ВСЕРОССИЙСКИЙ КОНКУРС НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ И ТВОРЧЕСКИХ РАБОТ МОЛОДЕЖИ

«Меня оценят в XXI веке»

Направление: право

Тема: «Цифровая урна под ударом: как защитить честность выборов от новых технологий манипуляций»

Соискатель: Пономарева Полина Вадимовна ученица 11 класса
МБОУ «Великомихайловская СОШ им. Г.Т. Ильченко»

Научный руководитель: учитель истории и обществознания
Песоцкая Алина Васильевна

Место выполнения работы: с. Великомихайловка

2026

Содержание

Введение……...3
История и практика электронного голосования в России…….5
Перспективы развития электронного голосования в Российской Федерации……7
Технология блокчейн как основа безопасности электронных выборов……..9
Современные технологические угрозы для систем электронного голосования……..….10
Меры по обеспечению конфиденциальности и анонимности избирателей…….….12
Роль наблюдателей и членов избиркома в процессе электронного голосования……..…14
Скептицизм общества: причины сомнений в честности электронных выборов……...14
Рекомендации по улучшению систем электронной демократии на базе анализа текущих практик.....16
Заключение…….18
Список литературы……....19

Введение

Актуальность. В последние годы электронное голосование приобрело значительную популярность как инструмент повышения доступности и удобства избирательного процесса. В России внедрение таких систем на федеральном уровне стало возможным благодаря накопленному опыту, особенно на примере столицы -Москвы. Использование новых технологий, включая блокчейн, предполагает не только ускорение голосования, но и повышение прозрачности и безопасности данных. Однако вместе с преимуществами возникает ряд вызовов, связанных с обеспечением честности выборов.

Обеспечение безопасности и конфиденциальности в условиях цифровизации голосования требует детального анализа применяемых технологий и сценариев угроз. В частности, вопросы анонимности избирателей и защиты результатов от возможных манипуляций остаются критическими. Современные кибератаки и внутренние риски, такие как утечки личных данных, вмешательство в программное обеспечение систем голосования или попытки подделки результатов, ставят под сомнение доверие к электронным процедурам. Это подчеркивает необходимость разработки комплексных мер защиты и контроля за процессом голосования.

Цель: разработать комплексный подход к обеспечению честности выборов при применении электронного голосования в условиях современных технологических угроз.

Задачи:

1. Изучить опыт внедрения электронного голосования в Москве и на федеральном уровне;
2. Проанализировать технологии блокчейн и их роль в обеспечении безопасности выборов;
3. Исследовать потенциальные технологические угрозы для электронного голосования;
4. Разработать рекомендации по повышению защиты данных и сохранению анонимности избирателей;
5. Предложить меры прозрачности и контроля процесса голосования;
6. Оценить эффективность предложенных рекомендаций на примере текущих практик

Проблема: современные технологии создают новые риски для честности выборов, связанные с возможными утечками данных, нарушениями анонимности избирателей и вмешательством в процесс голосования. Необходимы эффективные методы для обеспечения безопасности и доверия к электронному голосованию.

Идея: Использовать опыт российских региональных выборов с применением блокчейн-технологий для создания безопасной, прозрачной и надежной системы электронного голосования, которая эффективно противодействует современным технологическим угрозам.

Продукт: исследовательский отчет с анализом технологий электронной демократии и рекомендациями по обеспечению честности выборов при электронном голосовании

В рамках работы будет проанализирован опыт внедрения электронного голосования в Москве и на федеральном уровне, с акцентом на используемые технические решения и организационные механизмы. Особое внимание уделяется технологии блокчейн, которая посредством своей децентрализованной архитектуры способна повысить устойчивость и прозрачность голосования. Проанализируются основные свойства блокчейна, такие как неизменяемость и распределенность данных, а также их влияние на минимизацию традиционных рисков в выборах.

Далее исследуются существующие технологические угрозы -как внешние, так и внутренние. К ним относятся кибератаки, уязвимости в программном обеспечении, возможности вмешательства третьих лиц, а также риски утечки и реидентификации данных избирателей. Рассматриваются способы, применяемые для защиты систем, включая шифрование, многофакторную аутентификацию, средства обнаружения аномалий и процедурную организацию процесса голосования. Анализируются также риски, связанные с социальными и техническими аспектами, затрагивающими доверие общества к электронным выборам.

Особое место занимает рассмотрение мер по сохранению анонимности голосующих и гарантированию конфиденциальности данных. Будут обсуждены методы криптографической защиты, включая использование смешивания и подтверждений с нулевым разглашением, направленные на предотвращение связывания конкретного голоса с личностью избирателя. Рассматриваются способы обеспечения прозрачности для наблюдателей и членов избирательной комиссии, а также инструменты контроля, позволяющие обнаружить и предотвратить попытки мошенничества.

Настроения и восприятие общественностью честности электронных выборов также станут предметом исследования. Скептицизм и недоверие могут возникать вследствие отсутствия прозрачности или недостатка разъяснительной работы, поэтому будут проанализированы причины таких настроений и предложены пути повышения доверия через открытость процессов и информирование граждан.

В заключительной части работы будут выработаны рекомендации по совершенствованию систем электронного голосования с учетом выявленных проблем и возможностей современных технологий. Оценка эффективности данных мер будет проведена на основе текущих практик, включающих опыт Москвы и пилотных проектов на федеральном уровне. Отдельное внимание уделено перспективам развития электронной демократии в России с целью создания более безопасных, прозрачных и доступных выборов в будущем.

1. История и практика электронного голосования в России

Первые шаги в развитии электронного голосования в России были сделаны еще в 1996 году, когда началась работа по внедрению цифровых технологий в избирательные процессы. В течение последующих десятилетий система прошла через несколько этапов, каждый из которых характеризовался разным уровнем технологической оснащенности и законодательного регулирования. Переход к дистанционному электронному голосованию (ДЭГ) стал важным вехой, расширившим возможности граждан участвовать в выборах без необходимости посещения избирательных участков [3].

Москва сыграла роль лидера и своего рода «лаборатории» для внедрения дистанционного голосования в России. В 2019 году на выборах в Московскую городскую Думу был проведен первый масштабный эксперимент с использованием ДЭГ. Для этого были приняты федеральный и столичный законы, закрепляющие правовые основы дистанционного голосования. Разработка и сопровождение системы возлагались на Департамент информационных технологий мэрии Москвы, а сам процесс голосования осуществлялся через официальный портал mos.ru. Перед выборной кампанией платформа прошла четыре поэтапных тестирования, что обеспечило возможность выявления и устранения технических неполадок заранее [10].

В России проведение ДЭГ регламентируется Федеральным законом от 12 июня 2002 года №67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации». Закон признает дистанционное электронное голосование разновидностью электронного голосования, регулирует процедуру регистрации избирателей и подсчет голосов, а также Постановлением ЦИК РФ от 3 июля 2024 года №175/1389-8 «О Порядке электронного голосования на выборах и референдумах, проводимых в Российской Федерации». Постановление определяет порядок проведения ДЭГ, включая использование комплексов для электронного голосования (КЭГ).

Участие в электронном голосовании было доступно избирателям с постоянной регистрацией в Москве, при условии создания на портале полной учетной записи. При этом сохранялась возможность проголосовать традиционным способом на избирательных участках, что способствовало постепенному и добровольному переходу к новым технологиям. В первое испытание на выборах 2019 года около 10% участников воспользовались дистанционным голосованием, что относительно невысоко, но уже показало потенциал для развития. К 2023 году доля таких избирателей на выборах мэра Москвы выросла до 81%, чему способствовали как широкое распространение цифровых сервисов, так и многократные улучшения и оптимизация работы системы [12].

За пределами Москвы развитие электронного голосования происходило более постепенно. К 2020 году дистанционное голосование было задействовано и на федеральных выборах, например, на голосовании по поправкам в Конституцию, где зарегистрировалось свыше миллиона участников из Москвы. Такой масштабный опыт позволил закрепить технологические и организационные подходы, необходимы для проведения электронных выборов на уровне всей страны [20].

Несмотря на значительный прогресс, опыт московского ДЭГ выявил ряд проблем, связанных с обеспечением доверия к процессу. В частности, отсутствие доступа наблюдателей к ключам расшифровки голосов и программному коду системы вызвало вопросы относительно прозрачности и неподкупности результатов. Эти вопросы актуальны в контексте общественного восприятия новых технологий – часть избирателей и экспертов выражают

опасения по поводу возможных угроз безопасности и манипуляций, что требует повышения уровня открытости и доступности информации о работе систем голосования [12].

Таким образом, история и практика электронного голосования в России, на примере Москвы, отображают эволюцию восприятия цифровых технологий в избирательном процессе: от начальной осторожности к более широкой адаптации и массовому использованию. Для дальнейшего развития и распространения электронного голосования на федеральном уровне необходимо усилить меры по повышению доверия граждан к этим технологиям, включая улучшение прозрачности и взаимодействия с обществом.



Рисунок 1 История и практика электронного голосования в России с акцентом на опыт московских выборов

2. Перспективы развития электронного голосования в Российской Федерации

Перспективы развития электронного голосования в Российской Федерации зависят от динамичной интеграции законодательных, технологических и социальных факторов. Уже сегодня заметна активная работа по укреплению правовой базы, начиная с 2005 года, что создает надежную основу для масштабного внедрения электронных форм голосования. Государственные институты, включая Министерство цифрового развития и Центральную избирательную комиссию, активно способствуют развитию дистанционного электронного голосования, что подтверждается планами распространения данной технологии на все регионы к президентским выборам 2024 года [16].

Стремительное развитие инноваций в области криптографии, в частности методов защиты данных и анонимизации избирателей, создает дополнительные возможности для повышения безопасности и доверия к системам электронного голосования. Улучшение криптографических алгоритмов, основанных на современных протоколах, а также внедрение новых решений, способных противостоять возникающим угрозам, обеспечат надежность и устойчивость голосования в цифровой среде без необходимости раскрытия частной информации избирателей [15].

Растущая цифровая грамотность населения, особенно среди молодежи, расширяет поле применения электронных технологий в избирательных процедурах. По данным опросов, большинство российских граждан поддерживают идею онлайн-голосования, а значительная часть готова использовать электронные подписи и участвовать в дистанционном голосовании, что создает благоприятные социальные предпосылки для устойчивого развития электронной демократии [5]. Повышение доверия к цифровым избирательным форматам возможно через систематизацию образовательных программ и информационных кампаний, направленных на формирование критически осознанного отношения к новым технологиям.

Успешные региональные проекты, применяющие блокчейн и другие инновационные технологии, демонстрируют действенные модели, которые могут служить ориентиром для расширения практики на федеральном уровне. В то же время адаптивность и гибкость систем, а также способность быстро реагировать на новые вызовы, остаются ключевыми требованиями для эффективного функционирования электронного голосования в изменяющейся технологической и социокультурной среде [20].

Исходя из представленных трендов, можно сделать вывод, что дальнейшее развитие электронного голосования должно опираться на комплексный и поэтапный подход, сочетающий совершенствование законодательного регулирования, внедрение передовых криптографических методов и расширение цифровой грамотности населения. Только такая многоуровневая и адаптивная стратегия позволит создать надежную, безопасную и широко доступную систему электронной демократии, способную отвечать современным требованиям и вызовам.



Рисунок 1 -История и практика электронного голосования в России с акцентом на опыт московских выборов

3. Технология блокчейн как основа безопасности электронных выборов

Блокчейн представляет собой распределенный реестр, организованный в виде цепочки блоков, каждый из которых хранит информацию о совершенных транзакциях или событиях. Эти блоки связаны между собой с помощью криптографических методов, что обеспечивает целостность данных и невозможность их последующего изменения без согласия участников сети. Такая архитектура исключает наличие единого центра управления, что критически снижает риски подделки или утраты информации [3].

Принцип децентрализации -ключевой элемент технологии блокчейн, позволяющий хранить данные одновременно на множестве независимых узлов. В контексте избирательных процедур это означает, что информация о каждом голосе не контролируется одной организацией, а распространяется по всей сети. Такая система существенно усложняет попытки вмешательства в ход выборов, поскольку злоумышленникам необходимо скомпрометировать подавляющее большинство узлов для внесения изменений, что практически невыполнимо [4].

Защита данных обеспечивается внедрением современных методов криптографии, в том числе цифровых подписей и шифрования голосов. Каждый избиратель аутентифицируется посредством цифрового ключа, обеспечивающего однозначное подтверждение личности без раскрытия ее данных. После того как голос зашифрован, он отправляется в сеть, где проверяется валидаторами -участниками блокчейн-системы, обладающими полномочиями на подтверждение подлинности и исключение повторного голосования. Это гарантирует как конфиденциальность, так и уникальность каждого избирательного действия [2].

Неизменность информации -еще одно важное свойство блокчейна, критически важное для выборов. После записи блока в цепочку данные практически нельзя изменить без обнаружения, поскольку это потребовало бы пересчета всех последующих блоков и согласования с большинством узлов распределенной сети. Данная особенность обеспечивает прозрачность и прослеживаемость результатов голосования, позволяя любому участнику подтвердить правильность подсчета и исключить сомнения в подделках [4].

Использование цифровых кошельков, представляющих собой адреса, связанных с кандидатами и партиями, обеспечивает удобный и защищенный механизм передачи голосов. Избиратели анонимно передают свои «электронные монеты» в пользу выбранных участников, исключая возможность идентификации конкретного лица по конкретному голосу и предотвращая манипуляции с бюллетенями [16].

В международной практике блокчейн-технология уже доказала свою эффективность в проектах избирательного характера, позволяя повысить уровень доверия граждан к демократии, уменьшить количество фальсификаций и обеспечить прозрачность выборов. Интеграция распределенного реестра и криптографических методов в избирательные процессы отвечает современным требованиям к безопасности и конфиденциальности данных, что особенно важно в условиях растущих технологических угроз [4].

Для борьбы с фальсификациями и повышения доверия общества к избирательной системе внедрение блокчейн-технологий становится необходимым шагом. Это позволяет создать устойчивую, прозрачную и защищенную платформу для электронного голосования, минимизируя риски манипуляций и обеспечивая сохранность избирательных прав каждого гражданина.

4. Современные технологические угрозы для систем электронного голосования

Одним из ключевых вызовов для систем электронного голосования остаются современные технологические угрозы, способные существенно повлиять на целостность и доверие к избирательному процессу. Как уже отмечалось в предыдущем разделе, безопасность алгоритмов и прозрачность процедур являются фундаментальными для обеспечения честности выборов; тем не менее, именно цифровые риски создают дополнительные сложности для их реализации в дистанционном электронном голосовании (ДЭГ).

Основные угрозы связаны с возможностью взломов и манипуляций систем. В частности, практика показала, что существует риск двойного голосования -когда один пользователь получает возможность отдать более одного голоса, нарушая равенство избирателей и подрывая легитимность результатов. Нарушения целостности данных могут происходить не только технически, но и юридически, ведь правовая база пока не полностью адаптирована к многообразию цифровых угроз, что осложняет защиту избирательных данных и контроль за процедурами [20].

Угрозу представляет и так называемая идентификация голосующих по устройствам или IP-адресам -такие данные могут раскрыть тайну голосования и привести к компрометации конфиденциальности. Это особенно критично в случаях, когда участие в голосовании связано с личной или общественной безопасностью избирателей. Кроме того, дистанционный характер голосования затрудняет подтверждение искренности и свободного волеизъявления избирателей, что порождает риски манипуляций и давления, включая продажу голосов [8].

Утечки и кражи персональных данных создают дополнительные репутационные и практические угрозы. Потеря контроля над информацией может не только нарушить конфиденциальность, но и привести к мошенничеству, фальсификациям и искажению результатов. Последствия таких утечек затрагивают не только отдельных граждан, но и подрывают доверие к институту выборов в целом, снижая легитимность политических процессов и создавая предпосылки для общественных протестов и сомнений в психологической безопасности избирателей [6].

Рассматривая угрозы комплексно, следует отметить, что дистанционное электронное голосование требует особого подхода к обеспечению безопасности, учитывающего специфику цифрового пространства. Возрастающая сложность сетевых атак, наличие внутренних и внешних угроз со стороны злоумышленников делает систему уязвимой без постоянного мониторинга и своевременного реагирования. Кроме того, отсутствие достаточного количества общественных наблюдателей или прозрачных механизмов аудита затрудняет выявление и нейтрализацию подозрительных действий [20].

Для повышения устойчивости систем необходима интеграция комплексных мер. Предложения включают внедрение механизмов многократного изменения выбора с фиксацией только последнего варианта, что способствовало бы устранению риска продажи голосов и принудительных манипуляций. Общественное наблюдение и расширение доступа экспертов к процедурам голосования повышают прозрачность и формируют доверие общества. Кроме того, необходимость координации между техническими специалистами, государственными органами и гражданским обществом становится очевидной для комплексного обеспечения кибербезопасности и устойчивости выборов [20].

Таким образом, технологические угрозы для электронных систем голосования не только потенциально ставят под сомнение анонимность и достоверность избирательных данных, но и несут риски утраты общественного доверия к избирательным процедурам. Это

подчеркивает необходимость системного подхода к защите -как технического, так и организационного -с и использованием современных интеллектуальных механизмов контроля и аудита. Только такой комплексный подход позволит нивелировать существующие угрозы и обеспечить честность выборов в эпоху цифровизации.

5. Меры по обеспечению конфиденциальности и анонимности избирателей

Приватность избирателей является фундаментальным элементом построения доверия к любой системе электронного голосования. Обеспечение конфиденциальности во многом определяет готовность граждан участвовать в выборах через цифровые платформы, поскольку гарантия сохранности их выбора и личных данных снижает риски давления и манипуляций. В связи с этим конфиденциальность и анонимность необходимы для укрепления легитимности и устойчивости избирательных процессов в условиях цифровизации.

Для сохранения анонимности участников применяются специализированные технические решения, выходящие за рамки базовой криптографии блокчейна. Важным элементом является использование анонимайзеров -механизмов, которые позволяют обезличивать пользователей в момент голосования, создавая так называемую «анонимную зону». В этом режиме идентификация личности избирателя отвязывается от конкретных действий с электронным бюллетенем или IP-адресом, что предотвращает связывание гражданина с конкретным голосом. Однако в отечественной практике голосование через портал Госуслуг требует обязательной авторизации, что снижает уровень анонимности из-за возможности отслеживания через IP-адреса и учетные записи пользователей [15].

Именно баланс между прозрачностью системы и приватностью избирателей выступает сложной задачей. С одной стороны, избиратели и общественные контролеры требуют открытости и прослеживаемости результатов -чтобы убедиться в честности подсчета голосов и отсутствии фальсификаций[3]. С другой стороны, обеспечение полной анонимности исключает возможность идентификации выбранного варианта конкретным человеком, что критично для соблюдения основополагающего принципа тайны голосования. Решения, направленные на усиление прозрачности, могут непреднамеренно снижать уровень приватности, создавая потенциальные риски раскрытия личности. Поэтому система должна находить оптимальный компромисс, используя технические меры и процедурные барьеры, чтобы минимизировать возможность дезанонимизации без ущерба для проверки результатов [6].

Среди организационных мер в российской практике ключевое значение имеет проведение независимого аудита процесса голосования и систем защиты персональных данных. Такие проверки выполняют внешние общественные институты и эксперты, что добавляет уверенности в отсутствии ошибок, фальсификаций или атак на информационные ресурсы. Важно, что эти мероприятия происходят независимо от администраций, управляющих системами электронного голосования, что исключает конфликт интересов и повышает уровень доверия со стороны избирателей и общественности [6].

Кроме того, законодательство устанавливает основные рамки для защиты анонимности. Федеральный закон № 60-ФЗ от 14 марта 2022 года регламентирует применение дистанционного электронного голосования, предусматривая меры по обеспечению тайны голосования. Вместе с тем, абсолютная анонимность в определенных ситуациях остается недостижимой, например при оказании избирателям законодательно установленной помощи. Таким образом, тайна голосования часто носит относительный характер, требующий от системы учета и контроля всеобъемлющих мер защиты [20].

Постоянный мониторинг соответствия установленным стандартам конфиденциальности и анонимности становится обязательным условием дальнейшего развития электронного голосования. Новые технологические решения и обновления программного обеспечения должны проходить регулярную проверку на предмет уязвимостей

и риска утечки данных. Такой подход позволяет своевременно реагировать на появляющиеся угрозы и совершенствовать механизмы защиты, что в итоге способствует сохранению баланса между прозрачностью системы и приватностью пользователей, а также поддержанию высокого уровня доверия к электронным выборам.

В итоге, обеспечение конфиденциальности и анонимности в электронном голосовании требует сочетания современных технических средств, независимого аудита и продуманной нормативной базы. Только комплексный и системный подход создает условия для честного, прозрачного и одновременно приватного голосования, гарантирующего право граждан на тайну своего выбора в цифровую эпоху [15].

6. Роль наблюдателей и членов избиркома в процессе электронного голосования

Социальный контроль выступает важнейшим элементом обеспечения прозрачности и доверия к выборам, включая дистанционное электронное голосование. Несмотря на высокий уровень технической защиты, роль человеческого фактора в надзоре за избирательным процессом остается незаменимой. Наблюдатели и представители избирательных комиссий выполняют функции, которые не могут быть полностью автоматизированы или переданы системам, обеспечивая дополнительный уровень контроля и проверок.

Наблюдатели на выборах обладают правом присутствовать на ключевых этапах голосования, фиксировать ход процедур и оказывать влияние на соблюдение избирательного законодательства. Их присутствие в помещениях для наблюдения и возможность анализировать данные, предоставляемые программно-техническими комплексами, позволяет выявлять потенциальные нарушения и создавать атмосферу прозрачности [17].Ограничения, связанные с дистанционным форматом голосования, усложняют контроль, однако своевременная организация рабочих мест для наблюдателей, например, в Общественной палате РФ, частично компенсирует эти вызовы, предоставляя возможность наблюдать за процессом в режиме реального времени [1].

Избирательные комиссии, как территориальные, так и участковые, отвечают за организацию и проведение голосования, а также взаимодействие с наблюдателями. Они регистрируют наблюдателей, обеспечивают доступ к рабочим зонам и способствуют выполнению их функций[23]. Участие членов комиссий поддерживает стабильность работы системы и соблюдение нормативных требований, особенно в частях процедуры, которые невозможно передать цифровым механизмам. Важнейшая задача комиссий -обеспечить не только техническую корректность, но и законность всего процесса, что требует внимательного и компетентного человеческого участия [20].

Влияние человеческого фактора на восприятие честности выборов также проявляется в эмоциональном и психологическом аспектах. Граждане зачастую больше доверяют процессу, когда видят присутствие представителей разных политических сил и общественных организаций, что создает ощущение общественного контроля и возможности оперативного реагирования на нарушения. Отсутствие или символическое участие наблюдателей может вызвать подозрения и подорвать доверие даже к технически надежной системе голосования [20].

Более того, социальный контроль способствует формированию коллективной ответственности за результаты выборов и укреплению демократических институтов. Объединение усилий технических систем с деятельностью наблюдателей и членов комиссий создает многоуровневую модель контроля, где минимизируются риски злоупотреблений и повышается открытость процедур. Интеграция этих элементов обеспечивает возможность не только выявлять и предотвращать инциденты, но и формировать отчеты, которые служат доказательной базой при рассмотрении спорных ситуаций.

Таким образом, несмотря на развитие сложных технических инструментов электронной демократии, интеграция человеческого фактора остается неотъемлемой частью обеспечения честности и прозрачности выборов. Роль наблюдателей и избирательных комиссий нельзя заменить алгоритмами и программными комплексами -их функции дополняют друг друга. Без социального контроля даже самая продвинутая технологическая система лишается критического элемента доверия, который способен поддержать легитимность избирательного процесса в глазах общества [19].

7. Скептицизм общества: причины сомнений в честности электронных выборов

После рассмотрения роли наблюдателей и членов избирательных комиссий важно отметить, что общественное мнение об электронном голосовании в России и других странах демонстрирует значительное разнообразие и неоднозначность[19]. Около половины граждан поддерживают расширение возможностей дистанционного голосования, отмечая его потенциал для повышения доступности и вовлеченности избирателей. Вместе с тем, существенная часть населения выражает сомнения и опасения, связанные с недостаточной прозрачностью процедур и возможностью фальсификаций[9]. Такие настроения находят отражение в социальных медиа и политических дискуссиях, которые часто демонстрируют смешанную или критическую тональность в отношении электронных избирательных технологий [14].

Психологический аспект недоверия к электронному голосованию во многом обусловлен чувством неопределенности, возникающим при взаимодействии с новыми технологиями. Многие избиратели испытывают трудности при восприятии цифровых процедур, что подпитывается страхом потерять контроль над процессом, опасениями утраты приватности и возможного вмешательства в выборы. [11]. Отсутствие физических бюллетеней и привычных процедур голосования усиливает чувство дистанцированности и недостаточности официальной информации. В этом контексте значительную роль играют слухи, домыслы и теории заговора, которые активизируются в условиях информационного шума и недостаточного разъяснения со стороны официальных источников [19].

Кроме того, скептицизм подпитывается низким уровнем доверия к государственным институтам и цифровым сервисам в целом. [18]. Это особенно заметно в странах с историей электоральных споров и политической нестабильности, где электронные системы воспринимаются либо как технически сложные «черные ящики», либо как инструменты, способные усиливать существующие злоупотребления. Общественное восприятие эффективности и честности электронного голосования напрямую зависит от прозрачности коммуникации и возможностей граждан получить объективную и доступную информацию о механизмах и гарантиях системы [14].

В социальных сетях, таких как YouTube, представители различных политических позиций и общественные деятели выражают как поддержку, так и критику электронного голосования. Противники системы акцентируют внимание на рисках кибератак и возможности искажения результатов, уподобляя электронное голосование играм азартного характера. Сторонники же отмечают рост явки и удобство технологии, выступая за ее дальнейшее совершенствование и широкое внедрение. Такая поляризация отражает общий тренд -пока электронное голосование остается процессом, вызывающим и надежды, и серьезные сомнения [14].

Обоснованным ответом на существующий скептицизм становится повышение уровня информированности общества. По мере распространения дистанционных форм голосования усилия по просвещению избирателей через открытые коммуникации, разъяснительные кампании и диалог на цифровых платформах способны снизить страхи и барьеры восприятия. Более того, вовлечение граждан в обсуждение технологий, их возможностей и ограничений помогает формировать критически осознанное отношение и укреплять доверие. Только через систематическую работу с общественным мнением можно обеспечить не только техническую безопасность, но и социальную легитимность электронного голосования в будущем.

8. Рекомендации по улучшению систем электронной демократии на базе анализа текущих практик

Анализ общественного мнения и опыта внедрения электронного голосования подтверждает наличие значительных вызовов, связанных с обеспечением доверия, сохранением тайны голосования и защитой от технологических угроз. Для повышения качества электронной демократии необходимо последовательно внедрять меры, способные снизить риски и одновременно обеспечить максимальную анонимность и прозрачность избирательного процесса[26].

Во-первых, необходимо разработать и принять комплексное законодательство, которое четко сформулирует правовые гарантии соблюдения конституционных принципов: всеобщности, равенства, прямоты и тайны голосования. Такой нормативный базис должен предусматривать обязательное проведение пилотных проектов с различными техническими решениями и механизмами защиты, что позволит оценить эффективность и устойчивость систем в реальных условиях перед масштабным применением [17].

Важнейшим направлением является создание единой интегрированной платформы для электронного голосования, реализующей стандартизированные процессы аутентификации, шифрования и подсчета голосов. [7].Такая система должна поддерживать использование современных криптографических протоколов, минимизирующих риски реидентификации избирателей, а также обеспечивать защиту от кибератак и попыток вмешательства. При этом архитектура платформы должна допускать горизонтальное масштабирование и взаимодействие со сторонними аудиторами и наблюдателями без раскрытия личных данных [19]

Закрепление на законодательном уровне института общественного контроля за дистанционным электронным голосованием создаст дополнительный канал прозрачности. Это предусматривает предоставление наблюдателям и экспертам доступа к процессам аудита, техническим журналам и результатам независимых проверок. Внедрение системы открытых отчетов и открытого программного кода, где это возможно, повысит уровень доверия общества и позволит своевременно выявлять уязвимости [18].

Также необходимо развивать образовательные программы и информационные кампании, направленные на повышение цифровой грамотности населения и формирование объективного восприятия электронной демократии. Предоставление доступных и понятных материалов о работе систем, их преимуществах и мерах защиты позволит снизить страхи и скептицизм, а также повысить гражданскую активность через дистанционные формы голосования [7].

Для снижения технологических рисков при сохранении анонимности предложено использовать механизмы мультифакторной аутентификации с применением электронных идентификаторов, не позволяющих напрямую связывать личность с голосом. Также перспективно внедрение протоколов с доказательствами с нулевым разглашением (zero-knowledge proofs), обеспечивающих проверку корректности подсчета без раскрытия содержания отдельных голосов [19].

Направления будущих научных исследований охватывают вопросы разработки устойчивых к квантовым атакам криптографических алгоритмов, моделирования комплексных сценариев угроз и взаимодействия технических систем с правовыми и социальными институтами[18]. Особое внимание заслуживает изучение психологии доверия

к электронным технологиям и способов интеграции обратной связи от граждан в процессы непрерывного улучшения систем голосования [18].

Таким образом, комплексный подход, объединяющий законодательные инициативы, технические инновации, общественный контроль и образовательные мероприятия, создаст основу для развития эффективной, прозрачной и безопасной системы электронной демократии, способной отвечать современным вызовам и ожиданиям общества.

Заключение

Проведенное исследование электронного голосования в России, основанное на анализе столичного опыта и федеральных инициатив, выявило комплекс проблем и возможностей, связанных с внедрением цифровых технологий в избирательный процесс. Рассмотренный материал продемонстрировал, что модель дистанционного электронного голосования, интегрированная с блокчейн-технологиями, обладает потенциалом для значительного повышения безопасности, прозрачности и доступности выборов. Децентрализованная архитектура блокчейна обеспечивает неизменность и надежность хранения данных, что существенно снижает риски манипуляций и обеспечивает доверие к результатам голосования.

Анализ технологических угроз выявил существующие уязвимости, связанные с возможностью утечек персональных данных, вмешательством в программное обеспечение и потенциальной компрометацией анонимности избирателей. Эти вызовы подчеркивают необходимость реализации комплексных мер защиты, в том числе современных криптографических методов, многофакторной аутентификации, а также процедурной прозрачности для предотвращения злоупотреблений. Роль человеческого фактора, представленная деятельностью наблюдателей и членов избирательных комиссий, остается критически важной для поддержания общественного контроля и укрепления легитимности процесса.

Общественные настроения вокруг электронного голосования демонстрируют значительный скептицизм, причиной которого служит недостаток информации, страхи перед новыми технологиями и недоверие к государственным институтам. Для повышения уровня доверия необходимы открытость систем, регулярные аудиты, активное информирование граждан и вовлечение экспертов и общества в процесс контроля. Только сочетание технического совершенствования и общественного взаимодействия способно обеспечить принятие электронного голосования как надежного института демократии.

На основе проведенного анализа сформулированы рекомендации, направленные на развитие российской системы электронной демократии. Важными направлениями являются совершенствование законодательной базы, создание интегрированных и масштабируемых платформ с применением современных криптографических протоколов, а также обеспечение институционализированного общественного контроля. Образовательные программы и информационные кампании необходимы для формирования цифровой компетентности населения и формирования критического и осознанного отношения к электронным избирательным системам.

В целом, результаты исследования подтверждают, что электронное голосование с использованием блокчейна при условии последовательного и системного развития технологий, нормативного регулирования и общественного взаимодействия может стать эффективным инструментом повышения качества и доверия к избирательным процессам в России. Применение комплексного подхода позволит минимизировать технологические угрозы, гарантировать анонимность избирателей и обеспечить максимальную прозрачность, что соответствует современным вызовам цифровой эпохи и требованиям устойчивого развития демократии.

Список литературы

Источники

1. Постановление ЦИК России от 08.06.2022 N 86/716-8 (ред. от 23.07.2025) «О Порядке дистанционного электронного голосования с использованием федеральных государственных информационных систем». – Доступ из справ.-правовой системы «КонсультантПлюс.

2. Федеральный закон от 12.06.2002 N 67-ФЗ (ред. от 29.12.2025) «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации»– Доступ из справ.-правовой системы «КонсультантПлюс.

Исследования

1. «Единая Россия» применяет технологию блокчейн для обеспечения и прозрачности выборов [Электронный ресурс]. – URL: https://nnov.er.ru/activity/news/edinaya-rossiya-primenyaet-tehnologiyu-blokchejn-dlya-obespecheniya-bezopasnosti-i-prozrachnosti-vyborov (дата обращения 5.09.2026)

2. Безопасные выборы: как гарантируют анонимность и прозрачность во время электронного голосования [Электронный ресурс]. – URL: https://svao.mos.ru/presscenter/news/detail/8954508.html (дата обращения 5.09.2026)

3. Блокчейн и голосование: прозрачность и безопасность выборов [Электронный ресурс]. – URL: https://www.block-chain24.com/articles/blokcheyn-i-golosovanie-prozrachnost-i-bezopasnost-vyborov (дата обращения 17.08.2026)

4. ВЦИОМ. Новости: Цифровое голосование в России: первые эксперименты и перспективы [Электронный ресурс]. – URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/czifrovoe-golosovanie-v-rossii-pervye-eksperimenty-i-perspektivy (дата обращения 17.08.2026)

5. Выборы и электронное голосование: насколько безопасно голосование через интернет [Электронный ресурс]. – URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/346188.php (дата обращения 8.09.2026)

6. Болтенкова, А.А. Совершенствование процедур электронного голосования [Электронный ресурс]. – URL: https://solncesvet.ru/tv/430067/ (дата обращения 18.01.2026)

7. Дистанционное электронное голосование: мониторинг [Электронный ресурс]. – URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/distancionnoe-ehlektronnoe-golosovanie-monitoring (дата обращения 28.08.2026)

8. Из эксперимента в базу: электронному голосованию в Москве испольнилось пять лет [Электронный ресурс]. – URL: https://www.mos.ru/news/item/141132073/ (дата обращения 28.08.2026)

9. К электронному голосованию https://www.rcoit.ru/upload/iblock/71f/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D0%B [Электронный ресурс]. – URL: E%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F%20%D0%BA%D1%83%D0%BB%D1%8C%D1%82%D1%83%D1%80%D0%B0%20%D0%BA%D0%B0%D0%BA%20%D1%84%D0%B0%D0%BA%D1%82%D0%BE%D1%80%20%D1%82%D1%80%D0%B0%D0%BD%D0%B7%D0%B8%D1%82%D0%B0%20%D0%BA%20%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%BE%D0%BC%D1%83.pdf (дата обращения 6.09.2026)

10. Как развивалось электронное голосование в Москве [Электронный ресурс]. – URL: https://regnum.ru/news/3908547 (дата обращения 6.09.2026)

11. Как технологии помогают сохранить анонимность и тайну голосования [Электронный ресурс]. – URL: https://moscow.er.ru/activity/news/kak-tehnologii-pomogayut-sohranit-anonimnost-i-tajnu-golosovaniya (дата обращения 6.09.2026)

12. Мертвые души, вбросы и дыры -кто и как в России критикует электронное голосование [Электронный ресурс]. – URL: https://rtvi.com/stories/mertvye-dushi-vbrosy-i-dyry-kto-i-kak-v-rossii-kritikuet-elektronnoe-golosovanie/ (дата обращения 4.09.2026)

13. Могут ли выборы через Госуслуги и по почте в России быть анонимными? [Электронный ресурс]. – URL: https://www.ural56.ru/news/645006 (дата обращения 19.02.2026)

14. Туманян, Г.В. Влияние блокчейн-технологий на избирательные институты в рамках «сервисной» модели государства и концепции партисипативного управления [Электронный ресурс]. – URL: https://www.rcoit.ru/upload/iblock/7a2/%D0%92%D0%BB%D0%B8%D1%8F%D0%BD%D0%B8%D0%B5%20%D0%B1%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD%20%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B9%20%D0%BD%D0%B0%20%D0%B8%D0%B7%D0%B1%D0%B8%D1%80%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5%20%D0%B8%D0%BD%D1%81%D1%82%D0%B8%D1%82%D1%83%D1%82%D1%8B%20%D0%B2%20%D1%80%D0%B0%D0%BC%D0%BA%D0%B0%D1%85.pdf (дата обращения 10.09.2026)

15. Наблюдатели на выборах в 2024 году: права и обязанности, как фиксируют нарушения при электронном голосовании [Электронный ресурс]. – URL: https://secretmag.ru/enciklopediya/kto-takoi-nablyudatel-na-vyborakh.htm (дата обращения 9.09.2026)

16. Новые рекомендации Совета Европы о правилах электронного [Электронный ресурс]. – URL: https://rfsv.ru/law/pravovye-innovatsii/novye-rekomendatsii-soveta-evropy-o-pravilakh-elektronnogo-golosovaniia-na-vyborakh (дата обращения 9.09.2026)

17. Опыт использования инструментов электронного голосования [Электронный ресурс]. – URL: https://saf.petrsu.ru/journal/article.php?id=13881 (дата обращения 9.09.2026)

18. Основные киберугрозы дистанционного электронного голосования в России [Электронный ресурс]. – URL: https://apni.ru/article/10422-osnovnye-kiberugrozy-distancionnogo-elektronnogo-golosovaniya-v-rossii (дата обращения 7.09.2026)

19. Основные негативные факторы распространения дистанционного электронного голосования [Электронный ресурс]. – URL: https://moluch.ru/archive/401/88811 (дата обращения 20.08.2026)

20. Памятка наблюдателю [Электронный ресурс]. – URL: https://vestnik37.ru/documents/%D0%BE%D0%B1%D1%83%D1%87%D0%B5%D0%BD%D0%B8%D0%B5/%D0%BF%D0%B0%D0%BC%D1%8F%D1%82%D0%BA%D0%B0%20%D0%BD%D0%B0%D0%B1%D0%BB%D1%8E%D0%B4%D0%B0%D1%82%D0%B5%D0%BB%D1%8E.pdf (дата обращения 28.09.2026)