комиссией на 58-й пленарной сессии, Венеция, 12–13 марта 2004 г.) // [https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD\(2004\)012-e](https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2004)012-e) (дата обращения: 11.01.2022).
 16. Кравченко О.А. Понятие и основания классификации искажений волеизъявления народа при голосовании // *Актуальные проблемы российского права*. 2018. № 9.
 17. Парамонов Д.О., Кириченко В.В. Методы фальсификации выборов. М.: Южно-Росс. ин-т информ. технологий, 2003.
 18. Скрипкина Ж.Б. Избирательные системы и технологии. М., 2006.
 19. Фурса Е.А. Подпись избирателя: векторы эволюции понятия и принципы правовой охраны // *Государственная власть и местное самоуправление*. 2019. № 4.
 20. Титовская А.В. Электронное тайное голосование в России и за рубежом: сравнительно-правовой анализ // *Юридическая наука*. 2012. № 4.

21. Kersting N. Online-Wahlen im internationalen Vergleich // Aus Politik und Zeitgeschichte. — Bonn, 2004. — Bd.18. (Керстинг Н. Сравнительный анализ выборов с использованием интернета).
22. Руководство по наблюдению за использованием новых технологий голосования (БДИПЧ — Бюро ОБСЕ по демократическим институтам и правам человека). — Warsaw, 2013. — 96 с. Сайт ОБСЕ [Электронный ресурс] // <https://www.osce.org/ru/odihr/elections/107771> (дата обращения: 24.12.2021).
23. Леви Д.А. Институт выборов: перспективы развития в эпоху информационных технологий // Азимут научных исследований: экономика и управление. 2015. № 2 (11).
24. Цаплин А.Ю. Перспективы дистанционного электронного голосования в России // Изв. Саратов. ун-та. Нов. сер. Сер. Социология. Политология. 2016. Т. 6. Вып. 3.
25. Гриценко Е.В. Обеспечение основных гарантий избирательных прав в условиях информатизации избирательного процесса // Конституционное и муниципальное право. 2020. № 5.
26. Савченко М.С., Кадлец В.А. Правовое регулирование и практика электронного голосования в зарубежных странах // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2016. № 117.
27. Шульга-Морская Т.В. Электронное голосование: опыт и перспективы Швейцарии и России // Адвокат. 2013. № 3.