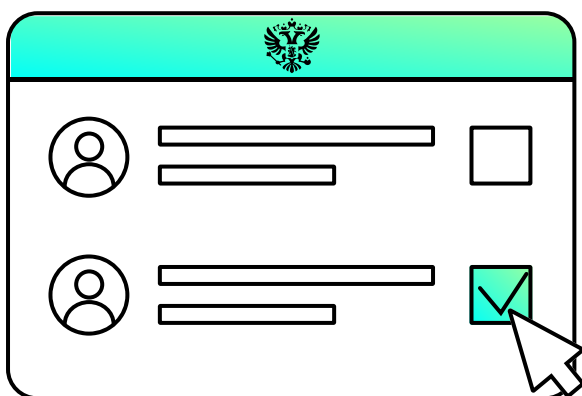


Единые дни голосования 2020–2024 гг. в России



Голосование



Web3 Tech совместно с ПАО «Ростелеком» на основе блокчейна разработала систему дистанционного электронного голосования, которую используют на федеральных выборах в России с 2020 года.

✓ Требования к системе

Основные требования, предъявляемые к системе для дистанционного электронного голосования, в целом совпадают с требованиями к системе традиционного очного голосования, и определены Федеральным законом от 12.06.2002 N 67-ФЗ (ред. от 31.07.2020) «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации».

01

Голосование на выборах и референдуме является тайным, исключающим возможность какого-либо контроля за волеизъявлением гражданина.

02

Возможность голосования должна быть предоставлена только лицам, обладающими активным избирательным правом на этом голосовании.

03

Один избиратель — один голос, не допускается «двойное» голосование.

04

Процесс голосования должен быть открытым и гласным для избирателей и наблюдателей.

05

Должна обеспечиваться неизменность поданного голоса.

06

Должна отсутствовать возможность подсчитать промежуточные итоги голосования до его завершения.

Итак, в системе три основных участника: избиратель, избирательная комиссия и наблюдатель, между которыми определен порядок взаимодействия. Еще можно выделить четвертого участника — органы, осуществляющие регистрационный учет граждан на территории (прежде всего, органы МВД, а также другие органы исполнительной власти), поскольку активное избирательное право связано с гражданством и местом регистрации. Все эти участники взаимодействуют друг с другом.

Разработкой системы дистанционного электронного голосования занимались ПАО «Ростелеком» и Web3 Tech по заказу ЦИК РФ. Команда разработки Web3 Tech подготовила техническое решение, состоящее из набора криптографических библиотек, смарт-контрактов, серверов учета бюллетеней и вспомогательных утилит для обеспечения необходимого набора функций, свойств и характеристик системы дистанционного электронного голосования (ДЭГ).

«В основе у нас лежит технология блокчейн, российская криптография. У нас полностью проработана модель угроз вместе с профильными ведомствами. Мы уверены, что, с точки зрения информационной безопасности, анонимизации пользователей, мы всем необходимым требованиям соответствуем»



Максут Шадаев

Министр цифрового развития, связи и массовых коммуникаций РФ

Единый день
голосования
2020
13 сентября

КАК ПРОГОЛОСОВАТЬ ОНЛАЙН

НА ДОПОЛНИТЕЛЬНЫХ ВЫБОРАХ ДЕПУТАТОВ ГОСУДАРСТВЕННОЙ ДУМЫ 7-ГО СОЗЫВА



ВАЖНО! Чтобы проголосовать онлайн необходимо иметь подтвержденную учетную запись на портале госуслуг.

✓ Техническая реализация

Подготовка к голосованию

01

Для участия в дистанционном голосовании избирателю необходимо подать заявление на едином портале государственных и муниципальных услуг. После завершения периода подачи заявлений представители ЦИК проверяют их и записывают данные избирателей на внешний носитель. При этом они удаляются из списков на традиционных участках.

02

В присутствии СМИ территориальная избирательная комиссия ДЭГ с помощью аппаратного модуля безопасности генерирует ключевую пару из закрытого и открытого ключа голосования. Открытый ключ записывают в блокчейн-сеть. Закрытый ключ разделяют, и каждую часть передают на хранение ответственным лицам — представителям партий и общественных движений — на отдельных носителях. Исходный ключ при этом уничтожается.

03

Затем территориальная избирательная комиссия ДЭГ загружает все данные голосования в программно-технический комплекс. Для избирательных округов создаются ключевые пары — впоследствии они будут использованы для проверки права доступа избирателей к голосованию при сохранении их анонимности. С этого момента для доступа к ним потребуется собрать закрытый ключ, разделенный между ответственными лицами.

Голосование

01

На портале голосования избиратель авторизуется с помощью Госуслуг. Через этот сервис система получает все необходимые данные для идентификации избирателя. Происходит проверка его браузера на совместимость с системой, а затем на мобильный телефон избирателя направляется SMS-код авторизации.

02

Осуществляется разрыв персональных данных избирателя, которые проверяются при запросе доступа к голосованию, и его уникального идентификатора (открытого ключа), с которым избиратель далее будет присутствовать в системе голосования. Он перенаправляется в анонимную зону голосования, где его ключ, слепая подпись и идентификатор проверяются на уникальность — это необходимо для защиты от повторного голосования.

03

Избиратель получает электронный бюллетень и отдает свой голос. Этот голос сразу же шифруется таким образом, чтобы его невозможно было сопоставить с данными избирателя. При разрыве связи с системой голосования пользователь может вновь зайти в нее и завершить заполнение бюллетеней.

С 2022 года каждый избиратель по итогам электронного голосования смог получить электронную квитанцию, подтверждающую, что его голос был учтен. Квитанция выдавалась после анонимизации избирателя, поэтому по ней невозможно было его идентифицировать. Но с её помощью сам избиратель может найти свой голос в истории транзакций и убедиться, что он учтен.

Подведение итогов голосования

01

По истечении времени голосования смарт-контракт системы получает соответствующую блокчейн-транзакцию и прекращает прием голосов. Бюллетени избирателей в зашифрованном виде проверяются на корректность заполнения с помощью технологии zero-knowledge proof (доказательства с нулевым разглашением). Затем также без расшифровки происходит сложение всех бюллетеней.

02

Ответственные лица собирают из доверенных им частей закрытый ключ голосования, экспортируя его в защищенном контейнере на аппаратный модуль безопасности. Этот ключ вместе с ключом территориальной избирательной комиссии используется для расшифровки итогов голосования. Они публикуются в расшифрованном виде.

03

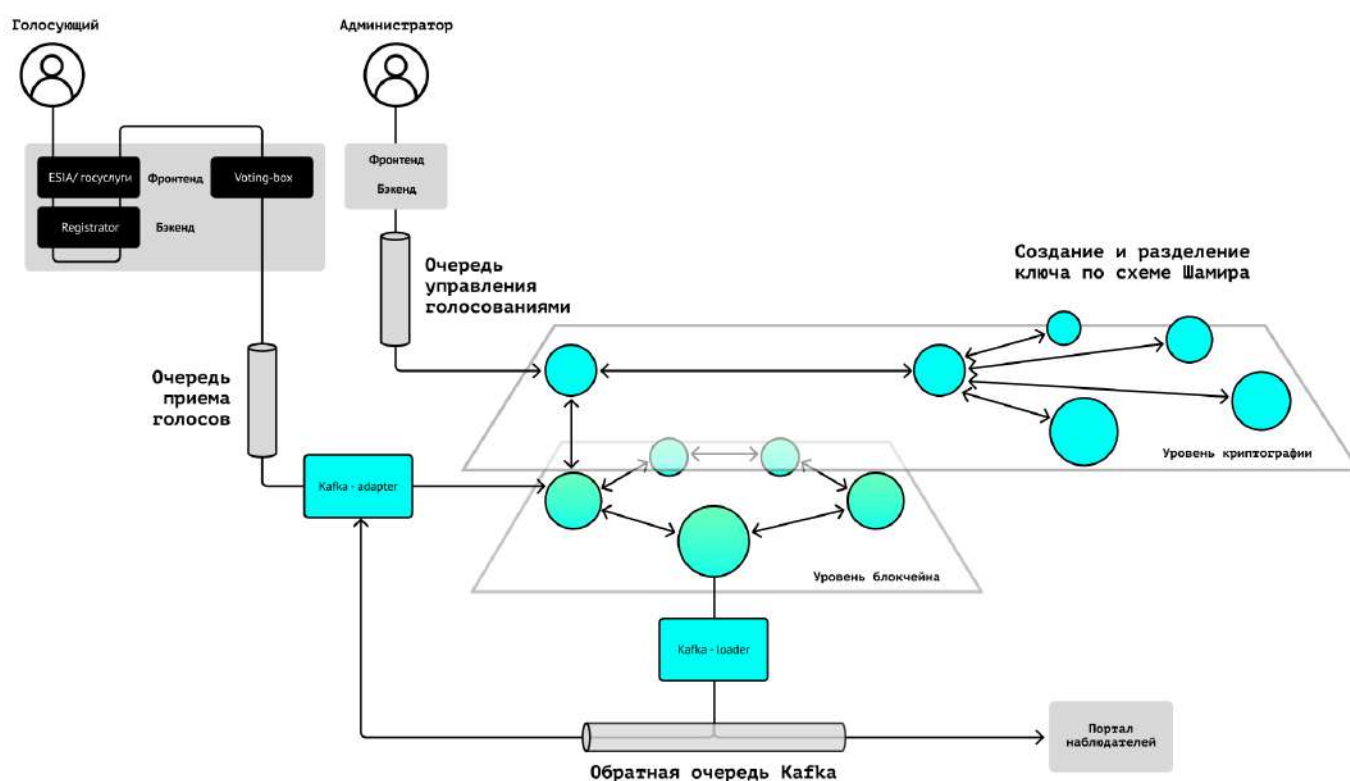
С помощью специального инструмента наблюдатели могут проверить корректность подсчета итоговых голосов. Таким образом, сочетание современных технологий блокчейна и криптографии позволяют организовать надежный, безопасный и прозрачный процесс приема, обработки, хранения и подсчета голосов избирателей, а также невозможность фальсификации итоговых результатов.

В **2021 году** для независимых наблюдателей на основе открытого исходного кода была создана специальная утилита, с помощью которой можно отслеживать ход голосования и убедиться в отсутствии фальсификаций. Наблюдатели развернули эту утилиту на разных операционных системах и подтвердили ее стабильную и прозрачную работу.

С **2022 года** в голосовании было задействовано еще одно нововведение платформы – watcher-ноды. Они не выпускают блоки самостоятельно, а получают их от майнеров и применяют к своему стеиту. Наблюдатели могут самостоятельно подключаться к таким нодам, чтобы получать данные голосования напрямую из блокчейна.

С 2022 года дистанционное электронное голосование на федеральной платформе проводится в регионах, расположенных в разных часовых поясах (-4 часа в Томске, +1 час в Калининграде к московскому времени), с разным числом дней голосования (2 дня в Томске и Калуге, 3 дня в остальных регионах) и на выборах нижнего, муниципального уровня. С 2023 года голосования в разных часовых поясах были разделены на независимые потоки, и регионы могли получить результаты, не дожидаясь «самого позднего» из них – Калининградской области. Ни технических, ни организационных сбоев в связи с этим замечено не было.

В **2023 году** ключи голосования и часть криптографических операций были вынесены в HSM (hardware secure module – аппаратный модуль безопасности). Такая реализация обеспечивает максимальный уровень защиты от злоумышленников. Криптографические операции, требующие операций с закрытыми ключами – генерация ключей, суммирование бюллетеней и часть процесса расшифровки – проходят прямо в модуле без передачи ключей куда-либо еще. Сочетание открытых и доступных инструментов мониторинга вместе с возможностью доступа к блокчейну в реальном времени позволили обеспечить максимальную прозрачность дистанционного голосования.



✓ Ход голосования

В **2020 году** электронное голосование в системе «Ростелекома» и Web3 Tech проводилось в двух избирательных округах в Курской и Ярославских областях. По итогам успешной работы в 2021 году география ДЭГ была расширена: на выборах 17–19 сентября система использовалась в качестве федеральной уже в 6 регионах РФ — в Курской, Мурманской, Нижегородской, Ярославской, Ростовской областях, а также в городе Севастополе. В 2021 году через нашу систему проголосовало около 600 тысяч избирателей. Явка составила более 90%. В 2022 году голосование охватило Курск, Ярославль, Калининград, Калугу, Новгород Великий, Псков и Томск.

В **2023 году** дистанционное электронное голосование охватило 24 субъекта РФ — от Камчатского края до Калининградской области — где проголосовало примерно 1,2 млн избирателей. Весной 2024 года на выборах президента РФ был установлен рекорд ДЭГ: в 28 регионах проголосовало 4,5 млн человек.

В отличие от Москвы, чья система ДЭГ многократно обозначалась «полигоном инноваций», федеральная ДЭГ предельно консервативна — будучи качественно спроектированной в 2020 году, она почти не менялась ни в 2021, ни в 2022. В силу этого связанных с ней вопросов оказалось значительно меньше, а вот практика наблюдения совершила качественный скачок.

Все действия в системе контролируются математически, а данные не могут быть фальсифицированы без оставления заметных и неустранимых следов, которые будут обнаружены либо наблюдателями, либо самим избирателями.

В первую очередь, в федеральной системе ДЭГ реализовано сквозное применение криптографических алгоритмов — все действия в системе контролируются математически, а данные не могут быть фальсифицированы без оставления заметных и неустранимых следов, которые будут обнаружены либо наблюдателями, либо самим избирателями.

Такая реализация системы ДЭГ является ответом на традиционную претензию — отсутствие исходных кодов ПО, выполняемого на серверах (более того, наличие этих кодов претензию бы не сняло: эффективных механизмов контроля, выполняется ли на серверах именно этот код, а также — в каком окружении, просто нет). Именно сквозной криптографический контроль снимает эту проблему: за три года существования системы так и не была показана ни одна модель атаки, которая позволила бы незаметно фальсифицировать данные на стороне серверов ДЭГ.



Олег Артамонов

Руководитель группы научно-технической экспертизы Партии Прямой Демократии

▼ Результат

В ходе выборов в сентябре 2020 дистанционно проголосовали около 30 000 избирателей, в сентябре 2021 — около 600 000. В сентябре 2023 года — 1,2 млн, а на президентских выборах весной 2024 — 4,5 млн. В процессе голосования не было выявлено каких-либо значимых сбоев и ошибок в системе. Команда Web3 Tech совместно с ПАО «Ростелеком» продолжают развитие системы электронного голосования для проведения более масштабных национальных голосований.

Подробный отчет Партии Прямой Демократии о голосовании 2022 года вы можете прочитать на [сайте](#) ее экспертного клуба. В 2023 году состоялось первое заседание экспертов по технологиям дистанционного электронного голосования (ДЭГ), обзор которого можно почитать на [Хабре](#).

Статистика ДЭГ по президентским выборам весной 2024 года доступна на vybory.gov.ru.

4,5 МЛН ИЗБИРАТЕЛЕЙ

проголосовали дистанционно на выборах президента весной 2024 г.

28 СУБЪЕКТОВ РФ

охватило голосование весной 2024 года

>200 TPS

(операций в секунду) составила пиковая нагрузка на блокчейн-сеть ДЭГ весной 2024 года