2025

Архитектура доверия

Краткий аналитический отчёт
по ключевым темам создания
честной системы ДЭГ

Отчет подготовлен
экспертной группой Петра Лосева

1

Введение

1.1 Цели и задачи исследования

Цели

Описать устройство системы дистанционного электронного голосования (ДЭГ), собрать спектр теоретических вопросов и практических проблем, которые необходимо исследовать для разработки системы электронного голосования, заслуживающей доверие со стороны участников избирательного процесса.

Задачи

1. Разработать первичный документ, который станет основой для создания технического задания на систему ДЭГ
2. Определить ключевые принципы, требования и архитектурные решения для обеспечения надежности, прозрачности и безопасности системы.
3. Выявить технологические и организационные аспекты, влияющие на доверие к системе ДЭГ.

1.2

Словарь терминов

Блокчейн *(Распределённая система)*

Система, в которой множество равноправных и независимых участников (узлов) совместно ведут единый реестр записей. Данные синхронизируются без централизованного управления, что обеспечивает устойчивость, доверие между сторонами и защиту от одностороннего контроля или подмены информации.

Нода блокчейна

Узел (компьютер или сервер) в сети блокчейна, хранящий копию цепочки блоков и участвующий в поддержании ее целостности и функционирования.

Разделение секрета *(Secret Sharing)*

Криптографический метод, при котором секретный ключ делится на части, распределяемые между участниками. Для восстановления ключа требуется объединение всех или некоторого количества частей.

Слепая подпись *(Blind Signature)*

Криптографический протокол, позволяющий подписывать сообщение без раскрытия его содержимого, обеспечивающий анонимность и защиту от подмены.

Консенсусный механизм

Алгоритм, с помощью которого участники распределенной системы достигают согласия о содержимом общего реестра данных. Важен для обеспечения согласованности записей в условиях отсутствия централизованного контроля.

Дистанционное электронное голосование *(ДЭГ)*

Форма голосования, позволяющая избирателям отдавать голоса удаленно через интернет с использованием специализированных программных решений.

Блокчейн *(База данных)*

Распределенная и криптографически защищенная база данных, реализованная в виде последовательной цепочки блоков. Обеспечивает неизменяемость, верифицируемость и защиту от несанкционированных изменений.

Нода наблюдения

Специализированный узел в системе ДЭГ, предназначенный для мониторинга, аудита и обеспечения прозрачности процессов голосования.

Криптографический ключ

Секретная или публичная информация, используемая для шифрования и расшифровки данных, обеспечивающая безопасность и конфиденциальность.

Смарт-контракт

Программный код, автоматически выполняющийся при наступлении определенных условий и фиксирующий правила формирования и записи транзакций в блокчейне.

Гомоморфное шифрование

Метод шифрования, позволяющий выполнять вычисления над зашифрованными данными без их расшифровки.

Логирование

Сбор и хранение событий, происходящих в системе.

Агентство

Институализированный участник системы голосования, обладающий определённой ролью и полномочиями, независимый от других участников.

1.3 Базовая архитектура ДЭГ и блокчейн-системы

Электронное голосование — не просто программа для подсчета голосов, а сложная система взаимосвязанных компонентов и процедур: от формирования списков избирателей и механизмов идентификации и авторизации до непосредственно голосования и механизмов контроля со стороны участников избирательного процесса.

Дистанционное голосование может применяться в разных контекстах. Например, в корпоративных структурах и в общественных организациях при принятии коллективных решений, как механизм выявления общественного мнения, как часть избирательного процесса, как инструмент прямой демократии на различных уровнях организации общественной жизни. Детали архитектуры и реализации, организация процессов могут существенно различаться для оптимизации баланса рисков и открытости, удобства использования и гарантий целостности. Заложенные в систему принципы голосования (например: тайность, конфиденциальность или открытость голосования; заявительное, автоматическое или обязательное участие в голосовании) и сопутствующие процедуры также могут варьироваться в зависимости от контекста использования. В конкретной реализации, вероятно, придется учитывать интересы и требования тех или иных институциональных акторов, вовлеченных в избирательный и политический процесс. Все это влияет на выбор архитектурных решений для системы ДЭГ и на совокупность процедур контроля работы системы со стороны заинтересованных участников.

Несмотря на контекстуальную зависимость можно выделить набор универсальных принципов и архитектурных решений. Например, в качестве технологического ядра для проведения транзакций и хранения данных целесообразно использовать блокчейн-системы.

Термин «блокчейн» в электронном голосовании используется в двух значениях. С одной стороны, он обозначает распределенную систему консенсуса — способ достижения доверия между участниками сети без централизованного управляющего органа. С другой стороны, блокчейн понимается как особая архитектура хранения данных — упорядоченная и криптографически связанная цепочка записей, обеспечивающая их неизменяемость.

В системах электронного голосования чаще применяется именно второй подход: блокчейн используется как база данных с встроенными мерами защиты от подмены и несанкционированного доступа. Такой формат позволяет интегрировать в систему механизмы прозрачности и аудита без необходимости реализовывать полноценный децентрализованный консенсус. Тем не менее, существуют решения, в которых реализована и распределенная модель управления — в таких случаях база данных является неотъемлемым компонентом распределенного протокола, обеспечивающего независимое участие узлов сети в хранении и проверке данных.

Блокчейн как база данных представляет собой особую архитектуру ведения реестров — криптографически защищенную, неизменяемую и доступную для проверки цепочку записей, отражающих волеизъявления и сопутствующие события голосования. Вместе с протоколами взаимодействия такая система может обеспечить как защищенное хранение, так и доступ к данным для последующего контроля и аудита.

1.3

Полноценный блокчейн — это совокупность технологий, предназначенных для решения различных задач, от распределенного консенсуса до устойчивого хранения данных. Например, в криптовалютах блокчейн реализует именно распределенные механизмы управления и хранения, обеспечивая независимость участников сети и автоматическую верификацию операций.

Существует широкий спектр открытых блокчейн-платформ, которые могут быть адаптированы под нужды электронного голосования путем разработки надстроек, учитывающих особенности конкретного контекста. К основным преимуществам таких систем относят прозрачность, встроенную в архитектуру, криптографическую целостность записей, распределенность хранения и устойчивость к несанкционированным изменениям.

Однако такие качества, как полная децентрализация и анонимность, не всегда применимы в условиях публичного голосования: например, требование верификации избирателя и управляемости процесса со стороны уполномоченных органов нередко вступает в противоречие с принципами классического блокчейна. Это требует адаптации технологий и сводит на нет часть их преимуществ. В российской практике уже существуют прецеденты применения блокчейн-решений в избирательной сфере, что может быть использовано при проектировании и внедрении новых систем ДЭГ. В государственных российских системах дистанционного электронного голосования распределенность используется лишь на техническом уровне: весь процесс контролируется централизованной государственной структурой. Однако в перспективных реализациях возможно задействовать более подлинную распределенность и расширить функциональность, что позволит повысить уровень доверия к системе.

Спектр ожиданий от систем ДЭГ также многослоен. Общими требованиями со стороны большинства участников выборной процедуры являются надежность, прозрачность функционирования и гарантии целостности голосования. При этом важным фактором остается удобство использования как для голосующих, так и для организаторов выборов.

Систему дистанционного электронного голосования можно условно разделить на несколько универсальных компонентов:

1 Подсистема работы со списками участников голосования

Обеспечивает составление списков или регистрацию голосующих, хранит персональную информацию участников голосования.

2 Подсистема авторизации

Комплекс технических средств и процедурных решений, позволяющих убедиться, что подключающийся удаленный участник имеет право голосовать.

3 Собственно система голосования

Принимает и регистрирует выбор избирателя, обеспечивая хранение волеизъявления в базе данных (блокчейне), обеспечивает реализацию протоколов валидации, проверки целостности и неизменности волеизъявления.

4 Система подведения итогов

Реализует подсчет результатов голосования, проводит необходимые проверки. Может быть реализована и как интегрированная часть системы голосования, и как технически и организационно независимая система.

5 Портал ДЭГ

Портал в Интернете, обеспечивающий публикацию информации о голосовании и его итогах, который может служить точкой входа для участников голосования и с помощью которого могут быть реализованы инструменты удаленного мониторинга работоспособности и целостности системы ДЭГ.

1.4 Основные роли в избирательном процессе *(и ином процессе голосования)*

- Избирательная комиссия или иной орган, непосредственно организующий голосование
- Кандидаты, партии, инициативные группы референдумов, в неэлекторальных контекстах — иные институализированные группы, выдвигающие кандидатов и заинтересованные в исходах голосований
- Избиратели, участники референдума, в неэлекторальных процедурах — голосующие лица
- Наблюдатели (обычно от общественных объединений, кандидатов или партий), в неэлекторальных процедурах — аудиторы, наблюдающие представители кандидатов и заинтересованных сообществ

1.5 Основные этапы дистанционного электронного голосования

1 Формирование списков избирателей

Для каждого проводимого голосования в систему ДЭГ загружаются актуальные списки избирателей (с подтвержденным правом голосования), которые имеют право получить электронный бюллетень.

2 Криптографическая пара ключей

Перед запуском голосования генерируется пара ключей: **шифрующий** и **расшифровывающий**.

- **Ключ шифрования** загружается в систему ДЭГ и используется для обеспечения целостности и анонимности голосов избирателей, а также для защиты данных от несанкционированного доступа.
- **Ключ расшифрования** либо хранится целиком, либо делится на части и распределяется между несколькими независимыми участниками для исключения расшифрования промежуточных итогов волеизъявления до завершения голосования.

3 Аутентификация избирателей

В течение установленного периода голосования избиратель проходит авторизацию для участия в электронном голосовании. Система проверяет его право голосовать и (в той или иной мере) самоличность голосования.

1.5

4 **Выдача электронных бюллетеней**

Авторизованный избиратель получает доступ к соответствующим электронным бюллетеням.

5 **Заполнение и шифрование бюллетеней**

Избиратель заполняет электронный бюллетень (на своем электронном устройстве или на ином устройстве, авторизованном избирательной комиссией). Выбранные варианты голосования шифруются с использованием ключа шифрования.

6 **Анонимизация**

Электронные бюллетени с волеизъявлением в зашифрованном виде отправляются в систему ДЭГ таким образом, чтобы система не могла связать бюллетень с конкретным избирателем.

7 **Запись данных в блокчейн**

Зашифрованные бюллетени и связанные транзакции записываются в блокчейн — открытый реестр, доступный для просмотра широким кругом участников.

8 **Завершение голосования**

Голосование завершается по окончании установленного периода: система ДЭГ перестает выдавать и принимать электронные бюллетени.

9 **Сборка ключа расшифровки**

В зависимости от выбранной схемы: ключ расшифрования либо собирается из частей, либо извлекается из хранилища целиком и используется для расшифрования зашифрованного волеизъявления.

10 **Расшифровка бюллетеней и подведение итогов**

Зашифрованные электронные бюллетени расшифровываются, голоса избирателей суммируются.

11 **Публикация результатов и ключа**

Итоги голосования и ключ расшифрования публикуются (в блокчейне, на портале ДЭГ) для проверки подведения итогов заинтересованными сторонами.

1.5

Примечание

В рамках соблюдения основных принципов голосования допустимы отклонения от описанной схемы. Например, используемое в российской федеральной системе ДЭГ гомоморфное шифрование дает возможность подвести итоги не расшифровывая все бюллетени, что однако имеет и отрицательные стороны. Также с определенного момента в этой системе перестали выкладывать в публичный доступ ключ расшифрования после завершения голосования. Подобные отклонения сужают возможности проверки целостности системы, что негативно отражается на доверии. Также возможны разные схемы анонимизации. Например, в эстонской системе интернет-голосования анонимизация проводится при публичном контроле на начальном этапе подведения итогов.

2

Учет опыта разработки и проведения ДЭГ

2.1 Применение электронного голосования в разных странах

История ДЭГ и выборов в России имеет ярко выраженную специфику, что делает независимый зарубежный опыт, сформированный вне российской правовой и политической среды, особенно ценным для выхода за рамки сформированных внутренних ограничений.
Перед разработкой конкретного технического задания полезно обратиться к международному опыту внедрения и учесть его при создании собственной системы. Анализ успешных и неудачных практик позволит полнее рассмотреть риски и ограничения, использовать продуманные идеи по процедурам и безопасности, механизмы прозрачности и способы повышения доверия к системе. Сейчас электронное голосование полноценно применяется только в Эстонии. В более чем десятке стран, среди которых Швейцария и Канада, ДЭГ используется на выборах в отдельных муниципалитетах или провинциях либо для ограниченных категорий граждан (например, пребывающих за границей).
Но и в этих странах, и в ряде стран, где по совокупности причин ДЭГ не стали применять, накоплены исследовательские материалы и отчеты разработчиков, доступные публично.

2.2 Опыт стран, внедривших ДЭГ, и отказавшихся от внедрения

Целесообразно проанализировать, по каким причинам дистанционное электронное голосование не получило широкого распространения в странах с устойчивыми демократическими системами. Несмотря на определенные преимущества такого способа голосования — удобство для избирателей, скорость и потенциальную прозрачность, отмечались существенные недостатки, которые заставляли либо отложить внедрение, либо существенно ограничить применение ДЭГ (среди таких стран, как Норвегия, Германия, Великобритания, частично Канада и Швейцария). Спектр таких причин

достаточно широк: неустранимые технологические риски вмешательства или сбоев, которые в силу централизации могут оказать неприемлемое влияние на учет волеизъявления; недостаточная совместимость со стандартами избирательных процедур, особенно в части прозрачности, самоличности и добровольности волеизъявления, сложности с организацией полноценного внешнего наблюдения, которое доказывало бы отсутствие нарушений и вмешательств либо эффективно их выявляло. Непубличность процедуры дистанционного голосования при прочих равных вызывает меньшее доверие результатам и по психологическим причинам.

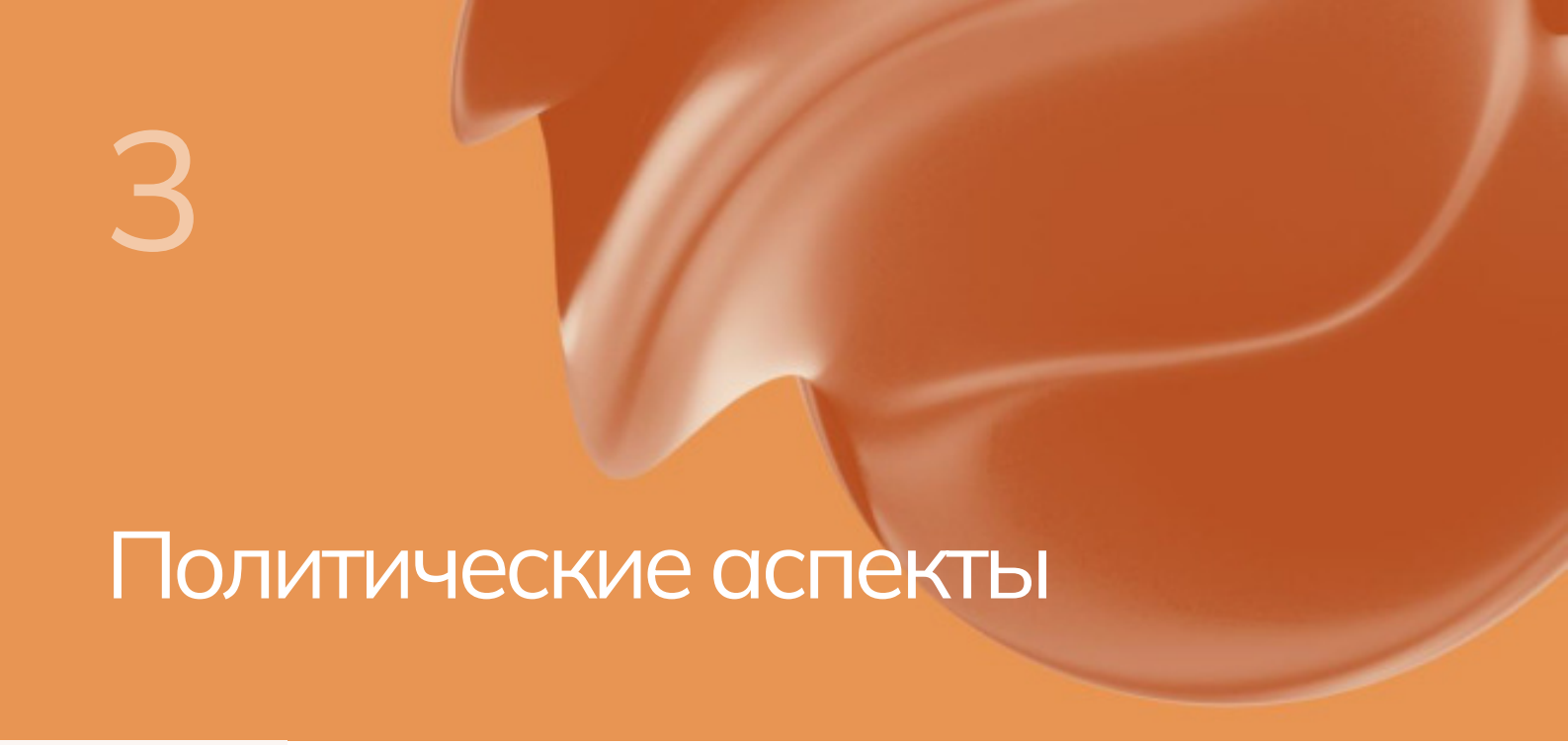
При проведении экспериментов и внедрении ДЭГ было непросто добиться достаточного политического согласия ведущих политических сил. В некоторых странах отмечалось недостаточное проникновение или доверие к системам типа электронного правительства, отсутствие распространения биометрических или криптографически защищенных цифровых ID среди населения, что не позволяет использовать более надежные способы верификации. Все это полезно учесть при разработке собственной системы, и, зная контекст ее применения на чужом опыте и исследовательской базе, рассмотреть разные варианты реализации.

2.3 Анализ текущих реализаций систем электронного голосования в России и их критика

В России существует две системы ДЭГ — федеральная и московская, которые уже неоднократно использовались на реальных выборах. Каждая из них имеет не только свои особенности, но и существенные различия между версиями. Анализ этих систем поможет выявить вектор развития и понять основные направления критики текущих реализаций. В силу политического контекста, фактически не было свободной публичной дискуссии по этим темам. Доступом к информации о системах обладали лишь разработчики проектов и внешние эксперты, неформально привлекавшиеся к внутренним дискуссиям в рамках Технической рабочей группы при московской системе и группы экспертов при Общественной Палате РФ. (Публично доступные материалы доступны только от имени первой группы экспертов.) Тем не менее, и имеющаяся информация о системах, реакция политических сил и избирателей на использование ДЭГ на выборах и связанные с этим скандалы позволят точнее оценить перспективы определенных архитектурных и процедурных решений.

2.4 Коммерческие продукты в области электронного голосования

Системы дистанционного голосования применяются не только в государственных электоральных процедурах, но и во внутренних голосованиях в коммерческих структурах, например, при выборах в советы директоров. Анализ таких коммерческих решений позволяет лучше понять, какие функции и свойства оказываются наиболее востребованными на практике вне полноценного государственного регулирования: от удобства пользовательского интерфейса до механизмов безопасности и масштабируемости. Есть и российские разработки в этой области, например блокчейн-система дистанционного голосования Polys, разработанная в 2018 году под эгидой Лаборатории Касперского, и отчасти легшая в основу московской системы ДЭГ.



3

Политические аспекты

3.1 Обоснование внедрения ДЭГ

Дистанционное электронное голосование в рамках избирательного процесса — это не только техническая реализация, но и политическое решение. Даже при достижении определенности в общих принципах и правилах проведения (что уже непросто), разногласия могут возникнуть на этапах согласования технического задания и реализации, где придется взвешивать риски и интересы, заведомо не имея консенсусного или идеального варианта. При разработке и внедрении подобных систем инициатор должен четко представлять спектр заинтересованных акторов и понимать, какие компромиссы и с чьими интересами допустимы.

Необходимо определить, для чего создается система электронного голосования и в каком политическом и правовом контексте она будет использоваться. От этого будут зависеть и выбор архитектуры и детали реализации: взаимодействие с государственными структурами предполагает одни подходы и технические решения, тогда как системы для общественных или частных организаций более свободны в выборе архитектуры.

Примеры дилемм и вопросов, которые могут возникнуть при разработке системы: важна или не важна реальная децентрализация основной базы данных; есть ли институализированное «второе агентство», с которым можно разделить часть технических функций в рамках более безопасных и устойчивых протоколов; насколько и до какой степени организатор должен предоставлять участникам выборов и избирателям проверять корректность работы системы, либо часть вопросов можно «закрыть» доверием организатору; какова ожидаемая пиковая нагрузка на систему и насколько технические возможности и пропускные способности сети будут ограничивать выбор реализации блокчейна, криптографических решений, пропускной способности сетей и производительности серверного оборудования, и т.д.

Однако разработка универсальной системы дистанционного голосования также может иметь смысл. При том что архитектура будет различаться в зависимости от контекста применения, разные реализации могут использовать общее ядро и разработанные протоколы, и адаптация потребуется лишь на уровне отдельных модулей.

3.2 Опыт взаимодействия с организаторами выборов и разработчиками государственных систем электронного голосования

Взаимодействие независимых экспертов, представителей политических партий и организаторов выборов также имеет свою специфику. В ходе контактов, в частности при внедрении ДЭГ в России, поднималось немало вопросов и было высказано немало критических замечаний, однако нельзя сказать, что это существенно повлияло на вектор развития российских систем ДЭГ. Политический расклад предполагал существенное несовпадение интересов и отсутствие необходимости искать оптимальные решения и компромиссы: организаторы выборов были заинтересованы заранее услышать критику, разработчики были заинтересованы обсудить более широкий набор идей и решений, но итоговые решения принимались в итоге из политической целесообразности, предполагающей наличие в руках организаторов непрозрачного инструмента проведения выборов. Легитимизация результатов строилась не через «доверие через проверки», а через подавление критики в публичном пространстве и активный пиар внедряемых решений. Это естественное положение дел в рамках нынешней политической системы. Однако при возвращении конкурентной политической среды и при разъединении вертикали власти и роли организаторов выборов с неизбежностью возникнут качественно иные установки и ожидания. При рассмотрении вопроса о разработке системы ДЭГ важно это учитывать.

3.3 Карта взаимодействия с органами власти

ДЭГ — это система, которая взаимодействуют с другими информационными системами, в том числе государственными, за каждой из которых стоит ответственное ведомство или владелец. Чтобы учесть аспекты такого взаимодействия, необходимо построить полную карту бизнес-процессов и потоков информации. Это определит точки интеграции и дополнительные риски информационной безопасности, разграничит зоны ответственности. Потребуется разработать регламенты взаимодействий и протоколы обмена данными с внешними подсистемами. Такая карта станет основой для разработки полного технического задания, обеспечит согласованную работу ДЭГ, повысит управляемость разработки и надежность системы.

3.4 Вопрос сертификации и процедурных требований

Разработка системы ДЭГ в Российской Федерации требует соблюдения нормативных и процедурных требований, направленных на обеспечение безопасности, защиты персональных данных и устойчивости критической информационной инфраструктуры. Для создания системы, соответствующей законодательству и обеспечивающей доверие со стороны надзорных органов и пользователей, необходимо изучить и сформировать полный перечень нормативных актов и процедур.

Формирование такого перечня позволит разработать систему ДЭГ, соответствующую требованиям законодательства, минимизировать юридические риски и риски в области информационной безопасности, а также повысить доверие со стороны надзорных органов, избирателей. Регулярное обновление нормативной базы (например, новых приказов ФСТЭК и ФСБ) и разработка модели угроз безопасности информации в соответствии с методическими рекомендациями ФСБ и ФСТЭК являются обязательными для обеспечения актуальности системы.

Данный аспект потребует привлечение профессиональных юристов к разработке системы ДЭГ, ориентированной на применение в России.

3.5 Лоббизм и интеграция в реальную систему

Для успешного внедрения системы дистанционного электронного голосования (ДЭГ) необходим комплексный план интеграции с существующей государственной и коммерческой инфраструктурой, а также работа по обеспечению поддержки со стороны органов власти, общественности и ключевых заинтересованных сторон. Интеграция включает разработку программных интерфейсов для совместимости с единой системой идентификации и аутентификации (ЕСИА) в соответствии с регламентом ЕСИА, согласование с операторами ЦОД (например, Ростелеком), а также сотрудничество с операторами сотовой связи и провайдерами интернета для стабильного доступа и двухфакторной аутентификации. Для кибербезопасности требуется разработка модели угроз и стресс-тестирование системы на устойчивость к атакам.

Продвижение системы предполагает взаимодействие с Минцифры, ЦИК РФ, ФСТЭК и ФСБ, участие в публичных площадках, а также формирование положительного имиджа через СМИ и общественные обсуждения. Хорошим дополнением усилий по лоббированию и GR стал бы независимый академический аудит системы. Управление юридическими, техническими, социальными и финансовыми рисками, включая соответствие ФЗ № 152-ФЗ от 27.07.2006 и ФЗ № 187-ФЗ от 26.07.2017, минимизирует угрозы штрафов и повысит легитимность системы, укрепляя прозрачность и доступность избирательных процессов.

4

Архитектурные решения

4.1 Тип дистанционного электронного голосования

Можно выделить ряд определяющих вопросов при планировании возможной архитектуры ДЭГ, выбор между которыми зависит от контекста и не является предметом консенсуса. У разных вариантов есть свои преимущества и недостатки. Решения по ним должны быть зафиксированы до старта разработки.

Для начала стоит зафиксировать, является ли ДЭГ исключительно голосованием избирателей через интернет, либо это голосование через терминалы электронного голосования, либо используется комбинированная схема.

(Мы предполагаем, что бумажное голосование остается основной формой волеизъявления на выборах, однако для иных типов голосования может быть рассмотрен вариант только дистанционного голосования). В российской практике реализованы оба варианта. Выбор модели влияет на набор технических решений, архитектуру безопасности, интерфейсы взаимодействия с избирателем, логистику процесса голосования, нормативную базу, и косвенно, на степень доверия общества.

4.2 Открытость технологий

Планируя процесс разработки, важно заранее определиться в степени открытости технологий и программного обеспечения, разрабатываемых для системы ДЭГ. Данное решение повлияет на выбор технологий и частично на решения по информационной безопасности.

Вопрос открытости технологий в существующих российских системах ДЭГ отчасти упирается в существующее нормативное регулирование, в коммерческие интересы разработчиков, а также в политические интересы и желание минимизировать прозрачность системы. В мировой практике также используются разные подходы: использовались и системы ДЭГ, основанные на коммерческих решениях и без публикации исходных кодов, есть и открытые подходы с открытыми исходными кодами. К достоинствам открытых систем можно отнести лучшую защищенность, прежде всего в силу более широкого и независимого аудита.

Открытость позволяет неограниченному кругу экспертов из академической и политической среды проводить аудит, выявлять уязвимости и подтверждать корректность и защищенность алгоритмов. При прочих равных, такие системы вызывают более широкое доверие пользователей в силу большей прозрачности. С другой стороны, решения на коммерческой основе нередко имеют уже накопленный опыт эксплуатации, быстрее адаптируются разработчиком. Кроме того, закрытость кода дает меньше возможности внешним злоумышленникам обнаружить уязвимости конкретной реализации.

Выбор осложняется тем, что система ДЭГ интегрируется во внешнюю серверную инфраструктуру и системы связи и сама представляет собой комплекс взаимосвязанных модулей — помимо реализации механизма непосредственно голосования, она включает системы авторизации, ведения списков избирателей, что предполагает интеграцию с различными государственными информационными системами. На практике допустимо использовать комбинированные подходы, определить степень открытости для различных компонентов независимо. Это позволит сбалансировать потребности в безопасности и прозрачности, более гибко определять зоны ответственности разработчиков и операторов.

4.3 Степень децентрализации инфраструктуры

Инфраструктура электронного голосования может быть децентрализованной — например, ноды блокчейна могут находиться под контролем разных акторов («агентств»). Важно заранее определить, какой тип инфраструктуры будет использоваться, насколько глубокой и какой именно предполагается децентрализация.

Условно можно выделить два подхода:

1 Централизованный подход

При котором критически важные элементы системы находятся под управлением одной стороны, а децентрализованные элементы используются лишь для (частичной) проверки целостности. Такой подход упрощает управление и снижает техническую сложность системы, однако требует высокой степени доверия к фактическому оператору.

2 Децентрализованный подход

При котором основные механизмы и управление распределены между независимыми агентствами. Этот вариант повышает уровень доверия и прозрачности, поскольку исключает возможность монополизации контроля, но одновременно увеличивает сложность архитектуры, требует более высокой квалификации организаторов и повышает вероятность сбоев.

4.3

В любом случае схема распределения нод и их функционал должны исключить захват полного контроля над системой одной стороной. Находящиеся под контролем разных агентств данные и процедуры должны обеспечить максимально возможное число взаимных проверок целостности и непротиворечивости. Это критично для обеспечения доверия к результатам голосования и устойчивости всей архитектуры. Децентрализация (наличие минимум двух независимых агентств) может быть эффективным инструментом гарантии тайности голосования. С другой стороны, чем больше децентрализована система, тем сложнее восстанавливать работоспособность системы при сбоях или атаках, что может быть критично в условиях ограниченности времени голосования.

В итоге, с одной стороны, децентрализация способствует укреплению доверия к голосованию, обеспечивая большую прозрачность и защиту от манипуляций. С другой стороны, умножение элементов и агентств, контролирующих свои части системы ДЭГ, усложняет управление и эксплуатацию системы, что повышает риск сбоев и ошибок. При проектировании инфраструктуры необходимо тщательно взвесить эти факторы и выбрать оптимальный баланс между степенью децентрализации, надежностью и удобством эксплуатации.

4.4

Разделение ключей

Одной из устоявшихся процедур в системах электронного голосования является разделение ключей в рамках механизма разделения секрета (secret sharing). Она предполагает, что ключ, используемый для расшифрования результатов выборов, до начала голосования разделяется и распределяется между несколькими независимыми сторонами, что затрудняет возможность несанкционированного доступа к информации о волеизъявлении до завершения голосования. Для того чтобы процедура разделения ключей была реальной, а не номинальной, она должна быть продумана с учетом рисков потери или недоступности частей ключа, а также обеспечивать невозможность незаметного копирования сформированного ключа.

Важно найти оптимальный баланс между обеспечением высокой степени безопасности и устойчивостью системы к саботажу, ошибкам или техническим сбоям. В российской практике сформировалась традиция сосредоточения разделенных частей ключа в руках ограниченного круга лиц, зачастую принадлежащих одной стороне, что полностью лишает процедуру ее первоначального смысла и снижает уровень доверия к системе.

5

Архитектурные дилеммы и компромиссы

5.1 Проверка корректности учета собственного голоса избирателем

В силу невозможности непосредственного контроля корректности работы сложной электронной системы голосования (даже при открытости кода системы), стандартным средством защиты от незаметной подмены голосов является схема, когда избиратели могут найти свой бюллетень среди зашифрованных бюллетеней, хранящихся в блокчейне до окончания голосования, а после расшифрования голосов — найти свой бюллетень с расшифрованным голосом.

Это качественно усложняет незаметную подмену волеизъявления или неправильное зашифрование голосов, а наличие полного набора расшифрованных бюллетеней, среди которых любой избиратель может однозначно идентифицировать свой — страхует от некорректного подведения итогов.

Однако в электоральной практике современной России существенное влияние на результат оказывает использование административного ресурса, когда администрации бюджетных и крупных окологосударственных предприятий в той или иной мере контролируют волеизъявление сотрудников. Поэтому возможность проверки корректности учета собственного голоса может облегчить контроль голосования администрациями или схему скупки голосов.

Таким образом, возникает парадоксальная ситуация: чем более верифицируемой и прозрачной становится система электронного голосования, тем выше риск того, что она будет использоваться для контроля над волеизъявлением

Здесь необходимо определенное политическое решение. Поскольку актуальность проблем админресурса и массового подкупа можно снизить иными способами, то целесообразно закрепить приоритет в этом вопросе за прозрачностью и соответствующим образом выстраивать архитектуру системы (включая способы идентификации, форматы электронных бюллетеней, механизмы анонимизации и проверки собственного голоса). Однако при этом подходе требуется заранее учитывать потенциальные формы вмешательства через административный ресурс и предусматривать технические и процедурные меры защиты на каждом уязвимом участке. С учетом случившейся публичной дискредитации переголосования из-за якобы сбоя и вероятных фальсификаций в московской системе ДЭГ на выборах в Госдуму в 2021 году, важно не только технологическое, но и стратегическое обоснование

5.1

выбранного подхода, готовность защищать выбор в публичной и экспертной дискуссиях.

Возможная альтернатива — проводить доказательство корректности зашифрования голоса криптографическими методами и подводить итоги без расшифрования бюллетеней с криптографическим доказательством корректности суммирования (как реализовано в федеральной системе ДЭГ на основе гомоморфного шифрования).

Однако на практике эти методы не решают проблему доверия в полной мере, поскольку, с одной стороны, для доверия требуется раскрытие параметров криптографических алгоритмов и доказательство невозможности их компрометации, а с другой — понимание этих вопросов недоступно не только рядовым избирателям, но и специалистам в близких областях. Что не соответствует базовому механизму доверия — возможности проверки сомнений и подозрений широким кругом независимых и неангажированных сторон.

5.2 Переголосование

Одним из наиболее дискуссионных и важных вопросов при проектировании системы дистанционного электронного голосования является допустимость процедуры переголосования. В теории и мировой практике такая схема для дистанционного непубличного голосования признается эффективным и практичным способом защиты от массовой скупки голосов и непосредственного влияния на волеизъявления (через административное принуждение и личное влияние). Возможность переголосовать обесценивает схемы подкупа или подконтрольного голосования, поскольку избиратель, проголосовавший недобровольно или под влиянием, может до окончания периода голосования изменить свое волеизъявление (в теории многократно). При наличии переголосования единственный способ контроля – заставить всех подконтрольных голосовать в последние минуты голосования, что трудно организовать в сколько-либо существенном масштабе и сложно скрыть. Также переголосование естественным образом страхует от потери избирательного права из-за технических проблем со связью или используемым устройством.

Однако с учетом распространенности административного контроля и структурных искажений избирательного процесса в реальных российских условиях неочевидной задачей оказывается совмещение возможности проверки корректности учета собственного голоса (предполагающее способ однозначно верифицировать свои бюллетени), полного контроля избирателя за действиями в системе ДЭГ от его имени и возможности повторного голосования при сохранении того, что работодатели или скупщики голосов не смогут эффективно отслеживать и контролировать все волеизъявления избирателя.

Кроме того, при внедрении возможности переголосования в ДЭГ в России придется преодолевать негативные последствия скандала 2021 года в Москве, где внезапно и некорректно внедренное переголосование («отложенный бюллетень») с большой вероятностью использовалось как одна из схем фальсификации. Из-за отсутствия механизма контроля избирателем всех действий в ДЭГ от своего имени (выдача бюллетеня, прием бюллетеня), из-за полного контроля и системы ДЭГ и системы аутентификации СУДИР одним ведомством и полной непрозрачности этапа авторизации для наблюдателей, из-за введения теневого непубличного блокчейна учета переголосований, который в итоге не показали ни наблюдателям, ни экспертам,

5.2

у фактических организаторов электронного голосования появилась возможность переголосовывать от имени избирателей (без их ведома).

Корректное и прозрачное переголосование в российских условиях потребует усложнения архитектуры системы и процедур контроля со стороны наблюдателей. Что требует страховки привносимых дополнительных рисков в части информационной безопасности.

Кроме того, с большой вероятностью потребуется публичная защита выбора решения с переголосованием, причем не только в части объяснения случившегося в 2021 году, но и из-за критики различия между электронным и традиционным голосованием, в котором подобная возможность отсутствует. Вопрос о целесообразности принятия подобных рисков либо полного отказа от практики переголосования остается дискуссионным и не имеет однозначного решения.

5.3 Тайность волеизъявления и анонимность голосования

Еще один сложный вопрос в теории электронных систем голосования — способы обеспечения и гарантии тайны волеизъявления. В традиционном голосовании тайность обеспечивается механически — путем естественного перемешивания непронумерованных, неразличимых бюллетеней в ящиках для голосования. Гарантия тайности также поддерживается публичным характером голосования на избирательных участках в присутствии наблюдателей.

В распределенных электронных системах циркулирует большое количество избыточной информации, частично сохраняемой в логах. Несмотря на наличие в системах ДЭГ механизмов анонимизации, на практике невозможно доказать участникам выборов, что реально исполняемый код и серверное программное обеспечение не ведут логирование информации, позволяющей восстановить связь между избирателями и их анонимизированными бюллетенями в блокчейне – со стороны организаторов, провайдеров серверного оборудования.

Вопрос возможной деанонимизации голосов принципиально упирается в доверие организаторам дистанционного электронного голосования и реально исполняемому коду системы ДЭГ. Что, учитывая историю российской электоральной практики, является серьезной проблемой, фактически лишающей свободы волеизъявления административно контролируемых избирателей, и тем самым подрывающей легитимность итогов ДЭГ.

В этой связи стоит отметить, что практика использования терминалов электронного голосования или специальных приложений для голосования с закрытым исходным кодом усугубляет проблему анонимности волеизъявления, поскольку увеличивает сбор информации о действиях избирателя со стороны организаторов.

Архитектурно, основным путем исправления проблемы считается подход «двух агентств», когда одно агентство выдает бюллетени (для чего в том или ином виде требуется идентификация избирателя с целью проверки его избирательного права и защиты от многократного голосования), а другое агентство принимает анонимизированные бюллетени на хранение (проверяя лишь подлинность бюллетеня).

Возможна и альтернативная схема, когда одно агентство выдает и принимает на хранение зашифрованные бюллетени (без возможности их расшифровать), а другое агентство под контролем наблюдателей/аудитов на несвязанном с сетью контролируемом оборудовании

анонимизирует массив бюллетеней и проводит расшифровку и подсчет с использованием прозрачных и контролируемых скриптов.

В современных российских реалиях сложность реализации схемы двух агентств заключается в отсутствии реально независимых институций среди государственных органов и желании властей максимально контролировать процесс голосования, не подпуская к нему возможные независимые институции извне государственной вертикали.

Поэтому при реализации системы ДЭГ в России следует архитектурно предусмотреть техническое разделение компонентов аутентификации/авторизации, проверки избирательного права и выдачи бюллетеней, приема и хранения зашифрованных бюллетеней и компонента подведения итогов. И исходя из актуальных политических реалий искать максимально независимую, политически не ангажированную институцию на роль второго агентства для выделения контроля над одним из трех последних узлов цепочки работы с бюллетенями.

5.4 Протоколы действий при сбоях, атаках и восстановлении данных

Следует заранее определить алгоритмы действий на случай сбоев в работе системы дистанционного электронного голосования. Сбои могут быть вызваны как техническими неисправностями и ошибками в коде, так и злонамеренными атаками. Возможны различные сценарии реагирования — от полной отмены голосования в случае серьёзных нарушений, затрудняющих достоверное определение результатов, до регламентированного восстановления работоспособности системы и, возможно, данных.

При выборе второго сценария особое значение приобретает наличие чётких процедур и технических решений, которые позволяют избирательным комиссиям, наблюдателям и участникам выборов убедиться в том, что в процессе сбоя и восстановления не произошла утрата или фальсификация информации о волеизъявлении и других критически важных данных.

Кроме того, необходима быстрая и прозрачная оценка масштабов сбоя, в том числе определение круга затронутых (не анонимизированных) пользователей, а также оперативное информирование граждан о необходимых действиях для реализации избирательного права. Все эти положения должны быть четко зафиксированы в регламентах и доведены до сведения участников избирательного процесса до начала голосования.

В российской практике сложилась традиция отрицания и сокрытия технических сбоев и иных проблем в ходе голосования и подведения итогов. Такая закрытость дополнительно подрывает доверие граждан к результатам голосования, порождая сомнения в легитимности выборов. Восстановление доверия возможно при кардинальном изменении подхода: обеспечить максимальную прозрачность и открытость процедур, включая своевременное информирование о технических проблемах, публикацию информации о мерах по их устранению.

5.5 Выбор авторизации

Авторизация — один из ключевых модулей системы электронного голосования. Актор, фактически контролирующий этот компонент, получает возможность технического влияния на реализацию избирательного права. Кроме того, это один из самых чувствительных этапов при проектировании и реализации системы, поскольку дистанционность голосования хуже всего вписывается в рамки общепризнанных стандартов демократических выборов. При голосовании в ДЭГ комиссии и наблюдатели не могут непосредственно убедиться, что голосующий действительно является избирателем и голосует самолично, нет эффективного способа отличить голосования реального избирателя и программного бота. Поэтому система аутентификации избирателей должна сама по себе обладать доверием, а процедуры должны обеспечивать защиту от многократного голосования и голосования за другого избирателя, при этом позволяя наблюдателям убедиться в этом, а также в отсутствии вмешательства на этом этапе.

В существующих российских реализациях ДЭГ авторизация осуществляется через сервис ЕСИА, через который граждане авторизуются в госуслуги, и через аналогичный московский сервис СУДИР, аутентифицирующий пользователей в mos.ru. Таким образом, процесс авторизации оказывается завязан на ведомства в системе исполнительной власти, что изначально порождает конфликт интересов. Работа этих сервисов никак не проверяется участниками выборов, нет данных о независимом аудите этих сервисов, что вызывает дополнительные сомнения в защищенности процедуры от вмешательства «изнутри».

Усложняет проблему выбора механизма авторизации нераспространенность в России биометрических и криптографически защищенных электронных паспортов (или иных ID), что не позволяет использовать более защищенные и схемы идентификации и аутентификации.

Если система дистанционного голосования будет использоваться для частных голосований, то возможно использовать более широкий спектр подходов к авторизации, выбор которых определяется контекстом использования. Становятся доступны более гибкие и разнообразные решения – от использования персональных аккаунтов до внедрения биометрии или одноразовых токенов. Однако в любом сценарии должны быть обеспечены высокие стандарты защиты персональных данных, защиты от злоупотреблений извне и изнутри, а также определенная прозрачность процесса для повышения доверия.

Выбор архитектурных решений для этапа авторизации, скорее всего, окажется самым сложным и вызывающим дискуссии. Именно поэтому при проектировании системы необходимо заранее выделить на него достаточное количество времени и ресурсов, а также предусмотреть возможность привлечения независимых экспертов для аудита и верификации механизмов.

6

Структура и компоненты системы

6.1 Научные основания выбора механизма консенсуса

Вопрос реализации механизма консенсуса в блокчейн-системах остается активно развивающимся направлением исследований в области распределенных систем и криптографии. Существует множество алгоритмов, каждый из которых решает задачу достижения согласия между участниками в условиях ненадежных каналов связи и возможного присутствия злоумышленников.

Для выбора подходящего механизма консенсуса необходимо учитывать специфику применения системы: требования к скорости, уровню доверия между участниками, устойчивости к сбоям и потенциальным атакам. Важно опираться на современные научные публикации, чтобы понимать актуальные тенденции, выявленные уязвимости и существующие методы их устранения. Такой анализ необходим для обоснованной оценки применимости того или иного метода в контексте электронного голосования.

Научное сообщество за последние два десятилетия накопило значительный массив знаний о свойствах алгоритмов распределенного консенсуса, методах противодействия атакующим узлам, надежности архитектур систем, а также о неизбежных компромиссах между децентрализацией, безопасностью и производительностью — так называемом треугольнике блокчейна. В научной литературе подробно описаны характеристики алгоритмов консенсуса, вероятностных моделей, гибридных подходов и практик масштабируемости. Изучение этого опыта — не формальность, а необходимое условие при проектировании систем электронного голосования, особенно если предполагается их использование в публичных или государственно значимых процессах. Игнорирование этих наработок или выбор решений на основе интуиции и краткосрочных целей увеличивает риск закладывания уязвимостей в архитектуру системы.

6.2 Требования к инфраструктуре

Необходимо сформулировать четкие требования к пропускной способности системы, исходя из предполагаемой нагрузки и существующих технических ограничений. Система должна быть способна обрабатывать одновременные запросы от десятков до тысяч избирателей, в масштабе региона не должна потерять работоспособность при пиковой нагрузке до миллиона избирателей в час (голосование в течение дня неравномерно). Должна быть предусмотрена защита от DDoS атак. При этом необходимо учитывать ограниченную пропускную способность сетевой инфраструктуры, вычислительные задержки при шифровании и расшифровке бюллетеней, а также ресурсы серверов и узлов блокчейна.

На ранних этапах необходимо провести расчет нагрузки для определения минимально допустимой производительности оборудования, при которой система остается устойчивой и не допускает критических задержек или отказов. На поздних этапах разработки и при внедрении требуется проводить нагрузочные тестирования. При этом должен быть сформулирован регламент действий при предполагаемых перегрузках или атаках. В российской практике есть разделение на несколько параллельных блокчейнов (шардирование) с целью ускорения работы системы. Этот подход может повысить производительность системы в целом, но при этом снижается степень прозрачности и усложняется контроль за неизменностью данных системы.

6.3 Требования к блокчейну и выбор технологии

Технологической основой предлагаемой системы ДЭГ выступает блокчейн-база данных, и при формировании технического задания необходимо будет выбрать одну из доступных технологий. В настоящее время существует широкий спектр блокчейн-реализаций — от публичных и полностью децентрализованных до частных и централизованных, каждая из которых обладает своими преимуществами, недостатками и техническими ограничениями. В связи с этим необходимо проведение отдельного исследования, посвященного сравнительному анализу различных архитектур блокчейн-систем и их применимости в контексте электронного голосования, с учетом специфики политической, правовой и технической среды.

Блокчейн для системы ДЭГ должен иметь самостоятельную, изолированную инфраструктуру, развернутую специально для нужд голосования, с возможностью полного локального управления и мониторинга.

Он не должен быть частью уже существующего публичного блокчейна, так как это создаст дополнительные риски из-за невозможности полного контроля, уязвимостей внешней сети и зависимостью от сторонних валидаторов.

Предпочтительно, чтобы выбранная блокчейн-платформа обладала открытым исходным кодом, была доступна для аудита и имела развитое сообщество, что обеспечит большую прозрачность и устойчивость функционирования. Кроме того, крайне желательно, чтобы платформа поддерживала использование смарт-контрактов — программируемых алгоритмов, которые позволяют формализовать правила проведения транзакций, зафиксировать их непосредственно в коде и обеспечить их автоматическое выполнение без вмешательства извне.

Смарт-контракты значительно повышают уровень автоматизации и прозрачности, снижая риски человеческого фактора и изменения правил в ходе процесса голосования.

6.3

Однако их использование сопряжено с рисками логических и технических ошибок, которые могут привести к серьезным последствиям — искажениям результатов, невозможности расшифровки или преждевременному завершению голосования. В связи с этим разработка и внедрение смарт-контрактов должны сопровождаться многоэтапным аудитом, формальной верификацией и стресс-тестированием, включая участие независимых экспертов.

При выборе блокчейн-архитектуры следует учесть возможность последующего масштабирования системы. При пиковом голосовании избирателей на практике возникали перегрузки блокчейн-подсистем. Одним из примененных в российской практике решений этой проблемы является шардирование — распределение нагрузки между несколькими параллельными инстанциями блокчейна с последующей агрегацией результатов.

Несмотря на выигрыш в производительности такое решение требует нестандартных расширений проверенных блокчейн-решений и создает риски, связанные с согласованностью и верифицируемостью итогов. Возникает необходимость в протоколах перекрестной проверки и объединения данных между шардами, что требует новых механизмов доверия и аккуратной технической реализации.

Выбор конкретных реализации блокчейна и необходимых расширений основан на поиске баланса между прозрачностью, безопасностью и управляемостью, минимизации рисков технологических провалов и претензий из-за закрытости, оптимизации затрат на разработку и эксплуатацию.

6.4 Требования к устройствам голосования

Одной из потенциально уязвимых зон в процессе дистанционного голосования являются пользовательские устройства, с которых осуществляется волеизъявление.

В этом моменте также есть архитектурная дилемма. Система ДЭГ может предусматривать голосование с любых устройств, способных открыть веб-страницу с бюллетенем и исполнять необходимые скрипты, или с заверенных приложений, выпущенных организатором выборов. Первый вариант гарантирует право избирателя голосовать в контролируемой им программной среде, не зависимой от организатора выборов. Второй вариант позволяет организатору предоставить избирателю возможность голосовать в среде гарантированно защищенной от внешнего вмешательства. Предпочтительно предоставить обе возможности, что позволит комфортно голосовать как тем, кто не доверяет организатору, так и тем, кто опасается вирусов и прочих недетектируемых вмешательств в свою программную среду.

В случае голосования с программного обеспечения пользователей речь идет прежде всего о веб-браузерах, установленных на персональных компьютерах, планшетах или мобильных телефонах. На сегодняшний день не зафиксировано достоверных случаев массовой компрометации дистанционного электронного голосования через массовое заражение пользовательских устройств, однако специалисты проводили демонстрации подобных ситуаций и риск такого вмешательства принимается во внимание. Риск возрастает, когда дистанционное голосование проводится в масштабах большой страны и охватывает широкий круг технически неподготовленных пользователей. Помимо вирусов, выдвигаются подозрения о возможности целенаправленного вмешательства в голосование через интернет IT-корпораций, например, через закладки в браузерах и антивирусах.

6.4

Подобные сценарии, однако, требуют тайной подготовки и сложной координации и сопряжены с высокими репутационными и юридическими рисками, так что могут считаться маловероятными.

Важным остается вопрос детектирования массовых несанкционированных вмешательств в процесс голосования. На серверной части инфраструктуры это можно решить стандартными методами, но дополнительный мониторинг окружения на устройствах избирателей со стороны организаторов голосования неприемлем, в силу неконтролируемых возможностей для раскрытия тайны голосования.

Механизм проверки корректности учета собственного голоса дает дополнительную возможность заметить несанкционированное вмешательство, однако обнаружение после завершения голосования не позволит предпринять меры для восстановления избирательного права в рамках проведенного голосования.

6.5

Внеблокчейновая часть архитектуры

Помимо блокчейна в системе ДЭГ присутствуют архитектурные и технические компоненты, которые плохо поддаются децентрализации. Одним из таких важных компонентов является система электронной очереди, служащая промежуточным звеном между избирателем и блокчейн-инфраструктурой. Ее задача — обеспечить стабильную, корректную и последовательную передачу зашифрованных бюллетеней в блокчейн, балансировать нагрузку на блокчейн-компоненты системы. Без этого элемента сложнее гарантировать передачу и запись зашифрованных бюллетеней при высоких нагрузках во время пиковой активности избирателей и DDoS атаках.

Это создает уязвимость с точки зрения наблюдаемости и прозрачности: на этом этапе между получением бюллетеня и записью в блокчейн возможно незаметное вмешательство путем подмены, фильтрации или искусственной задержки голосов. В российских реализациях подобные компоненты закрыты для общественного контроля и не поддаются независимой проверке, что вызывает обеспокоенность у наблюдателей и экспертов.

Одним из возможных путей повышения прозрачности этого компонента ДЭГ является обеспечение логирования действий электронной очереди с параллельной фиксацией соответствующих логов непосредственно в блокчейне. Это усложнит потенциальные изменения и даст возможность провести независимую проверку постфактум. Однако, чтобы это работало на повышение доверия, необходимо обеспечить криптографическое доказательство того, что была запущена именно проверенная и публично доступная версия данного программного компонента, а не модифицированная или скомпрометированная сборка.

При проектировании системы электронного голосования следует уделить особое внимание тем ее элементам, которые не могут быть полностью децентрализованы. Требуется заранее определить, каким образом независимые наблюдатели, технические аудиторы и иные заинтересованные стороны смогут удостовериться в корректности функционирования этих компонентов. Это предполагает не только технические меры, но и организационно-правовые гарантии доступа, прозрачности и сохранения неизменности логов, а также создание процедурных рамок, предотвращающих вмешательство со стороны операторов системы.

6.6 Проверка соответствия исполняемого кода заявленной архитектуре

Возможность независимой верификации исполнения программного обеспечения, задействованного в процессе голосования, является критически важной для доверия к системе. Аудита исходного кода недостаточно — необходимо гарантировать, что в процессе голосования задействована именно эта проверенная, не измененная версия. Для этого могут использоваться механизмы вроде детерминированной сборки, удаленного криптографического заверения исполнения, открытого окружения, доказательств с нулевым разглашением и внешней независимой верификации.

Однако к распределенной серверной инфраструктуре применение таких подходов не практике трудно реализуемо. В то же время, можно создать контролируемое (в том числе публично) окружение на отдельном устройстве без сетевых интерфейсов. На таких устройствах организующая избирательная комиссия или комиссия ДЭГ могли бы подводить итоги голосования на основании выгрузки избирательных бюллетеней из блокчейна и ключа расшифрования. Подобное решение хорошо зарекомендовало себя в эстонской системе интернет-голосования, как с точки зрения безопасности, так и с точки зрения повышения доверия ко всей процедуре.

6.7 Защита от несанкционированных голосований и ботов

Одной из неизбежных проблем в системах электронного голосования является обеспечение того, чтобы «от имени» учетных записей избирателей голосовали только сами избиратели и делали это самолично.

Это требует:

- исключения (или минимизации) возможности проголосовать от имени избирателей внешним злоумышленникам, получившим доступ к аккаунтам избирателей,
- исключения (или минимизации) возможности незаметного голосования от имени избирателей внутренними злоумышленниками, имеющими непосредственный доступ к системе верификации или системе ДЭГ.

Сопряженной проблемой является возможность включения несуществующих избирателей (ботов) в реестр электронных избирателей, голосуя от имени которых можно существенно влиять на итоги голосования.

Такой риск реален в условиях непрозрачности формирования реестра электронных избирателей, отсутствия эффективных процедур проверки такого реестра со стороны наблюдателей и членов комиссий.

7

Безопасность и защита данных

7.1 Шифрование голосов и защита данных

Важным моментом в электронном голосовании является шифрование голосов избирателей. Его реализация должна одновременно обеспечивать как тайну волеизъявления, так и возможность последующей проверки корректности подсчета голосов.

Личность посылающего заполненный и зашифрованный бюллетень в систему должна оставаться неизвестной для нее. При этом, на этапе выдаче электронного бюллетеня должна быть проведена проверка активного избирательного права, а после подачи голоса избиратель должен иметь возможность идентифицировать свой бюллетень. Другими словами, система ДЭГ должна гарантировать анонимность волеизъявления, результат волеизъявления не должен быть известен до начала подведения итогов, при этом избиратель должен иметь возможность проверить, что его волеизъявление принято и учтено корректно. Анонимность голосования подразумевает, что имеющий доступ к системе не может восстановить связь избирателей и их анонимизированных волеизъявлений.

Для решения этих задач применяются различные методы шифрования.
Их грамотное сочетание позволит создать надежную систему, обеспечивающую как анонимность, так и проверяемость голосования. Современным подходом можно считать использование асимметричного шифрования для безопасной передачи бюллетеней и использование слепой подписи (blind signature) для анонимной верификации избирателя. Одним из потенциальных направлений развития является использование гомоморфного шифрования для возможности быстрого подведения итогов без предварительного расшифрования голосов.
Однако в последнем случае для возможности проверки корректности учета собственного голоса избирателем все равно потребуется расшифровать и опубликовать голоса.

Выбор и комбинация алгоритмов шифрования узкоспециализированная тема, требующая проработки с участием квалифицированных специалистов в области прикладной криптографии. Правильный выбор позволит создать одновременно надежную, безопасную систему ДЭГ, соответствующую принципам демократического голосования.
При этом должны быть рассчитаны достаточная криптостойкость и производительность соответствующего оборудования, пиковая нагрузка.

7.2

Защита от атак

Система электронного голосования является потенциальной мишенью для атак — как со стороны внешних злоумышленников, так и со стороны организаторов ДЭГ и участников избирательного процесса. Поэтому вопросам обеспечения безопасности, защиты от вмешательств и устойчивости к сбоям необходимо уделить первостепенное внимание. Это касается всех уровней: от сетевой инфраструктуры и серверов до криптографических протоколов, механизмов идентификации и процедур взаимодействия операторов, наблюдателей и избирателей с системой.

При этом важно учитывать фундаментальное свойство любой сложной, распределенной, многокомпонентной и тем более незамкнутой системы: абсолютная безопасность недостижима и не гарантирована. В системе, взаимодействующей с широким кругом пользователей и подключенной к внешним государственным и частным информационным системам, всегда будут существовать уязвимости — пусть даже крайне маловероятные или сугубо теоретические. Более того, полный спектр возможных атак не может быть сформулирован. На этапе проектирования необходимо составить модель угроз: очертить спектр реалистичных атак и оценивать каждый из этих рисков, сформировать их градацию и принять реалистичный допустимый уровень угроз, исходя из так называемого «риск-аппетита». Важно заранее согласовать, какие угрозы и в какой степени считаются приемлемыми, а какие – недопустимыми ни при каких условиях. Для каждого рассмотренного риска – проработать архитектурные и организационные меры защиты.

Следует ожидать, что технологии в электоральной сфере, в которой изначально заложена конкуренция интересов участников, неизбежно будут подвергаться критике. Аргументация критики в плане информационной безопасности обычно строится на гипотетических сценариях, практическая вероятность которых близка к нулю.

Система не должна стремиться к защите от таких сценариев любой ценой — важно сохранять баланс между реальными угрозами, целесообразностью, прозрачностью, управляемостью и доступностью системы.

Исходя из этого, архитектура защиты должна строиться по принципу минимизации ущерба в случае реализации угроз. Это означает разумное усложнение системы (в пределах необходимого), резервирование ключевых компонентов, внедрение многоуровневой аутентификации, логирование действий, процедурного контроля доступа и внешнего аудита. Также необходимо предусмотреть механизмы реагирования на инциденты, включая восстановление работоспособности, фиксацию попыток вторжения и, при необходимости, процедуру приостановки или отката голосования до безопасной точки.

Наконец, следует особо подчеркнуть, в системах ДЭГ основным источником угроз может выступать не внешний злоумышленник, а сам организатор выборов, обладающий политическими интересами, административным ресурсом и контролем над всеми ключевыми компонентами системы.
В такой ситуации необходимо предусмотреть институциональные механизмы сдержек и противовесов, в том числе обязательное распределение полномочий, разделение ключей между независимыми сторонами и публичный контроль за критическими этапами голосования. Только в условиях признания этих рисков и их проработки можно надеяться на реальный рост доверия к системе дистанционного электронного голосования.

7.3 Логирование процессов и сбор данных

Одной из острых проблем большинства существующих систем электронного голосования является их закрытость и непрозрачность. Такие системы зачастую функционируют как «черный ящик», внутренняя логика и процессы которого недоступны для стороннего наблюдения или независимого аудита. Это порождает закономерное недоверие со стороны экспертного сообщества, политических сил и общества. В условиях, когда внешние наблюдатели и аудиторы не имеют возможности проследить за происходящим внутри системы, возрастает вероятность скрытых вмешательств и злоупотреблений, что подрывает доверие к результатам выборов. Помимо политических причин, в качестве препятствий к раскрытию происходящего внутри систем ДЭГ называются соображения безопасности.

Для снижения остроты проблемы необходимо найти оптимальный баланс между безопасностью и открытостью. В этой связи рекомендуется внедрить механизм прозрачного, детализированного логирования ключевых внутренних процессов, не раскрывающих тайну голосования. В первую очередь речь идет о фиксации действий администраторов и операторов системы, всех изменений конфигурации, обновлений программного обеспечения, параметров криптографических протоколов, а также взаимодействий между основными компонентами инфраструктуры. Логика и последовательность этих событий должны быть формализованы и защищены от нерегламентированного изменения. Контрольное логирование также имеет смысл осуществлять посредством блокчейн-технологий. Запись логов в отдельный блокчейн-реестр с периодическими зашифрованными подписанными выгрузками обеспечит их подлинность, хронологическую целостность, невозможность незаметного редактирования и возможность последующей проверки заинтересованными сторонами или судебными органами в случае спорных ситуаций.

Часть логов, некритичную для безопасности, можно давать в режиме реального времени официальным наблюдателям или сделать открытыми. Архитектура логирования должна гарантировать нераскрытие персональной и конфиденциальной информации, а также невозможность деанонимизации избирателей и преждевременное раскрытие результатов голосования.

При этом не следует стремиться к абсолютному контролю всех электронных процессов со стороны участников выборов и наблюдателей. Во-первых, в настоящее время не существует эффективных и практически применимых протоколов, позволяющих контролировать выполнение сложного, распределенного кода неограниченным кругом лиц, не обладающих специальной технической квалификацией. Во-вторых, контроль за внутренними компонентами системы ДЭГ должен рассматриваться как дополнительный по отношению к более доступному и воспроизводимому контролю целостности голосования на основе публичных, верифицируемых данных. Именно этот уровень наблюдения — контроль выходных данных системы, их соответствие правилам и допустимым сценариям — может обеспечить эффективную защиту от искажений результатов голосования.

8

Разработка и внедрение системы

8.1 Техническое задание

Техническое задание (ТЗ) на систему дистанционного электронного голосования должно разрабатываться заблаговременно и быть максимально детализированным. В нём необходимо зафиксировать архитектуру системы, принципы её функционирования, а также конкретные решения по вопросам, ранее рассмотренным в этом документе — включая выбор модели авторизации, механизмов анонимности, подходов к переголосованию, организации хранения голосов, взаимодействия между компонентами и др.

Структура документа должна включать разбивку по основным модулям, таким как: работа со списками избирателей, процедуры аутентификации, хранение и подсчёт голосов, модуль наблюдения и контроля, а также другие компоненты, обеспечивающие функционирование системы.

Документ должен быть публичным и доступным для оценки широким кругом независимых экспертов. Это позволит заранее выявить возможные уязвимости и недочеты, и в случае обнаружения критических замечаний — доработать ТЗ до начала разработки системы. Проектирование и обсуждение технического задания желательно вести с участием внешних специалистов: представителей академического сообщества, политических партий, общественных организаций. Это особенно важно для систем, предназначенных для проведения официальных выборов и референдумов. Целесообразно стремиться к консенсусу между различными политическими и общественными институциями.

Также желательно предусмотреть регулярную публикацию промежуточных отчетов о ходе разработки и доработке ТЗ, чтобы обеспечить прозрачность и учет общественного интереса. Закрытый характер подготовки технической документации повышает риск архитектурных и проектных ошибок, недостаточного учета интересов разных участников избирательного процесса и может вызвать публичное сопротивление и снижение доверия к системе еще до начала ее эксплуатации.

В случае разработки платформы для негосударственных инициатив — например, в рамках распределенной общественной или политической структуры — эти требования могут быть смягчены, хотя принципы прозрачности и внешнего контроля остаются обязательными.

8.1

Если система предполагается к применению в рамках официального избирательного процесса, необходимо соблюдение требований ГОСТ 34, поскольку это служит условием для ее сертификации в составе государственных информационных систем.
Следует учитывать, что на практике зачастую ГОСТ 34 оформляется уже после разработки системы, «задним числом», в рамках формальной процедуры сертификации.
Тем не менее, добросовестное предварительное соответствие этим требованиям желательно обеспечить на стадии подготовки ТЗ.

Для разработки и обеспечения прозрачности и доверия к системе ДЭГ необходимо подготовить документацию трех типов:

1 **Для разработчиков:**

Фактически это Техническое задание на систему, которое должно содержать описание архитектуры и технические детали

2 **Для независимых аудиторов и членов избирательных комиссий:**

В версиях как для специалистов, так и неспециалистов, чтобы они могли проверить корректность реализации и соответствие заявленным принципам

3 **Для участников голосования** *(партий, кандидатов, избирателей):*

Такое описание должно быть доступно публично неограниченному кругу желающих на официальных ресурсах избирательных комиссий. Здесь должны быть описаны основные принципы устройства и работы системы, даны инструкции по голосованию и осуществлению контроля за целостностью голосования, понятные неспециалистам.

Такая трипликация технической документации по адресным группам существенно повышает уровень доверия к системе. Она позволяет каждой из сторон — как профессиональным разработчикам, так и широкой общественности — получить необходимую информацию в подходящем формате, а также обеспечить возможность участия в контроле и проверке ее корректной работы. Этот подход минимизирует риски недопонимания, спекуляций и подозрений, усиливает восприятие системы как открытой, проверяемой и честной.

8.2 Тестирование, аудит и внешняя проверка

На этапе подготовки и до начала официального использования система дистанционного электронного голосования должна пройти комплексное тестирование и независимую проверку.
Это включает функциональное, нагрузочное и интеграционное тестирование, а также обязательное проведение пен-тестирования для выявления уязвимостей, связанных с внешними угрозами и попытками несанкционированного вмешательства.
Необходимым условием считается проведение хотя бы одного масштабного публичного тестового голосования, открытого для широкого круга голосующих.
Такое тестирование позволяет не только проверить техническую устойчивость и масштабируемость системы в условиях высокой нагрузки, но и познакомить избирателей с процедурой голосования, а также проверить корректность взаимодействия со смежными инфраструктурами — системами аутентификации, рассылки уведомлений, хранения логов и др.

При возможности, было бы целесообразно провести тестовое голосование, при минимальном участии команды разработчиков. Это важно для демонстрации независимости работы системы, допуска внешних специалистов и снижения рисков, связанных с возможным присутствием недокументированных механизмов или внутренних уязвимостей.
Все изменения, вносимые в архитектуру или программный код после прохождения предварительного аудита, должны быть документированы, зафиксированы в логах и по возможности доступны для последующего анализа третьими сторонами.

После проведения официального голосования необходимо обеспечить поствыборный аудит системы. Особенно предпочтительно применение риск-ориентированного аудита (Risk-Limiting Audit, RLA), как это практикуется, например, в Эстонии. Такой аудит должен сопровождаться открытой публичной отчетностью и включать анализ технических логов, проверку достоверности процессов голосования, выявление возможных аномалий и исключение фактов скрытого вмешательства.

8.3 Юридический аудит и сертификация

Если система применяется для официальных электоральных процедур в действующем правовом поле Российской Федерации, она должна соответствовать избирательному законодательству РФ (Федеральный закон «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» от 12.06.2002 N 67-ФЗ) и нормативным документам Центральной избирательной комиссии (ЦИК) РФ, регулирующим ДЭГ (доступны на сайте ЦИК).

(Специализированные законы к разным типам выборов синхронизированы с рамочным 67-ФЗ).

По текущему законодательству, системы ДЭГ фактически применяются с разрешения и по решению ЦИК. Кроме того, системы ДЭГ должны быть Государственными информационными системами (ГИС), что предполагает соответствующую сертификацию.

Однако важно учитывать, что существенные правки в регулирование ДЭГ вносятся фактически ежегодно.

8.3

Если систему предстоит применять не в текущем правовом электоральном режиме РФ, то ее стоит проектировать:

- через адаптацию принципов и процедур офлайн-голосования, заложенных в 67-ФЗ редакциях 2010-х годов, к формам удаленного голосования.
- в рамках системы принципов проведения электронных голосований, сформулированных в рекомендациях Совета Европы от 2017 года: https://rm.coe.int/0900001680726f6f
- с учетом документации и экспертных отчетов системы интернет-голосования в Эстонии, как единственной системы, используемой на практике более двух десятилетий и при этом достаточно открытой и хорошо исследованной (материалы есть в открытом доступе на сайтах valimised.ee и e-estonia.com).

При разворачивании и применении систем ДЭГ в России имеет смысл учесть рекомендации независимых российских экспертов. Для примера: независимый вариант требований к техзаданию на систему ДЭГ с учетом российских и московских реалий 2020 года собраны в «Требованиях к содержанию технического задания на систему дистанционного электронного голосования г. Москвы...»

(копия документа)

9

Заключение

Система дистанционного электронного голосования — это не просто технологическое решение, а сложный социально-политический проект, в котором на первый план выходят вопросы доверия, прозрачности, подотчетности и соблюдения базовых демократических принципов. Технические аспекты, правовые ограничения, архитектурные решения, организационные схемы и политический контекст — все это неразрывно связано между собой, и без комплексного подхода невозможно создать надежную и легитимную систему.

Анализ международного и российского опыта показывает, что универсального решения не существует. Существующие практики демонстрируют как потенциал технологии, так и ее уязвимости. Успешная реализация ДЭГ требует системного подхода: от формализации политических и юридических рамок до проработки детальных технических протоколов, механизмов аудита, разделения полномочий и взаимодействия с обществом.

Ключевым выводом является необходимость перехода от закрытых и непрозрачных схем к открытому, верифицируемому процессу, в котором каждый элемент — от авторизации до подсчета — должен быть подвержен независимому контролю. Архитектура должна включать в себя не только современные криптографические и инфраструктурные решения, но и институциональные гарантии: разделение ключей, внешние ноды наблюдения, публичный аудит, возможность проверки корректности исполнения кода и прозрачное логирование событий.

При этом нужно сохранять реалистичный взгляд: абсолютная безопасность невозможна, а значит, необходимо заранее определить границы допустимого риска и разрабатывать систему исходя из принципа минимизации последствий потенциальных атак и сбоев. Только такой подход способен обеспечить общественное доверие и устойчивость к политическим и техническим вызовам.

Представленный анализ формирует основу для разработки технического задания на систему электронного голосования, которая сможет отвечать как современным технологическим стандартам, так и требованиям гражданского общества.

Отчет подготовлен экспертной группой Петра Лосева