# **Актуальность**

Тема является очень актуальной сейчас, в период пандемии, да и вообще, когда все переходит в онлайн.

В Москве проводили ДЭГ, но, судя по всему, [вышло не очень хорошо](https://habr.com/ru/company/analogbytes/blog/504328/). И видимо сейчас нет системы для ДЭГ, обеспечивающей все, что дает очное (бумажное) голосование.

# **Общее описание решения**

Классическое бумажное голосование обеспечивает нам, как минимум:

тайну голосования (разрыв между аутентификацией избирателя и фиксацией его голоса);

аудит списка избирателей (поимённый перечень проголосовавших);

аудит результатов голосования (возможность пересчёта бюллетеней);

сокрытие результатов до окончания голосования (невозможность определения исхода до окончания голосования).

Обязательные:

1. никто, кроме голосующего, не должен знать его выбор;
2. только [легитимные](https://ru.wikipedia.org/wiki/%D0%9B%D0%B5%D0%B3%D0%B8%D1%82%D0%B8%D0%BC%D0%BD%D0%BE%D1%81%D1%82%D1%8C) участники могут проголосовать, и притом только один раз;
3. решение голосующего не может быть тайно или явно кем-либо изменено (кроме, возможно, им самим).
4. аудит списка избирателей (поимённый перечень проголосовавших);
5. аудит результатов голосования (возможность пересчёта бюллетеней);
6. сокрытие результатов до окончания голосования (невозможность определения исхода до окончания голосования).

Желательные:

1. каждый легитимный участник может проверить, правильно ли зачтён его голос;
2. каждый легитимный участник может передумать и изменить свой выбор в течение определённого периода времени;
3. система должна быть защищена от продажи голосов избирателями;
4. в случае, если голос зачтён неправильно, каждый легитимный участник может сообщить об этом системе, не раскрывая своей анонимности;
5. невозможно отследить, откуда дистанционно проголосовал избиратель;
6. [аутентификация](https://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F) оператора;
7. можно узнать, кто принимал участие в голосовании, а кто — нет;
8. поддержание системы не должно требовать много ресурсов;
9. система должна быть [отказоустойчива](https://ru.wikipedia.org/wiki/%D0%9E%D1%82%D0%BA%D0%B0%D0%B7%D0%BE%D1%83%D1%81%D1%82%D0%BE%D0%B9%D1%87%D0%B8%D0%B2%D0%BE%D1%81%D1%82%D1%8C) в случае технических неисправностей (потеря электропитания), непреднамеренных (потеря избирателем ключа) и злоумышленных (намеренная выдача себя за другого избирателя, [DoS](https://ru.wikipedia.org/wiki/DoS" \o "DoS)/[DDoS](https://ru.wikipedia.org/wiki/DDoS" \o "DDoS)) атак.

## **Тайна голосования**

При классическом старорежимном голосовании тайна голосования обеспечивается физическим разрывом между двумя местами — местом, где избиратель удостоверяет своё право голосовать, и местом, где он отдаёт голос. В первом месте — это столик избирательной комиссии участка — избиратель идентифицируется по паспорту и ему выдаётся анонимизированный бюллетень. Во втором месте — урне для голосования — сам факт наличия бюллетеня является подтверждением права на голосование, личность избирателя уже неважна и, собственно, неизвестна.

В абсолютном большинстве систем ДЭГ, внедрявшихся как властями, так и оппозицией, как в России, так и за её пределами, этого разрыва нет: аутентификация и голосование проходят на одном и том же сервере, находящемся под контролем одних и тех же людей. Каковые, разумеется, могут иметь собственные политические интересы и, соответственно, быть потенциально нечистоплотными на руку.

Единственным критичным требованием к реализации является наличие двух серверов, находящихся под управлением независимых друг от друга сил (это могут быть, например, две фракции или два комитета внутри партии, если речь о внутрипартийной системе).

**Cервер аутентификации пользователей** проверяет, может ли данный пользователь голосовать, и если да — генерирует две половинки ключа. Одна половинка отправляется на **сервер учёта голосов**, вторая передаётся избирателю на устройство, с которого он голосует.  
  
В момент отдачи голоса этот голос подписывается ключом избирателя и отправляется на сервер голосования, который сверяет ключи и учитывает голос. Сам факт наличия у избирателя его половинки ключа является подтверждением его права на голосование; знать личность избирателя сервер учёта голосов не знает и знать не может.  
  
В случае, если проводится открытое голосование, после получения голоса сервер учёта голосов отправляет информацию о нём на сервер аутентификации пользователей, который сопоставляет ключ с ФИО и публикует эту информацию в списке прошедших аутентификацию избирателей.  
  
В случае тайного голосования **сервер учёта голосов** только подтверждает серверу аутентификации факт свершившегося голосования.  
  
Важным нюансом в реализации такой схемы является учёт возможности атак по косвенным данным, в которые могут входить отпечаток устройства пользователя, IP-адрес пользователя и время голосования. При обеспечении независимости двух используемых серверов здесь критично лишь время голосования — можно сопоставить время аутентификации пользователя и время внесения в базу голоса; поэтому схема взаимодействия серверов и пользователей должна предусматривать разрушение этой связи в явном виде, как минимум, через добавление случайной задержки между аутентификацией и отправкой голоса со стороны устройства, используемого пользователем для голосования.  
  
В остальном же схема с двумя независимыми серверами — и только она! — позволяет реализовать тайну голосования в электронной форме.  
  
Схемы, в которых используется единый сервер, **доверенными в этом контексте считаться не могут по определению**; все заявления их авторов об отсутствии регистрации имён избирателей в связке с отданными ими голосами держатся исключительно на доверии к чистоплотности и аккуратности данных авторов (и все мы помним, что в IT-индустрии — тысячи примеров, когда автор сервиса не имел в виду ничего плохого, просто забыл в релизной сборке отключить отладочное логгирование).  
  
Корректно реализованная схема с независимыми серверами обеспечивает тайну голосования всегда, если владельцами обоих серверов не были сознательно предприняты меры к её устранению.

# **Аутентификация пользователей**

Это — самая простая часть системы. В зависимости от целей и важности голосования, аутентификация может проводиться:

Парой логин-пароль или PIN-кодом по SMS (например, соцопросы или решение локальных вопросов городского хозяйства)

По номеру партбилета пользователя, включая электронный партбилет на базе NFC/RFID (например, текущие внутрипайртийные голосования)

По аутентификации в ЕСИА (внутрипартийные праймериз, внепартийные голосования, включая общегосударственные выборы и референдумы)

(ЕСИА — Единая система идентификации и аутентификации — это система авторизации в «Госуслугах»; партиям недавно разрешили использовать её для праймериз и сбора подписей)  
  
Отметим, что биометрические датчики смартфонов (датчик отпечатка глаза, радужки глаза и т.п.) использоваться для аутентификации в электоральных системах не могут, т.к. не отдают наружу собственно биометрические данные, а лишь подтверждают, что данное лицо является владельцем данного смартфона. Владелец пяти смартфонов, соответственно, сможет аутентифицироваться пять раз. Эти датчики могут использоваться лишь для подтверждения доступа к приложению, используемому для голосования, чтобы посторонний человек, получивший доступ к смартфону, не отдал голос за его владельца.  
  
Использование биометрических данных для аутентификации в системе голосования потенциально возможно, но лишь в случае добровольного предоставления их пользователями и обработки со стороны сервера аутентификации пользователей — например, по фотографии лица.

# Аудит хода голосования

Одним из способов фальсификации результатов голосования являются вбросы «лишних» бюллетеней и так называемые «карусели».  
  
Влияние внешних сил в данной схеме может быть исключено проработкой системы аутентификации пользователей.  
  
Вместе с тем, даже при очень высокой надёжности системы аутентификации пользователей **владельцы сервера аутентификации могут начать генерировать «виртуалов»**, выдавая им ключи и отправляя их на сервер учёта голосов для голосования за нужный владельцам этих серверов пункт.  
  
Предотвратить это можно несколькими способами:  
  
выгрузкой с сервера аутентификации пользователей поимённого списка зарегистрировавшихся и проголосовавших избирателей, аналогичного бумажным спискам избирательной комиссии (ИК), на устройства наблюдателей и членов ИК;

анализом со стороны сервера учёта голосов аномалий в поведении пользователей (большое число пользователей с однотипных устройств, одинаковых IP-адресов, ненормальное распределение пользователей по времени голосования);

отсутствием возможности для наблюдателей или владельцев сервера аутентификации узнать текущее распределение голосов до окончания голосования.

Здесь мы впервые сталкиваемся с понятием «наблюдатель» — на дистанционных голосованиях наблюдатели также нужны, и нужны с той же целью, что на и голосованиях бумажных. Однако, в данном случае они контролируют происходящее не очно, а по выгрузке данных на их устройства с серверов аутентификации и учёта голосов.

# **Аудит результатов голосования**

Наиболее важна роль наблюдателей в аудите результатов голосования. Очевидно, что **владельцы сервера учёта голосов потенциально могут просто подменить числа** перед их публикацией.  
  
Чтобы не допустить этого, в течение всего хода голосования на устройства наблюдателей регулярно реплицируется текущая база данных голосов (при желании как раз сюда можно прикрутить блокчейн — но в общем не обязательно). Чтобы не допустить утечек результатов раньше окончания голосования, база криптографически защищается.  
  
В момент окончания голосования и публикации его результатов ключ от базы рассылается наблюдателям, так что они могут **самостоятельно подсчитать результат голосования** и сравнить его с опубликованным — это сделает невозможной подмену результата.  
  
Кроме того, наблюдатели могут сверить число голосов, зарегистрированных сервером учёта голосов, с числом избирателей, зарегистрированных сервером аутентификации, чтобы исключить вариант вброса анонимных голосов владельцами сервера учёта голосов (тем более, что потенциально они являются единственными людьми, способными отслеживать результаты голосования в реальном времени, и потому могут аккуратно подбрасывать голоса в нужную сторону так, чтобы это не было заметно).  
  
В этой же системе может решаться и задача недопущения **подмены голосов реальных пользователей** — возможна реализация так называемой аудируемой системы голосования, в которой пользователь может, использую индивидуальный криптографический ключ, проверить, за кого был засчитан его голос, при этом не раскрывая свою личность и не имея возможности проверить голоса других избирателей. Подчеркнём, что во многих статьях такой проверкой возможности аудита исчерпываются — это неверно, т.к. **личная проверка не исключает возможности вброса «мёртвых душ» или подмены итоговых результатов**.

# **Голосование под давлением**

Типичной проблемой дистанционных, да и очных голосований является голосование под давлением — в ситуации, когда руководитель (например, директор предприятия) предписывает сотрудникам голосовать за конкретного кандидата, отчитываясь фотографиями бюллетеней.  
  
Что интересно, в случае с дистанционными голосованиями эта угроза может быть нивелирована **возможностью изменения голоса** в течение всего хода голосования. То есть, пользуясь выданным ему ключом, избиратель может проголосовать несколько раз — и учтён будет только последний отданный ему голос, что позволит продемонстрировать начальнику «правильное» голосование, а далее отдать голос уже за реально желаемого кандидата.  
  
Кроме того, постфактумное обнаружение массовых переголосованный (база данных фиксирует *все* голоса, последний отданный учитывается уже при подсчёте) может указывать на наличие явной проблемы и повод для начала расследования.

Распределённый характер системы (независимая работа двух серверов, устройств наблюдателей и устройств пользователей) обеспечивает защиту от таких примитивных и типовых приёмов, как подмена кода или запуск сторонних приложений, модифицирующих работу системы, уже после проверки её экспертами — попытки вмешательства лишь в один из компонентов системы могут нарушить его работу, но не могут незаметно для эксплуатантов остальных компонентов системы фальсифицировать данные.  
  
При модульном построении системы она позволит проводить голосования с разными способами аутентификации, тайные и открытые, с разным уровнем доверия — в зависимости от решаемых вопросов.

Варианты протоколов голосвания:

[Протокол\_двух\_агентств](https://ru.wikipedia.org/wiki/Протоколы_тайного_голосования#Протокол_двух_агентств)

[Протокол\_Фудзиока-Окамото-Ота](https://ru.wikipedia.org/wiki/Протоколы_тайного_голосования#Протокол_Фудзиока-Окамото-Ота)

[Протокол\_He-Su](https://ru.wikipedia.org/wiki/Протоколы_тайного_голосования#Протокол_He-Su)

[Протокол\_на\_основе\_ANDOS](https://ru.wikipedia.org/wiki/Протоколы_тайного_голосования#Протокол_на_основе_ANDOS)

Источники:

<https://ru.wikipedia.org/wiki/Протоколы_тайного_голосования#Требования_к_системам_тайного_голосования>

<https://habr.com/ru/company/analogbytes/blog/502376/>