ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМ ДИСТАНЦИОННОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Гриднев В.А.[1], Жаров В.Г.[2], Самодурова У.С.[3]

Ключевые слова: *легитимность, криптография, защита данных, аутентификация, информационные системы, информационные технологии, законодательство, избирательный процесс, протокол.*

Аннотация

Цель работы: исследовать существующие криптографические протоколы тайного голосования, опыт проведения дистанционного электронного голосования в России и за рубежом, обосновать предложения по дальнейшему совершенствованию безопасности электронной системы тайного голосования.

Метод: системный и сравнительный анализ существующих криптографических протоколов тайного голосования.

Результат: в ходе исследования практик дистанционного электронного голосования были изучены различные криптографические протоколы тайного голосования и опыт применения таких систем, как в России, так и за рубежом; анализ показал, что существующие методы и подходы имеют ряд ограничений и проблем в области безопасности и эффективности; на основании проведенного системного и сравнительного анализа, авторы обосновали ряд продуктивных предложений по совершенствованию технических и правовых аспектов дистанционного электронного голосования, которые могут служить основой для дальнейшего развития и улучшения системы дистанционного голосования, повышая ее безопасность и доступность для граждан.

EDN: KNTRDT

Введение

В настоящее время голосование во всех демократических странах является неотъемлемой частью общественных процессов и обеспечивает возможность гражданам выражать свою волю при выборе представителей и принятии государственных и общественных решений. Традиционные методы голосования включают бумажные бюллетени и избирательные урны. Однако с развитием *информационных технологий* [8, 10] все большую популярность приобретает *дистанционное электронное голосование* (ДЭГ), которое предоставляет возможность голосовать через Интернет или другие электронные системы. Этот способ голосования представляет собой совокупность технологических и правовых решений, направленных на обеспечение возможности участия в выборах на расстоянии с использованием электронных средств.

В статье представлены результаты исследования различных аспектов ДЭГ, выявлены ключевые характеристики и определено влияние правовых и технологических факторов на его эффективность и *безопасность* [9], а также представлены результаты анализа практической реализации данного способа голосования в различных странах. Особое внимание уделено системному анализу [11] текущего состояния и перспектив развития ДЭГ в России, исследованию решенных задач и выявлению аспектов, требующих дополнительного изучения и улучшения.

История появления дистанционного электронного голосования

К середине 2010-х гг. первые законодательные инициативы в России были направлены на создание *нормативно-правовой базы* [10] для дистанционного голосования, однако настоящий прорыв произошел в 2020-х гг. В условиях пандемии COVID-19, когда мир перешел на дистанционный режим работы и общения, дистанционное голосование стало не просто удобной опцией, а необходимостью.

[1] ***Гриднев Виктор Алексеевич,*** *кандидат технических наук, доцент, доцент кафедры информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*
E-mail: vikadres@yandex.ru

[2] ***Жаров Василий Геннадиевич,*** *начальник управления защиты информации департамента безопасности негосударственного пенсионного фонда «Благосостояние», г. Тамбов, Российская Федерация.*
E-mail: qwertylight@ya.ru

[3] ***Самодурова Ульяна Сергеевна,*** *студентка выпускного курса Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*
E-mail: ms.ulyana.2001@mail.ru

Одним из ярких примеров начальных тестов ДЭГ в России является проект «Активный гражданин», запущенный в Москве в 2014 г. Эта инициатива позволяет гражданам участвовать в принятии решений на местном уровне, голосуя по различным вопросам через онлайн-платформу. Проект оказался весьма успешным: миллионы граждан приняли в нем участие и высказали свое мнение по таким вопросам, как транспорт, инфраструктура и государственные услуги[4].

Еще один пример, когда ДЭГ в ограниченном масштабе было введено в ходе президентских выборов 2018 г. Этот пилотный проект позволил гражданам России, проживающим за рубежом, проголосовать в электронном виде. Несмотря на то, что система подверглась критике и вызвала опасения по поводу безопасности и прозрачности, она стала важным шагом на пути к внедрению ДЭГ в более широком масштабе.

В 2020 г. в России впервые на федеральном уровне использовалась система ДЭГ — это было голосование по поправкам в Конституцию РФ. Позже способ начал применяться и на региональных выборах[5].

В ходе голосования по поправкам к Конституции 2020 г. в России дистанционное электронное голосование было введено в Москве и ряде других регионов. Центральная избирательная комиссия (ЦИК) России выпустила специальные рекомендации и инструкции для избирателей по регистрации и голосованию в режиме онлайн. С помощью мобильного приложения или веб-сайта избиратели могли участвовать в избирательном процессе дистанционно, что обеспечивало удобство и доступность, особенно в период пандемии COVID-19. ЦИК России внимательно следила за внедрением ДЭГ, чтобы обеспечить его справедливость и прозрачность, а общий опыт позволил получить ценные сведения для дальнейшего совершенствования и расширения данной системы голосования.

ДЭГ в России в последние годы набирает обороты, и выборы 10 сентября 2023 г. стали ярким примером его применения.

Дистанционное электронное голосование в других странах

Развитие ДЭГ в разных странах происходило поразному, в первую очередь из-за различий в технологической инфраструктуре, законодательной базе и политической воле.

Эстония — одна из немногих стран мира, где электронное голосование не только существует, но и активно применяется на практике. Это государство стало пионером в области электронного голосования, начав внедрение этой системы еще в 2005 г. Электронное голосование в Эстонии основано на использовании уникальных электронных *ID*-карт, которые выдаются каждому гражданину страны. Эти карточки позволяют идентифицировать личность гражданина и гарантировать анонимность его волеизъявления. Граждане могут проголосовать онлайн из любой точки мира, имея доступ к Интернету[6].

Южная Корея также добилась успехов в ДЭГ. Страна начала экспериментировать с электронным голосованием в 2002 г. и с тех пор расширила его применение на различных выборах. Используемая система требует от избирателей *аутентификации* с помощью цифрового сертификата, что обеспечивает безопасность и исключает возможность дублирования голосов. Удобство и эффективность ДЭГ способствовали повышению активности избирателей в Южной Корее.

Швейцария, известная своими демократическими традициями и частыми референдумами, активно исследует возможности внедрения ДЭГ. Однако, несмотря на технологические инновации и политическую волю, процесс внедрения проходит не без трудностей. В Швейцарии ДЭГ было введено в качестве альтернативного метода голосования в нескольких кантонах. Почта Швейцарии разработала систему, позволяющую избирателям голосовать в электронном виде с личных устройств. Однако использование этой технологии столкнулось с проблемами, связанными с безопасностью и прозрачностью. В результате некоторые кантоны приостановили использование ДЭГ [1].

ДЭГ в США применяется относительно ограниченно из-за опасений в отношении безопасности и неприкосновенности личности. Однако в некоторых штатах были проведены эксперименты с вариантами дистанционного голосования для определенных групп населения, таких как военнослужащие, проходящие службу за рубежом, или граждане, проживающие за границей[7].

Представленные примеры демонстрируют разнообразие подходов к ДЭГ в различных странах, подчеркивая актуальность исследований по повышению безопасности этого процесса.

Правовые аспекты дистанционного электронного голосования

На сегодняшний день основополагающими нормативными документами, регулирующими проведение ДЭГ в России, обеспечивающими прозрачность, безопасность и *легитимность* [7, 9, 10] процесса голосования являются:

1. Конституция Российской Федерации как высший нормативный акт, предоставляющий правовую основу для различных аспектов государственного управления, включая избирательный процесс. Конституция РФ

[4] «Активный гражданин»: И ты не один! URL: https://inlnk.ru/4yg5l0 (дата обращения: 05.09.2023).

[5] Электронное голосование-2020. URL: https://inlnk.ru/meyQk1 (дата обращения: 05.09.2023).

[6] Первый в мире блокчейн и электронное голосование. Как Эстония развивает е-сервисы для граждан. URL: https://inlnk.ru/zadG12 (дата обращения: 05.09.2023).

[7] Нятина Н. В. Гражданские инициативы молодежи : учебное пособие. Кемерово : КемГУ, 2022. 173 с.

не содержит конкретных упоминаний о дистанционном электронном голосовании, она устанавливает общие *принципы* [7] проведения выборов и право граждан на участие в них [6].

2. Федеральный закон «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации»[8], устанавливающий основные принципы и порядок проведения выборов и референдумов в России. Ст. 64.1 «Дистанционное электронное голосование» была введена 14 марта 2022 г. и впервые применена для проведения удаленного электронного голосования 5 декабря 2022 г. Решение о проведении ДЭГ может быть принято соответствующей избирательной комиссией или комиссией референдума. В данном решении должны быть определены сроки проведения ДЭГ, государственные информационные системы, используемые для проведения голосования, а также *условия*, при которых избиратель или участник референдума вправе принять участие в голосовании. Для проведения ДЭГ используются *государственные информационные системы*, в частности, такие как ГАС РФ «Выборы» и другие [10], прошедшие сертификацию и соответствующие требованиям, установленным ЦИК Российской Федерации.

3. Федеральный закон «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва»[9]. Этот закон был введен с целью проведения эксперимента по ДЭГ на выборах депутатов Московской городской Думы. В рамках эксперимента использовались электронные технологии для сбора и подсчета голосов избирателей на удаленных площадках. Закон устанавливает *требования* к системе электронного голосования, включая ее *безопасность*, *аутентификацию* и *защиту* [7, 9] данных. Он также регулирует процедуру регистрации избирателей для участия в дистанционном голосовании, а также правила подсчета и учета электронных голосов.

4. Постановление ЦИК РФ «О Порядке дистанционного электронного голосования с использованием федеральных государственных информационных систем»[10]. Постановление содержит ряд важных положений, регулирующих процесс ДЭГ: определяет процедуру голосования с использованием федеральных государственных информационных систем (ФГИС) [17], устанавливает требования к участникам, регулирует порядок регистрации участников и выдачи им доступа к системе голосования.

5. Постановление ЦИК РФ «О Требованиях к проведению дистанционного электронного голосования»[11], определяющее процедуру и условия, при которых избиратели могут использовать электронные средства для голосования на выборах, а также требования к электронным системам голосования и программному обеспечению, используемому при ДЭГ.

6. Постановление ЦИК РФ «О проведении дистанционного электронного голосования на выборах, которые должны быть назначены на 10 сентября 2023 года»[12]. Данный документ был принят в целях создания дополнительных условий для реализации активного избирательного права граждан и с учетом предложений, поступивших из избирательных комиссий субъектов Российской Федерации.

Анализ правовых аспектов ДЭГ в России показал, что несмотря на наличие комплекса законодательных и нормативных актов, регулирующих этот процесс, существует необходимость дальнейшего совершенствования нормативно-правовой базы [10]. Это связано с тем, что динамично развивающиеся технологии и методы голосования требуют адаптивного и гибкого подхода к законодательному регулированию для обеспечения легитимности, прозрачности и безопасности процесса голосования.

Тем не менее, учитывая достижения технического прогресса и появления все новых средств и методов дистанционного голосования, законодательство должно быть достаточно гибким и способным адаптироваться к изменениям. Это подчеркивает важность непрерывного диалога и сотрудничества между законодателями, ИТ-специалистами и гражданским обществом для формирования современного, эффективного и сбалансированного законодательства в рассматриваемой сфере. Поэтому актуальным становится анализ наиболее распространённых форм ДЭГ.

Протокол тайного голосования Фудзиока-Окамото-Охта

Данный *криптографический* [9, 18] протокол используется для защиты *конфиденциальности* голосования в электронных системах, где голоса избирателей передаются по сети. Он позволяет избирателям голосовать анонимно, не раскрывая своих личных данных или предпочтений другим участникам системы.

Схемы тайного голосования предлагались многими исследователями как с теоретической, так и с практи-

[8] Федеральный закон от 12 июня 2002 г. № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации) // СПС «КонсультантПлюс».

[9] Федеральный закон от 29 мая 2019 г. № 103-ФЗ «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования на выборах депутатов Московской городской Думы седьмого созыва» // СПС «КонсультантПлюс».

[10] Постановление Центральной избирательной комиссии Российской Федерации от 8 июня 2022 г. № 86/716-8 «О Порядке дистанционного электронного голосования с использованием федеральных государственных информационных систем» // СПС «КонсультантПлюс».

[11] Постановление Центральной избирательной комиссии Российской Федерации от 8 июня 2022 г. № 86/715-8 «О Требованиях к проведению дистанционного электронного голосования» // СПС «КонсультантПлюс».

[12] Постановление Центральной избирательной комиссии Российской Федерации от 7 июня 2023 г. № 117/927-8 «О проведении дистанционного электронного голосования на выборах, которые должны быть назначены на 10 сентября 2023 года» // СПС «КонсультантПлюс».

ческой точки зрения. В схеме с использованием многостороннего протокола процедуры управляются самими избирателями, однако для доказательства правильности всех действий требуется большое количество коммуникаций. Практическая секретная схема голосования требует дополнительных участников: доверенного центра или администратора[13].

Существуют два основных типа такого подхода: в одном из них избиратель отправляет бюллетень в зашифрованной форме, а в другом — отправляет его через анонимный канал связи.

Первый тип был предложен Джошем Бенало[14] в 1988 г. Данная схема использует технику шифрования с использованием остатков более высокой степени. Схема требует распределенных центров для защиты конфиденциальности избирателей, однако избиратель должен доказать, что распределенный бюллетень действителен, поэтому все голосование должно происходить одновременно.

В качестве схемы *второго* типа Дэвид Чаум предложил[15] схему голосования, использующую анонимный канал связи, и она обеспечивает безусловную защиту от отслеживания голосования. Впоследствии Казуо Охта предложил[16] практическую секретную схему голосования, используя только одного администратора по аналогичному принципу. Эти схемы более подходят для масштабных выборов, поскольку объемы коммуникаций и вычислений являются разумными даже при большом числе избирателей.

Японские криптографы Фудзиока, Окамото и Охта предложили[17] прагматичную и безопасную секретную схему голосования, подходящую для масштабных выборов и одновременно решающую проблемы конфиденциальности, анонимности и справедливости даже в случае сговора администратора и счетчика, а также обеспечивающую сокрытие ото всех даже промежуточных результатов голосования до его окончания. Схема предотвращает любые нарушения со стороны избирателей или администратора.

Соответствующий *протокол* тайного голосования в электронных системах предполагает безопасное и анонимное голосование на выборах, защищая тем самым целостность демократического процесса[18]. Кроме того, обеспечивается прозрачность и честность голосования, так как каждый избиратель имеет возможность лично убедиться в том, что его голос учтен правильно.

Протокол базируется на *модели*, включающей избирателей, администратора и счётчика (счётчик может быть заменен общественной доской), а также анонимный канал связи для общения избирателей и счётчика. При этом у каждого избирателя есть собственная схема обычной *цифровой подписи* [9], а у администратора — схема *слепой подписи*[19]. *Счётчик только создает список бюллетеней и публикует его. Упрощенно процедуру реализации данного протокола можно представить так:*

Шаг 1. Подготовка. Избиратель заполняет электронный бюллетень, создает сообщение с использованием техники слепой подписи для получения подписи администратора и отправляет его администратору.

Шаг 2. Администрирование. Администратор проверяет легитимность избирателя, отмечает в списке, что данный избиратель реализовал свое право голоса и подписывает сообщение, в котором скрыт бюллетень избирателя, и возвращает избирателю.

Шаг 3. Голосование. Избиратель получает бюллетень, подписанный администратором, и отправляет его анонимно счётчику.

Шаг 4. Сбор. Счётчик публикует список полученных бюллетеней.

Шаг 5. Раскрытие. Избиратель раскрывает свой голос, отправляя анонимно свой ключ шифрования.

Шаг 6. Подсчет. Счётчик подсчитывает голосование и объявляет результат.

К протоколу тайного электронного голосования предъявляют следующие *требования* [18]: голосовать могут только те, кто имеет на это право; каждый может голосовать только один раз; никто не может узнать, за кого проголосовал конкретный избиратель; никто не может проголосовать за другого; никто не может изменить результаты голосования; каждый голосующий может проверить, что его голос учитывался при подведении итогов голосования; каждый знает, кто голосовал, а кто нет.

Соответствующий обобщенный *протокол тайного голосования с одним Центром* позволяет избирателям отдать свой голос за пределами избирательного участка из любого месторасположения. То есть данный протокол предполагает наличие двух сторон: избиратель и Центральная избирательная комиссия, а реализуется в виде следующей процедуры:

Шаг 1. ЦИК публикует список всех правомочных избирателей.

Шаг 2. В течение определенного срока каждый избиратель сообщает в ЦИК о намерении голосовать.

Шаг 3. ЦИК публикует список избирателей, участвующих в выборах.

---

[13] Fujioka A., Okamoto T., Ohta K. A. practical secret voting scheme for large scale elections // Advances in Cryptology – Auscrypt '92: Lecture Notes in Computer Science, v. 718 / ed. by J. Seberry, Y. Zheng. Berlin, Heidelberg: Springer, 1993.

[14] Benaloh Josh. Dense probabilistic encryption (1994).

[15] Chaum D. Towards trustworthy elections. Springer-Verlag Berlin and Heidelberg GmbH & Co., 2010.

[16] Fujioka A., Okamoto T., Ohta K. A. practical secret voting scheme for large scale elections // Advances in Cryptology – Auscrypt '92: Lecture Notes in Computer Science, v. 718 / ed. by J. Seberry, Y. Zheng. Berlin, Heidelberg: Springer, 1993.

[17] Fujioka A., Okamoto T., Ohta K. A. practical secret voting scheme for large scale elections // Advances in Cryptology – Auscrypt '92: Lecture Notes in Computer Science, v. 718 / ed. by J. Seberry, Y. Zheng. Berlin, Heidelberg: Springer, 1993.

[18] Ермакова А. Ю. Криптографические методы защиты информации : учеб.-метод. пособие. М. : РТУ МИРЭА, 2021. 172 с.

[19] Разновидность цифровой подписи, предложенная Дэвидом Чаумом в 1982 г., при которой подписывающая сторона не может точно знать содержимое подписываемого документа.

Шаг 4. Каждый избиратель анонимно получает идентификационный номер (I) с помощью протокола *ANDOS* (*All or Nothing Disclosure of Secrets*)[20].

Шаг 5. Каждый избиратель с помощью ЭВМ генерирует пару «открытый ключ/закрытый ключ» $(<k,\ d>)$. Если v — это бюллетень, то избиратель создает и посылает в ЦИК следующее сообщение: $I,\ E_k\ (I,\ v)$[21]. Это сообщение должно быть послано анонимно.

Шаг 6. ЦИК подтверждает получение бюллетеня, публикуя: $E_k\ (I,\ v)$.

Шаг 7. Каждый избиратель посылает в ЦИК сообщение: $(I,\ d)$.

Шаг 8. ЦИК расшифровывает бюллетени. После окончания голосования ЦИК публикует результаты и для каждого варианта выбора список соответствующих значений: $E_k\ (I,\ v)$.

Улучшенный протокол тайного голосования отвечает большинству перечисленных требований, он не создает сложностей для избирателей, однако использует протокол *ANDOS*, который создает некоторые технические сложности при реализации. Кроме того, данный протокол не устраняет возможность незаконного вознаграждения избирателей за голосование в пользу определенного кандидата («покупка голосов»), а, наоборот, облегчает осуществление такой практики.

Протокол тайного голосования Фудзиока-Окамото-Охта выделяется своим акцентированием на *конфиденциальность*. С правовой точки зрения это позитивная особенность, так как она направлена на соблюдение принципа тайного голосования. Протокол также обеспечивает безопасность передачи данных, что является ещё одним важным аспектом, особенно в современных условиях, когда вопросы кибербезопасности становятся всё более актуальными. Данный протокол является хорошим примером *сбалансированного* подхода к обеспечению конфиденциальности и безопасности.

Протокол тайного голосования Хе-Су

Еще одним протоколом, основанным на идее слепой подписи, является протокол Хе-Су, опубликованный в 1997 г.[22] В данном протоколе участвуют три стороны: избиратель, администратор и счётчик. Но, в отличие от протокола Фудзиока-Окамото-Охта, в протоколе Хе-Су подписывается ключ избирателя, а не бюллетень. При этом в электронном голосовании участвуют три стороны[23]:

– избиратели, которые регистрируют свои ключи для голосования и отдают свои голоса;

– авторитет, который авторизует право голосования участников путем слепой подписи их ключей для подсчета голосов, которые будут использоваться для проверки подписей на бюллетенях;

– подсчитывающий, который собирает бюллетени, проверяет подлинность бюллетеней и публикует результаты выборов.

Процедура реализации протокола состоит из трех этапов:

– *регистрация*: на этом этапе избиратели регистрируются для участия в выборах, и авторитет авторизует их; каждый избиратель создает пару ключей (открытый и закрытый), авторитет слепо подписывает открытый ключ (ключ для подсчета голосов) и передает избирателю, который сохраняет закрытый ключ (ключ для голосования) для подписи бюллетеней на выборах (конечно, перед подписанием ключа для подсчета голосов авторитет должен проверить подлинность и право каждого избирателя);

– *представление ключей* (для подсчета голосов): на этом этапе каждый избиратель, у которого есть подтвержденный ключ для подсчета голосов (слепо подписанный авторитетом на этапе регистрации), отправляет свой ключ подсчитывающему, используя неразрывную почту; подсчитывающий проверяет подлинность представленного ключа для подсчета голосов с помощью открытого ключа авторитета и, наконец, публикует все допустимые представленные ключи для подсчета голосов;

– *голосование и подсчет голосов*: на этом этапе избиратели подписывают свои бюллетени с помощью ключей для голосования, прикрепляют подписи к своим бюллетеням и отправляют их подсчитывающему; подсчитывающий проверяет допустимость бюллетеней с помощью опубликованных ключей для подсчета голосов и публикует все допустимые бюллетени; каждый избиратель может проверить, был ли его голос учтен при подсчете; кроме того, любой может проверить правильность результатов с помощью бюллетеней, подписей и опубликованных ключей для подсчета голосов.

Протокол Хе-Су отличается сложностью и требовательностью к большому объему коммуникаций. С правовой стороны, это может создать определенные трудности. Например, чрезмерная сложность может сделать процесс менее доступным для широкой публики и увеличить риск ошибок или злоупотреблений.

Организационно-технические аспекты дистанционного электронного голосования

Дистанционное электронное голосование — голосование без использования бюллетеня, изготовленного на бумажном носителе, с использованием специального программного обеспечения, а также один из способов участия в выборах или референдумах без физического присутствия на избирательном участке [13]. Участковая избирательная комиссия по ДЭГ — коллегиальный орган, обеспечивающий организацию,

[20] Brassard G., Crepeau C., Robert J.-M. All-or-nothing disclosure of secrets. Springer Lecture Notes in Computer Science.1987. V. 263.

[21] $E_k\ (I,\ v)$ — правило зашифрования на ключе k идентификационного номера I и бюллетеня v.

[22] URL: https://www.researchgate.net/publication/228920120_A_new_secure_and_practical_electronic_voting_protocol_without_revealing_voters_identity .

[23] He Q., Su Zhongmin. A New Practical Secure e-Voting Scheme // School of Computer Science, Carnegie Mellon University. 1997. 25 Dec.

осуществление и установление итогов дистанционного электронного голосования. Протокол об итогах дистанционного электронного голосования — документ участковой избирательной комиссии по ДЭГ, отражающий ее решение об итогах голосования.

Основные характеристики ДЭГ [14]:

– для проведения дистанционного электронного голосования часто используются специализированные электронные платформы, которые должны обеспечивать высокий уровень безопасности и анонимности: *E-voting*, *EVoting*, *SecureBallot*, платформа Программно-технического комплекса дистанционного электронного голосования, Система дистанционного электронного голосования ЦИК РФ с применением технологии блокчейн [1, 15, 16];

– система способствует повышению явки избирателей; традиционные методы голосования часто требуют физического присутствия на избирательных участках, что может быть неудобным или невозможным для некоторых людей;

– использование электронных систем голосования позволяет значительно сократить расходы на организацию и проведение выборов: нет необходимости печатать бумажные бюллетени, обеспечивать места для голосования и нанимать дополнительный персонал.

ДЭГ подвержено угрозам кибербезопасности, таким как хакерские атаки, фишинг и вредоносное программное обеспечение [9]. Ни одна система не является полностью защищенной от кибератак и попыток фальсификации голосов [9, 12].

Основные современные организационно-технические *требования* к системам ДЭГ можно сформулировать следующим образом:

– для участия в ДЭГ необходима *верификация* [7] личности; обеспечение *достоверности* идентификации избирателей в онлайн-среде является сложной задачей; недостаточная *аутентификация* может привести к подделке голосов или многократному голосованию; поскольку заполнение электронного бюллетеня происходит вне контроля со стороны избирательной комиссии и общественного наблюдения, нельзя исключить так называемое «семейное» голосование — эта проблема влечет риск покупки голосов и иного воздействия на волеизъявление избирателей в момент его совершения;

– платформа для проведения голосования должна быть безопасна и надежна, системы ДЭГ должны быть устойчивы к взломам, а данные — зашифрованы; особую опасность представляет утечка информации по акустоэлектрическому каналу, образующемуся из-за наличия преобразователей информативного сигнала из акустического в электрический (в электрических цепях технических устройств) [2—4];

– система ДЭГ должна быть доступна для широкого круга граждан, включая тех, кто имеет ограниченный доступ к Интернету или не имеет навыков работы с компьютером; должна быть также обеспечена возможность голосования из любой точки мира в удобное для избирателей время, без затрат времени на посещение избирательных участков;

– разработка и поддержка надежной системы ДЭГ требует значительных финансовых и временных ресурсов;

– требуется учесть возможные юридические споры относительно легитимности результатов ДЭГ;

– система ДЭГ должна автоматизировать процесс подсчета голосов и получение результатов в режиме реального времени;

– для успешной реализации необходимо обеспечить прозрачность процесса и доверие избирателей к системе голосования; это включает доступность информации о системе, аудит результатов голосования и возможность повторной проверки голосов;

– требуется решить проблему сохранения тайны голосования и обеспечить доверие к голосованию у граждан.

Участие в ДЭГ возможно для граждан, достигших избирательного возраста и имеющих доступ к ФГИС. Для участия в голосовании необходимо зарегистрироваться в системе и получить доступ к электронному голосованию. Система обеспечивает *конфиденциальность* данных и защиту от *несанкционированного доступа* [9].

В России порядок проведения ДЭГ определен законодательно[24]:

– прежде чем принять участие в ДЭГ, избиратель или участник референдума должен быть зарегистрирован; регистрация осуществляется в соответствии с установленными правилами и процедурами; избиратель или участник референдума должен предоставить необходимые данные и подтвердить свою личность; регистрация может быть произведена как до начала голосования, так и во время его проведения;

– после регистрации избиратель или участник референдума получает доступ к ФГИС, используемой для проведения ДЭГ; доступ предоставляется посредством выдачи уникального логина и пароля, которые обеспечивают конфиденциальность и безопасность голосования;

– избиратель или участник референдума имеет возможность проголосовать посредством ФГИС в установленные сроки; голосование проводится в соответствии с *требованиями*, установленными ЦИК РФ или избирательной комиссией соответствующего субъекта РФ;

– после окончания срока голосования производится подведение итогов ДЭГ; результаты голосования фиксируются и подтверждаются соответствующей избирательной комиссией или комиссией референдума.

В дни голосования на главной странице портала ДЭГ будет доступна кнопка для перехода к голосованию. При ее нажатии избирателям будет предложено авторизоваться с использованием учетной записи

[24] Федеральный закон от 12 июня 2002 г. № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» // СПС «КонсультантПлюс».

портала «Госуслуги»[25]. Для участия в ДЭГ потребуется также подтвердить свою личность цифровым кодом из смс-сообщения, которое будет направлен на номер мобильного телефона, указанный в учетной записи избирателя на портале «Госуслуги». Существует возможность узнать, правильно ли учтен голос.

Результаты волеизъявления участников ДЭГ незамедлительно зашифровываются и сохраняются в виде транзакций в цепочке блоков.

После отправки бюллетеня система предоставляет избирателю «квитанцию», которая содержит данные о его транзакции, в том числе уникальный номер. По нему с помощью специального сервиса на портале наблюдения ДЭГ можно будет найти транзакцию и убедиться в ее наличии в цепочке блоков.

Тип транзакции «Принят бюллетень» будет означать, что транзакция содержит зашифрованный результат волеизъявления, а само наличие транзакции — факт ее учета.

Тайна голосования при ДЭГ обеспечивается путем процедуры *анонимизации* [5], которая запускается после корректного ввода кода подтверждения вашей личности при голосовании на портале ДЭГ. Для обеспечения анонимности происходит отделение всех персональных данных избирателя и их замена на уникальный код, с помощью которого предоставляется доступ к электронному бюллетеню.

В момент голосования система знает уникальный код избирателя, но не может сопоставить его с персональными данными.

При голосовании волеизъявление избирателя зашифровывается на его личном устройстве и уже в зашифрованном виде передается в систему.

Впервые документ с описанием протокола тайного голосования в России был представлен[26] 7 сентября 2023 г. В одном из подразделов кратко перечислены основные участники протокола ДЭГ и их функции:

– Избиратель — участник, обладающим активным избирательным правом и включенный в списки участников ДЭГ;

– Организатор — участник, осуществляющий организацию процесса голосования (в том числе соответствующая избирательная комиссия);

– Аутентификатор — участник, осуществляющий идентификацию и аутентификацию избирателей (с помощью Единой системы идентификации и аутентификации — ЕСИА);

– Регистратор — участник, предоставляющий избирателям право получения бюллетеня (путем формирования подписи вслепую);

– Урна — участник, выдающий избирателям бюллетени и принимающий обратно заполненные зашифрованные бюллетени;

– Учётчик — участник, представляющий собой хранилище транзакций (бюллетеней избирателей и других данных), к которому есть постоянный доступ на запись и/или чтение у следующих участников: Урна, Организатор, Регистратор, Наблюдатель, а также осуществляющий подсчет итогов;

– Наблюдатель — участник, осуществляющий наблюдение за процессом голосования и аудит результатов голосования, имеющий доступ к хранилищу транзакций, а также предоставляющий публичный доступ ко всему содержимому хранилища транзакций через Портал наблюдения.

Процедура реализации соответствующего протокола состоит в следующем[27]:

Шаг 1. Формирование исходных данных: формирование списков участников ДЭГ; передача данных голосования.

Шаг 2. Инициализация системы: генерация ключей; загрузка данных голосования; загрузка ключа шифрования бюллетеней.

Шаг 3. Предоставление права получения бюллетеня: идентификация и аутентификация избирателя; получение подписи вслепую и ключа шифрования бюллетеней.

Шаг 4. Подача заполненного бюллетеня: волеизъявление; публикация бюллетеня; проверка бюллетеня.

Шаг 5. Подведение итогов: прекращение выдачи и приема бюллетеней; восстановление разделяемого ключа шифрования; подсчет итогов; расшифрование итогов.

Шаг 6. Аудит.

Шаг 7. Публикация результатов.

Для *примера* рассмотрим более подробно реализацию задачи *волеизъявление* на *Шаге* 4:

1. Избиратель анонимно обращается к Урне и запрашивает текст бюллетеня по идентификатору $VotingID_i$ для каждого $i \in \{1, \dots, n\}$, где n — количество избирателей.

2. Урна отправляет Избирателю текст бюллетеня для каждого идентификатора i.

3. Избиратель для каждого идентификатора i заполняет бюллетень, определяя набор $(m_1^i, \dots, m_{t_i}^i)$, где значение $(m_j^i \in \{0,1\}$ обозначает голос «за» (1) или «против» (0) за j-й вариант, $j = 1, \dots, t_i$, и зашифровывает его:

$$((c_1^i, \dots, c_{t_i}^i), d^i) = \\ = SE.Enc(pk_i, (m_1^i, \dots, m_{t_i}^i), min_i, max_i).$$

4. Избиратель для каждого идентификатора i формирует транзакцию tx^i (где tx^i — идентификатор транзакции для конкретного избирателя с номером i)[28], включающую следующие данные: идентификатор, зашифрованный бюллетень, открытый ключ Избирателя, значение подписи.

[25] Портал дистанционного электронного голосования ЦИК России. URL: https://vybory.gov.ru/

[26] Там же.

[27] *См.*: Публичное акционерное общество «Ростелеком» (ПАО «Ростелеком»). Описание доработанного протокола тайного голосования (проект): [Текст] / ПАО «Ростелеком». М., 2023. 23 с.

[28] tx^i представляет собой электронную запись, которая содержит информацию о голосе избирателя и необходимые данные для проведения голосования и последующего подсчёта голосов.

5. Избиратель для каждого идентификатора i подписывает транзакцию tx^i: $\sigma^i = S.Sign(sk^i_{изб}, tx^i)$.

6. Избиратель отправляет Урне подписанные транзакции (tx^i, σ^i), $i=1,\ldots,n$.

7. Урна проверяет для каждого идентификатора i: корректность формата транзакции, корректность подписи Регистратора в транзакции, корректность подписи Избирателя под транзакцией, уникальность транзакции.

Если какая-то из проверок завершена неуспешно, то Урна возвращает Избирателю ошибку и отбрасывает бюллетень.

В противном случае Урна:

– добавляет ключ ($pk^i_{изб}$) в свою *внутреннюю базу данных* [8];

– отправляет транзакции Учётчику (не подписывая дополнительно);

– формирует квитанцию о приеме транзакции (подписанная Урной принятая транзакция и ее идентификатор) и отображает ее Избирателю.

На экране устройства избирателя отображается содержимое его транзакций и квитанций, которые избиратель сохраняет.

Рассмотренные протоколы были апробированы в ходе проведения более 4 *тыс*. избирательных кампаний в 86 субъектах РФ в период с 8 по 10 сентября 2023 г. Всего замещению подлежали более 33 *тыс*. мандатов и выборных должностей. В онлайн-голосовании на выборах приняли участие 24 региона страны на федеральной платформе, а также Москва на собственной платформе. Всего дистанционным электронным голосованием воспользовались более трех миллионов граждан России[29].

Анализ организационно-технических аспектов ДЭГ выявляет несколько ключевых направлений для дальнейшего развития. Особое внимание требует безопасность и надежность используемого программного обеспечения, что подразумевает необходимость его регулярного аудита и обновления. Следующим важным элементом является подготовка и обучение персонала участковых избирательных комиссий, которые играют центральную роль в организации и контроле процесса. Кроме того, критическую важность приобретает разработка надежных и безопасных методов документирования и хранения данных, чтобы обеспечить прозрачность и доступность для общественного контроля. В целом фокусирование на этих аспектах не только повысит доверие к системе, но и сделает ее более эффективной и безопасной.

Заключение

Таким образом, на основе системного и сравнительного анализа выявлены ключевые характеристики, организационно-технические и правовые возможности и ограничения дистанционного электронного голосования, а также обоснованы предложения по его улучшению.

С точки зрения законодательства в России — создана основа, включающая ряд законов и нормативов, обеспечивающих реализацию дистанционного электронного голосования. С технической точки зрения — активно разрабатываются и внедряются новые методы и технологии, направленные на повышение безопасности и доступности ДЭГ. Это включает не только разработку новых технологических решений, но и постоянное тестирование и отладку существующих систем для обеспечения их стабильности и надежности.

Вместе с тем выявлено, что, несмотря на определенные достижения в технологическом и правовом аспектах, существует ряд вопросов и уязвимостей, требующих дополнительного внимания и решения. Прежде всего, требуется повысить уровень доверия избирателей к ДЭГ, для чего нужно, в частности, реализовать возможность для избирателя проверить, что его голос учтен правильно, и принять меры для исключения «покупки голосов». Это включает обновление законодательства для адаптации к технологическим изменениям и соответствия международным стандартам, а также разработку и внедрение новых технологических решений для улучшения защиты данных и удобства использования системы ДЭГ.

Осознавая важность образования и осведомленности в этой области, необходимо разработать и внедрить специализированные образовательные программы и тренинги. Это поможет повысить уровень понимания и компетенции среди избирателей, законодателей и технических специалистов, что, в свою очередь, способствует формированию более сознательного и ответственного подхода к дистанционному электронному голосованию.

Дистанционное электронное голосование продолжает быть предметом научных исследований и общественных дебатов. Будущее ДЭГ во многом зависит от успешности решения вопросов, связанных с внедрением и проведением голосования. Имея большое значение для развития современных демократических механизмов, ДЭГ будет продолжать эволюционировать в соответствии с технологическими инновациями и социально-политическими изменениями.

Рецензент: ***Алексеев Владимир Витальевич,*** *доктор технических наук, профессор, член-корреспондент РАЕН, почетный радист РФ, заведующий кафедрой информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*
E-mail: vvalex1961@mail.ru

[29] Интерфакс. URL: https://inlnk.ru/emyXKx

Литература

1. Алексеев Р. А., Абрамов А. В. Проблемы и перспективы применения электронного голосования и технологии избирательного блокчейна в России и за рубежом // Гражданин. Выборы. Власть. 2020. № 1. С. 9—21.
2. Алексеев В. В., Гриднев В. А., Яковлев А. В., Машкова О. С., Савилова У.А., Шибков Д. А., Яковлева Д. А. Системный подход к построению программно-аппаратного комплекса для подготовки специалистов по информационной безопасности // Вестник Тамбовского ГТУ. 2021. № 1. С. 20—30.
3. Алексеев В. В., Емельянов Е. В., Кастерин Д. А., Стрельцов А. А. Правовой подход к построению системы защиты информации в организации // Правовая информатика. 2020. № 2. С. 54—61. DOI: 10.21681/1994-1404-2020-2-54-61 .
4. Алексеев В. В., Клинков Д. А., Яковлев А. В. Способ защиты речевой информации в офисном помещении // Правовая информатика. 2023. № 2. С. 44—53. DOI: 10.21681/1994-1404-2023-2-44-53 .
5. Борисов Р. С., Ефименко А. А. Протокол анонимизации наборов данных для публикации в открытых источниках // Правовая информатика. 2023. № 2. С. 54—66. DOI: 10.21681/1994-1404-2023-2-54-66 .
6. Кондращенко Д. А. Конституционно-правовое регулирование использования информационных технологий в избирательном процессе Российской Федерации: проблемы и перспективы развития // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2021. № 2. С. 215—222.
7. Ловцов Д. А. Информационная теория эргасистем. Тезаурус : монография. М. : Наука, 2005. 248 с. ISBN 5-02-033779-X.
8. Ловцов Д. А. Информационная теория эргасистем : монография. М. : РГУП, 2021. 314 с. ISBN 978-5-93916-887-8.
9. Ловцов Д. А. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2021. 276 с. ISBN 978-5-93916-896-0.
10. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере : монография. М. : РГУП, 2016. 316 с. ISBN 978-5-93916-505-1.
11. Ловцов Д. А. Системный анализ. Часть 1. Теоретические основы. М. : РГУП, 2018. 224 с. ISBN 978-5-93916-701-7.
12. Ловцов Д. А. Информационная безопасность автоматизированных блокчейн-систем: угрозы и способы повышения // Тр. II Междунар. науч.-прак. конф. «Трансформация национальной социально-экономической системы России» (22 ноября 2019 г.) / РГУП. М. : РГУП, 2020. С. 464—473.
13. Петрова С. В., Сидорова А. В. К вопросу о внедрении дистанционного электронного голосования в избирательную систему России // Северо-Кавказский юридический вестник. 2021. № 4. С. 80—84.
14. Петрова С. В., Сидорова А. В. Система дистанционного электронного голосования в Российской Федерации и пути совершенствования электронной демократии // Государственное и муниципальное управление. Ученые записки. 2022. № 1. С. 192—196.
15. Черных А. М. Защищенность данных об объектах недвижимости и земельных ресурсах на базе геоинформационных и блокчейн-технологий // Правовая информатика. 2019. № 4. С. 75—85. DOI: 10.21681/1994-1404-2019-4-75-85 .
16. Черных А. М. Блокчейн и обработка судебной информации // Российское правосудие. 2021. № 9. С. 54—62. DOI: 10.37399/issn2072-909x.2021.9-54-62 .
17. Черных А. М. Основные направления интеграции федеральных государственных информационных систем и пространственных данных // Правовая информатика. 2018. № 2. С. 47—56. DOI: 10.21681/1994-1404-2018-2-47-56 .
18. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М. : Триумф, 2012. 816 с.

ENSURING THE SECURITY OF REMOTE ELECTRONIC VOTING SYSTEMS

Viktor Gridnev, *Ph.D. (Technology), Associate Professor at the Department of Information Systems and Information Protection of the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: vikadres@yandex.ru

Vasilii Zharov, *Head of the Information Protection Directorate of the Department of Security of the Non-Govermental Pension Fund "Blagosostoianie" (Welfare), Tambov, Russian Federation.*
E-mail: qwertylight@ya.ru

Ul'iana Samodurova, *graduate year student at the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: ms.ulyana.2001@mail.ru

Keywords: *legitimacy, cryptography, data protection, authentication, information systems, information technologies, legislation, electoral process, protocol.*

Abstract

Purpose of the paper: studying existing cryptographic protocols for secret voting and the experience of remote electronic voting in Russia and abroad, justifying proposals for further improving the security of the electronic secret voting system.

Methods used: system and comparative analysis of existing cryptographic secret voting protocols.

Study findings. In studying remote electronic voting practices, different cryptographic secret voting protocols and the experience of using such systems both in Russia and abroad were examined. An analysis showed that existing methods and approaches have a number of limitations and problems as regards security and efficiency. Based on the system and comparative analysis carried out by the authors, a number of productive proposals for improving the technical and legal aspects of remote electronic voting was justified which can be a basis for further developing and enhancing the remote voting system, increasing its security and accessibility for citizens.

References

1. Alekseev R. A., Abramov A. V. Problemy i perspektivy primeneniia elektronnogo golosovaniia i tekhnologii izbiratel'nogo blokcheina v Rossii i za rubezhom. Grazhdanin. Vybory. Vlast', 2020, No. 1, pp. 9–21.
2. Alekseev V. V., Gridnev V. A., Iakovlev A. V., Mashkova O. S., Savilova U. A., Shibkov D. A., Iakovleva D. A. Sistemnyi podkhod k postroeniiu programmno-apparatnogo kompleksa dlia podgotovki spetsialistov po informatsionnoi bezopasnosti. Vestnik Tambovskogo GTU, 2021, No. 1, pp. 20–30.
3. Alekseev V. V., Emel'ianov E. V., Kasterin D. A., Strel'tsov A. A. Pravovoi podkhod k postroeniiu sistemy zashchity informatsii v organizatsii. Pravovaia informatika, 2020, No. 2, pp. 54–61. DOI: 10.21681/1994-1404-2020-2-54-61 .
4. Alekseev V. V., Klinkov D. A., Iakovlev A. V. Sposob zashchity rechevoi informatsii v ofisnom pomeshchenii. Pravovaia informatika, 2023, No. 2, pp. 44–53. DOI: 10.21681/1994-1404-2023-2-44-53 .
5. Borisov R. S., Efimenko A. A. Protokol anonimizatsii naborov dannykh dlia publikatsii v otkrytykh istochnikakh. Pravovaia informatika, 2023, No. 2, pp. 54–66. DOI: 10.21681/1994-1404-2023-2-54-66 .
6. Kondrashchenko D. A. Konstitutsionno-pravovoe regulirovanie ispol'zovaniia informatsionnykh tekhnologii v izbiratel'nom protsesse Rossiiskoi Federatsii: problemy i perspektivy razvitiia. Izvestiia Saratovskogo universiteta. Novaia seriia. Seriia: Ekonomika. Upravlenie. Pravo, 2021, No. 2, pp. 215–222.
7. Lovtsov D. A. Informatsionnaia teoriia ergasistem. Tezaurus : monografiia. M. : Nauka, 2005. 248 pp. ISBN 5-02-033779-X.
8. Lovtsov D. A. Informatsionnaia teoriia ergasistem : monografiia. M. : RGUP, 2021. 314 pp. ISBN 978-5-93916-887-8.
9. Lovtsov D. A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 276 pp. ISBN 978-5-93916-896-0.
10. Lovtsov D. A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere : monografiia. M. : RGUP, 2016. 316 pp. ISBN 978-5-93916-505-1.
11. Lovtsov D. A. Sistemnyi analiz. Chast' 1. Teoreticheskie osnovy. M. : RGUP, 2018. 224 pp. ISBN 978-5-93916-701-7.
12. Lovtsov D. A. Informatsionnaia bezopasnost' avtomatizirovannykh blokchein-sistem: ugrozy i sposoby povysheniia. Tr. II Mezhdunar. nauch.-prak. konf. "Transformatsiia natsional'noi sotsial'no-ekonomicheskoi sistemy Rossii" (22 noiabria 2019 g.). RGUP. M. : RGUP, 2020, pp. 464–473.
13. Petrova S. V., Sidorova A. V. K voprosu o vnedrenii distantsionnogo elektronnogo golosovaniia v izbiratel'nuiu sistemu Rossii. Severo-Kavkazskii iuridicheskii vestnik, 2021, No. 4, pp. 80–84.
14. Petrova S. V., Sidorova A. V. Sistema distantsionnogo elektronnogo golosovaniia v Rossiiskoi Federatsii i puti sovershenstvovaniia elektronnoi demokratii. Gosudarstvennoe i munitsipal'noe upravlenie. Uchenye zapiski, 2022, No. 1, pp. 192–196.
15. Chernykh A. M. Zashchishchennost' dannykh ob ob"ektakh nedvizhimosti i zemel'nykh resursakh na baze geoinformatsionnykh i blokchein-tekhnologii. Pravovaia informatika, 2019, No. 4, pp. 75–85. DOI: 10.21681/1994-1404-2019-4-75-85 .
16. Chernykh A. M. Blokchein i obrabotka sudebnoi informatsii. Rossiiskoe pravosudie, 2021, No. 9, pp. 54–62. DOI: 10.37399/issn2072-909kh.2021.9-54-62 .
17. Chernykh A. M. Osnovnye napravleniia integratsii federal'nykh gosudarstvennykh informatsionnykh sistem i prostranstvennykh dannykh. Pravovaia informatika, 2018, No. 2, pp. 47–56. DOI: 10.21681/1994-1404-2018-2-47-56 .
18. Shnaier B. Prikladnaia kriptografiia. Protokoly, algoritmy, iskhodnye teksty na iazyke Si. M. : Triumf, 2012. 816 pp.