МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича»

На правах рукописи

Салман Васан Давуд Салман

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МОДЕЛИ И ПРОТОКОЛА ЗАЩИЩЕННОЙ СИСТЕМЫ ДИСТАНЦИОННОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ ДЛЯ АРАБСКИХ ГОСУДАРСТВ С ПАРЛАМЕНТСКОЙ ПРАВОВОЙ СИСТЕМОЙ (НА ОПЫТЕ И ПРИМЕРЕ РЕСПУБЛИКИ ИРАК)

2.3.6. Методы и системы защиты информации, информационная безопасность

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель
доктор технических наук , профессор
Яковлев Виктор Алексеевич

Санкт-Петербург – 2023

Оглавление

ВВЕДЕНИЕ

Актуальность темы исследования. В современном мире стремительно развиваются информационно-коммуникационные технологии (ИКТ), оказывающие влияние на общество, и на такие его сферы как образование, здравоохранение, банковское дело, медиа, транспорт, производство, торговля и другие. Происходящий научно-технический прогресс затронул и такую важную и необходимую сферу человеческой деятельности, как различные виды голосования, предназначенные для свободного волеизъявления граждан. Уже несколько десятков лет голосования на различных уровнях общественной деятельности проводятся в электронном виде, с использованием современных технологий. Это позволяет отказаться от использования бумажных бюллетеней, сократить сроки подсчета голосов, повысить явку избирателей за счет привлечения к голосованию малоподвижных граждан и молодых избирателей, и создания других удобств голосующим.

Дистанционное электронное голосование (ДЭГ) — переход к системе онлайн-голосования, базирующейся на интернет-платформе с использованием криптографических методов. Система ДЭГ должна отвечать требованиям безопасности: обеспечивать тайну голосования, анонимность голосующего, аутентификацию избирателя, уникальность, точность и подтверждение голоса.

ДЭГ является междисциплинарным предметом, который должен исследоваться экспертами в области программного обеспечения, криптографии, политики, права, экономики и социальных наук. В основном электронное голосование известно, как сложная тема в криптографии из-за необходимости достижения анонимности избирателей и обеспечения конфиденциальности их волеизъявления.

В настоящее время известно несколько практических систем ДЭГ. Это система ДЭГ России [93], которая использовалась в тестовом режиме на выборах 2021г.; система «КриптоВече» [92] (Россия) 2020г., разработанная в Санкт-Петербургском Государственном университете. (КриптоВече -

платформа для сбора предложений и проведения онлайн-голосований); система «Helios» [81], разработанная в Гарвардском университете в 2008г. (система Helios - веб-система электронного голосования с открытым исходным кодом); система Provotum [87] (Швейцария), разработана в Цюрихском университете в 2020г. (система Provotum - основана на публичном блокчейне). Данные системы реализованы с учетом конкретных условий использования, связанных с особенностями выборов (количеством избирателей, актуальными угрозами, техническими возможностями реализации и др.). Однако, до настоящего времени не существует электронной системы голосования, которую можно было бы использовать на различных выборах.

Вопросы построения выборной системы регулируются законодательно индивидуально для каждой страны. Однако, можно выделить страны со схожим законодательством, что исторически обусловлено национальными особенностями, вероисповеданием, традициями и менталитетом населения этих стран. К группе таких стран относятся страны арабского мира с принятой в них парламентской формой управления. Это страны: Ирак, Ливан, Сирия, Марокко, Тунис, Алжир, Йемен и Бахрейн.

Использование открытой среды (Интернета) для функционирования системы ДЭГ в свою очередь создает много рисков безопасности информации и надежности системы ДЭГ. При построении системы голосования должны учитываться также угрозы безопасности информации, характерные для данного региона или группы стран.

Такие угрозы в основном связаны с влиянием субъективного (человеческого) фактора и технологией обработки бумажных бюллетеней, в частности, атаками со стороны административного ресурса системы. Стоит отметить, что в разработанных системах этому вопросу уделяется недостаточно внимания. В республике Ирак и других арабских государствах системы дистанционного электронного голосования отсутствуют.

Поэтому, исследование и разработка надежных и современных способов проведения электронного голосования, является актуальной научно-

практической задачей в области безопасности информации. Актуальность решения этой задачи усилилась в последнее время в связи с пандемией коронавируса, охватившей весь мир.

В данной работе на опыте и примерах проведения выборов в республике Ирак предлагается научно-методический аппарат для построения современной защищенной системы ДЭГ для арабских государств.

Степень разработанности темы. Дистанционное электронное голосование – активно развивающаяся исследовательская область. Использование Интернет для этой цели создает серьезные проблемы связанные с вопросами безопасности такой системы, что отмечают академические исследователи и промышленные практики. Причина отчасти в том, что внедренные системы ДЭГ не соответствуют всем международным стандартам безопасности и не могут обеспечить адекватное предъявляемым требованиям использование на различных типах выборов.

Основоположниками в данной научной области можно назвать таких ученых, как J.C. Benaloh, P. Paillier, B. Adida, R. Cramer, M. Franklin, B. Schoenmakers, M. Yung, D. Chaum, Н.А. Молдавян, В.И. Коржик,V. Mateu, F. Sebé, M. Valls, K. Peng, Kaiser, R., Chalabi, M. H. и др. Наиболее значимые работы, посвященные разработке системы электронного голосования, принадлежат таким ученым как B. Adida , K. Peng, R. Cramer, В.И. Коржик, Н.А. Молдавян, А. А. Молдовян, А.В.Черемушкин.

Объект и предмет исследования. Объектом исследования является система дистанционного электронного голосования (ДЭГ), а предметом – модель и протоколы обеспечения безопасности функционирования этой системы.

Цель и задачи исследования. Целью работы является обеспечение защищенности от угроз безопасности информации в системах дистанционного электронного голосования на парламентских выборах в республике Ирак и других арабских государствах.

Для достижения цели исследования в работе решена научная задача: разработка научно-методического аппарата для создания безопасной системы дистанционного электронного голосования на парламентских выборах в арабских государствах, с учетом особенностей избирательного процесса на основе использования гомоморфного шифрования с распределенным дешифрованием.

Данная научная задача подразделяется на следующие частные задачи:

- анализ принципов построения современных систем ДЭГ;
- анализ недостатков существующих систем ДЭГ и обоснование требований к перспективным системам;
- анализ угроз информационной безопасности в системе ДЭГ и способов их предотвращения и блокирования;
- исследование методов защиты от угрозы преднамеренного или случайного неправильного заполнения бюллетеня избирателем в системе дистанционного электронного голосования;
- разработка модели перспективной системы дистанционного электронного голосования с учетом специфики голосования в арабских странах и требований по обеспечению ее безопасности;
- разработка протокола функционирования перспективной системы дистанционного электронного голосования с учетом особенностей процесса голосования в арабских странах;
- разработка метода проверки корректности заполнения зашифрованного избирательного бюллетеня избирателем.

Научная новизна результатов исследования. Научная новизна полученных результатов состоит в следующем:

- Модель перспективной системы дистанционного электронного голосования создана с учетом специфики голосования в арабских странах. В отличие от известных систем ДЭГ предложенная модель строится на основе распределенной сети узлов блокчейна-консорциума (БЧ) с использованием смарт-контрактов. Для каждой

провинции создается узел голосования, включающий в себя серверную платформу, состоящую из сервера регистрации; сервера аутентификации; нескольких независимых серверов голосования, предназначенных для генерации ключей и частичного расшифрования бюллетеней. На каждый узел замыкаются избирательные участки и округа провинций. Также на узле голосования провинции есть несколько смарт-контрактов, в которых хранятся зашифрованные голоса избирателей избирательного участка. Такая архитектура системы ДЭГ позволяет реализовать на ней функционирование протокола голосования, обеспечивающего выполнение требований информационной безопасности процесса голосования.

- Протокол перспективной системы дистанционного электронного голосования разработан с учетом особенностей угроз системе ДЭГ в арабских странах и основан на гомоморфном шифровании и распределенном дешифровании, что обеспечивает выполнение требований безопасности информации: тайна волеизъявления; анонимность голосующего; аутентификация избирателя; уникальность и точность голосования, подтверждение факта голосования. Отличается от известных тем, что обеспечивает дополнительную защищенность от атаки, нацеленной на нарушение анонимности избирателя со стороны административного ресурса системы. Это достигается за счет применения распределенного дешифрования, при котором никто из участников системы не имеет доступа к ключу дешифрования.
- Метод проверки корректности заполнения избирательного бюллетеня в целом, в отличие от известных методов, позволяет контролирующему органу убедиться в том, что избиратель правильно выбрал количество кандидатов из диапазона возможных значений. При этом обеспечивается скрытность суммарного числа голосов в бюллетене, поданном избирателем, тем самым блокируется атака на

систему ДЭГ, заключающаяся в анализе и оценке статистики хода голосования до окончания выборов.

Теоретическая и практическая значимость работы

Теоретическая значимость работы заключается в следующем:

1. Разработан подход к построению системы ДЭГ на основе использования технологии блокчейна и применении криптографических преобразований, обеспечивающих защиту системы ДЭГ от многих угроз ее безопасности. Предлагается систему ДЭГ республики Ирак создавать в виде объединения подсистем ДЭГ провинций, построенных по принципу блокчейн-консорциума. Взаимодействие избирательной комиссии провинции и избирательных участков провинции предлагается осуществлять с использованием смарт-контрактов. В смарт-контрактах хранятся зашифрованные голоса избирателей избирательного участка, что гарантирует полноту подсчета голосов, сокращает время подсчета голосов и снижает нагрузку на блокчейн-сеть.
2. В протоколе перспективной системы ДЭГ в отличие от многих протоколов ДЭГ, использован подход, основанный на применении криптосистемы шифрования с единым для всех избирателей ключом шифрования и разными ключами дешифрования бюллетеней распределенными между независимыми (принадлежащими разным партиям) серверами, что обеспечивает повышенную анонимность избирательного процесса.
3. Метод проверки корректности заполнения избирательного бюллетеня расширяет класс методов проверки корректности заполнения бюллетеня, основанного на доказательства с нулевым разглашением секрета, и обеспечивает повышение безопасности избирательного процесса поскольку в ходе процедуры проверки не раскрывается суммарное число голосов, отданное избирателем за кандидатов.

Практическая значимость диссертации заключается в том, что:

1. Модель системы ДЭГ предлагается использовать для перехода от системы голосования с использованием бумажных бюллетеней к безопасной и экономичной системе дистанционного электронного голосования с возможностью сокращения времени подсчета голосов за счет использования распределенной сети блокчейн-узлов с использованием смарт-контрактов и применения гомоморфного шифрования.
2. Предлагаемый протокол может применяться на выборах, где требуется выполнение требований обеспечения информационной безопасности голосования в условиях угроз со стороны административного ресурса и других угроз, связанных с человеческим фактором. Функционирование протокола апробировано на разработанном макете системы ДЭГ, что подтверждает его реализуемость.
3. Предлагаемый метод проверки корректности заполнения бюллетеня может быть использован для доказательства корректности заполнения бюллетеня в различных системах дистанционного электронного голосования.

Методология и методы исследования. Для решения поставленных в диссертации задач использовались криптографические методы на основе схем гомоморфного шифрования (Эль-Гамаля) в числовом поле и на эллиптической кривой; схема доказательства с нулевым разглашением секрета; методы доказательства корректности заполнения бюллетеня, технология блокчейна-консорциума. Моделирование функционирования предложенного протокола ДЭГ выполнено на основе комплекса приложений, разработанного на языке программирования Python 3.10 с использованием библиотеки PyQt5 для создания графического интерфейса приложений.

Положения, выносимые на защиту:

1. Модель системы дистанционного электронного голосования (ДЭГ) для арабских государств с парламентской правовой системой, основанная

на распределенной сети блокчейн-узлов, объединяющей подсистемы ДЭГ провинций, построенные по принципу блокчейн–консорциума с использованием смарт-контрактов.

2. Протокол функционирования перспективной системы дистанционного электронного голосования на основе гомоморфного шифрования с распределенным дешифрованием, учитывающий угрозы безопасности информации актуальные для арабских государств, и обеспечивающий повышение защищенности от угроз, связанных с субъективным (человеческим) фактором.
3. Метод проверки корректности заполнения бюллетеня избирателем, обеспечивающий скрытность волеизъявления избирателя по отдельным кандидатам и по всем кандидатам в целом.

Степень достоверности и апробация результатов.

Достоверность результатов, обоснованность положений и выводов, сформулированных в диссертации, обеспечивается учетом большого количества факторов, влияющих на решение поставленной научной задачи; обоснованным выбором основных допущений и ограничений, принятых в качестве исходных данных при ее постановке; использованием современного математического аппарата; обсуждением результатов диссертационной работы на конференциях; публикацией основных результатов диссертации в ведущих рецензируемых журналах.

Основные результаты диссертации докладывались и обсуждались на: конференции Национальная безопасность России: актуальные аспекты (Санкт-Петербург, 2020); конференции Новые импульсы развития: вопросы научных исследований (Саратов, 2020); Всероссийской научно-теоретическая конференции Теория и практика обеспечения информационной безопасности (Москва, 2021); 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (Турция, Анкара, 2021), Международных научно-технических и научно-методических конференциях

«Актуальные проблемы инфотелекоммуникаций в науке и образовании» (Санкт-Петербург, АПИНО в 2021, 2022, 2023 годах).

Публикации по теме диссертации. Всего по теме диссертации опубликовано 13 работ, из них 4 статьи в рецензируемых научных журналах, входящих в перечень изданий, рекомендуемых ВАК Министерства высшего образования и науки Российской Федерации, 1 статья в рецензируемых изданиях, входящих в международные базы данных SCOPUS, 8 статьи в журналах и сборниках конференций, включенных в РИНЦ.

Реализация и внедрение результатов работы.

Результаты диссертационного исследования внедрены в образовательный процесс Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича.

Значимость результатов диссертационной работы подтверждена актом реализации Независимой Высшей избирательной комиссии республики Ирак, как составная часть тематики работ, проводимых комиссией по применению современных выборных технологий при переходе от традиционной системы голосования к системе дистанционного голосования особенно в части реализации процедур регистрации и голосования. Подтверждена целесообразность внедрения результатов работы в будущие проекты.

Соответствие паспорту специальности. Содержание диссертации соответствует следующим пунктам паспорта специальности 2.3.6 Методы и системы защиты информации, информационная безопасность: п. 3. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса; п.5. Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет. п.19. Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.

Личный вклад автора. Часть публикаций по проведенным исследованиям написано лично, а часть в соавторстве совместно с научным руководителем, д.т.н., профессором В.А. Яковлевым. С научным руководителем проводились обсуждение и контроль полученных результатов. В работах, выполненных в соавторстве, личный вклад автора заключается в анализе существующих систем голосования в Республике Ирак, арабских государствах, и по всему миру, принципов построения современных систем ДЭГ. Результаты теоретических и экспериментальных исследований получены автором самостоятельно.

Структура и объем диссертации. Диссертации состоит из введения, четырех глав с выводами по каждой из них, заключения, списка литературы. Общий объем работы – (177) страницы, из них основного текста (131) страниц. Работа содержит (21) рисунок и (40) таблицы. Список литературы включает 114 источников.

ГЛАВА 1. АНАЛИЗ ПРИНЦИПОВ ПОСТРОЕНИЯ СИСТЕМ ГОЛОСОВАНИЯ В РЕСПУБЛИКЕ ИРАК И АРАБСКИХ ГОСУДАРСТВАХ

1.1 Анализ существующих систем голосования в республике Ирак

Первые парламентские выборы в Ираке состоялись 15 декабря 2005 года, после войны 2003 года. Они были основаны на пропорциональном представительстве по закрытым спискам. В парламенте Ирака, согласно конституции на этот период было 275 мест. Кандидаты избирались среди “политических партий" и любая партия, которая набрала не менее 1/275 голосов от общего количества избирателей (около 31 000 голосов), имела право получить место в парламенте. На этих выборах провинции Ирака были разделены на несколько избирательных участков [1,2].

В 2010 году состоялись вторые выборы в парламент. Тогда избирательная система была изменена с закрытого списка на специальный открытый пропорциональный список или так называемый полуоткрытый список [2]. В 2014 году состоялись парламентские выборы, после вывода американских войск из Ирака в 2011 году. В иракском парламенте согласно конституции было 328 места. Явка избирателей на выборах превысила 60%, что составляет более 12 миллионов избирателей, имеющих право голоса [1,3].

На выборах 2014 года для распределения мест в парламенте был принят "метод Сент-Лагю (Sainte-Laguë)" [4]. Метод Сент-Лагю – является одним из способов распределения мандатов при пропорциональном представительстве, изобретённый французским математиком Андре Сент-Лагю[1]. В данном методе происходит распределение мест последовательно, одно за другим. На каждом шаге очередное место присуждается партии, обладающей наибольшей квотой, вычисляемой по формуле:

$$\frac{V}{2s+1}, \qquad (1.1)$$

[1]URL:https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4_%D0%A1%D0%B5%D0%BD%D1%82-%D0%9B%D0%B0%D0%B3%D1%8E

где V — общее количество голосов, отданных за ту или иную партию, а s — число мест, полученных партией к данному шагу. После присуждения места, происходит пересчет квоты партии с учётом нового количества полученных мест.

Выборы 2018 года являются вторыми иракскими выборами с момента вывода войск США из Ирака в 2011 году, а также четвертыми выборами с момента вторжения США в Ирак в 2003 году. В парламенте Ирака, согласно конституции 329 мест [3]. Иракский парламент избирался по модели пропорционального представительства по открытым спискам. Как и на выборах 2014 года, для распределения мест в парламенте был принят “метод Сент-Лагю”.

Выборы 2021 году стали шестыми парламентскими выборами после войны 2003 года и третьими выборами после ухода США из Ирака и были проведены после революции иракского народа против существующей системы до окончания срока полномочий парламента. На этих выборах избирательное законодательство изменилось.

Правовая основа выборов в республике Ирак определяется «Законом о выборах» № 9 от 2020 года. В соответствии с этим законом установлено 83 избирательных участка в 18 провинциях республики. Каждый избирательный участок состоит из нескольких местных избирательных округов, где каждый избирательный округ обслуживает примерно 450 избирателей. В иракском парламенте согласно конституции 329 мест [3,5]. 320 общественных мест распределяются между мухафазами (провинциями) в их избирательных округах, в соответствии с административными границами (см. рисунок 1.1). Остальные 9 мест распределятся по конфессиям (христиане, езиды, сабейцы, шабаки и курды-Филен) [5].

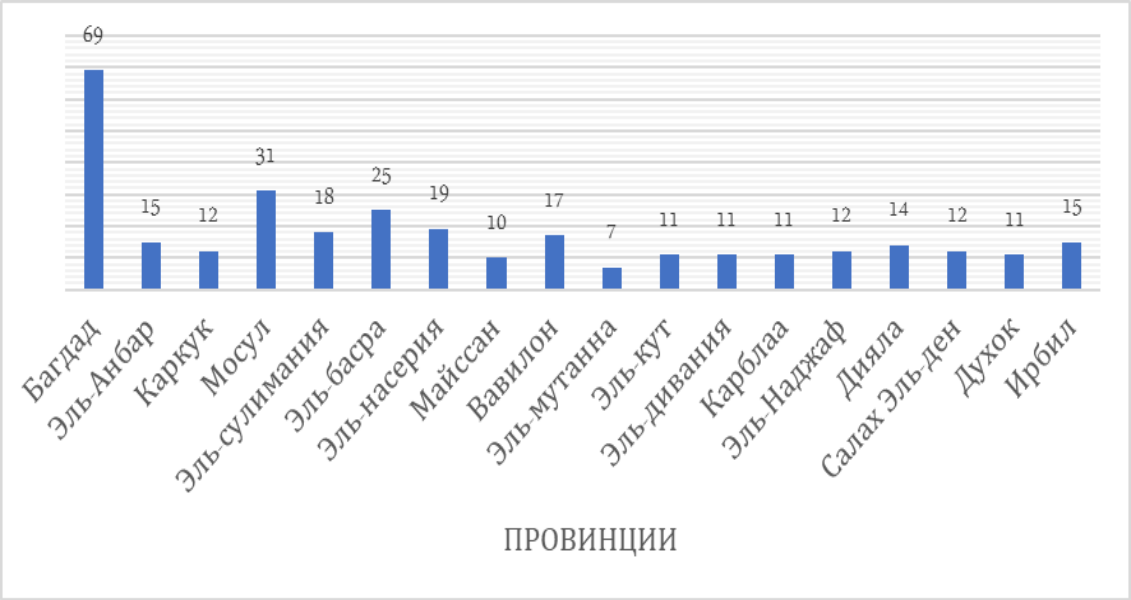

Рис.1.1. Распределение общих мест в парламенте

Кандидаты избираются по открытому и единому списку, где каждому конкретному региону выделяется определенное число мест в соответствии с законом о выборах. 25% и более членов парламента должны составлять женщины [3].

Кандидаты в избирательном округе, независимо от того, включены они в общий список или представлены самостоятельно, по итогам голосования распределяются в соответствии с количеством действительных голосов, которые были получены ими от самого высокого к самому низкому. Кандидат, который получил наибольшее число голосов (мужчина или женщина), признается победителем. В случае, если два или более кандидатов набирают равное количество голосов, то для определения места используется лотерея, которая проводится в присутствии кандидатов с равными голосами или их уполномоченных [3].

Избиратель для голосования должен лично прийти на избирательный округ по месту жительства. Согласно закону о выборах, избиратель имеет право проголосовать только за одного кандидата, который участвует в его местном избирательном округе. Легитимные избиратели, имеющие право голоса, должны иметь гражданство Ирака, возраст не менее 18 лет, быть

зарегистрированы в списке избирателей и иметь биометрическую карту избирателя (см. рисунок 1.2).

Рис. 1.2. Биометрическая карта избирателя

Легитимные кандидаты должны иметь иракское гражданство, возраст не менее 30 лет, иметь свидетельство об образовании (минимальная степень бакалавра) и не иметь судимости. Кандидат может участвовать в выборах на конкретном избирательном участке, где он проживает [1-3]. В таблице 1.1 приведены факты о парламентских выборах 2021г.

Таблица 1.1. Факты о парламентских выборах 2021 года[2]

Факты	Количество
Иракское население	41 миллион
Количество избирателей, имеющих право голосовать	20,919,844 миллион
Провинции	18
Избирательные участки	83
Зарегистрированные избиратели	22116368
Зарегистрированные политические партии	108
Количество проголосовавших избирателей	9629601
Количество правильных голосов	8854025
Количество неверных голосов	775576
Процент проголосовавших	43.54%

[2] URL:https://ihec.iq/result2021/

Требования к системе голосования

Основные требования к системе голосования в Ираке определены Законом № 9 от 05.11.2020 ("Выборы иракского парламента") [3]:

1. Свобода выбора избирателями своего кандидата;
2. Обеспечение равенства;
3. Обеспечение справедливости, свободы и неподкупности выборов;
4. Обеспечение прав избирателя и кандидата на участие в выборах;
5. Обеспечение правовой защиты этапов и процедур избирательного процесса.

Центральная избирательная Комиссия Ирака (ЦИК)

ЦИК является независимым избирательным органом, состоящий из девяти членов, назначаемых Советом представителей, а также находящихся под его наблюдением [1].

Основные функции ЦИК представлены в законе ЦИК № 11 от 2007 года [1,2]:

- Создание и обновление регистрации избирателей;
- Регистрация и аттестация партий для участия в выборах;
- Регулирование и удостоверение списков кандидатов на выборах;
- Аккредитация наблюдателей, представителей партий и средств массовой информации; рассмотрение всех избирательных жалоб и апелляций (могут быть обжалованы только в специальной судебной избирательной коллегии);
- Удостоверение процедуры подсчета голосов;
- Объявление и удостоверение итогов выборов и референдумов;
- Установление нормативных актов и инструкций по обеспечению справедливого избирательного процесса;
- Удостоверение структуры и назначение руководящего состава избирательной администрации;
- Установление финансовой политики для ЦИК.

Процедуры выборов

Рассмотрим технологию и методологию использованные на парламентских выборах 2021 года [5]. Для этого рассмотрим процедуры выборов по этапам. На рисунке 1.3 показана общая блок-схема нынешней системы голосования Ирака.

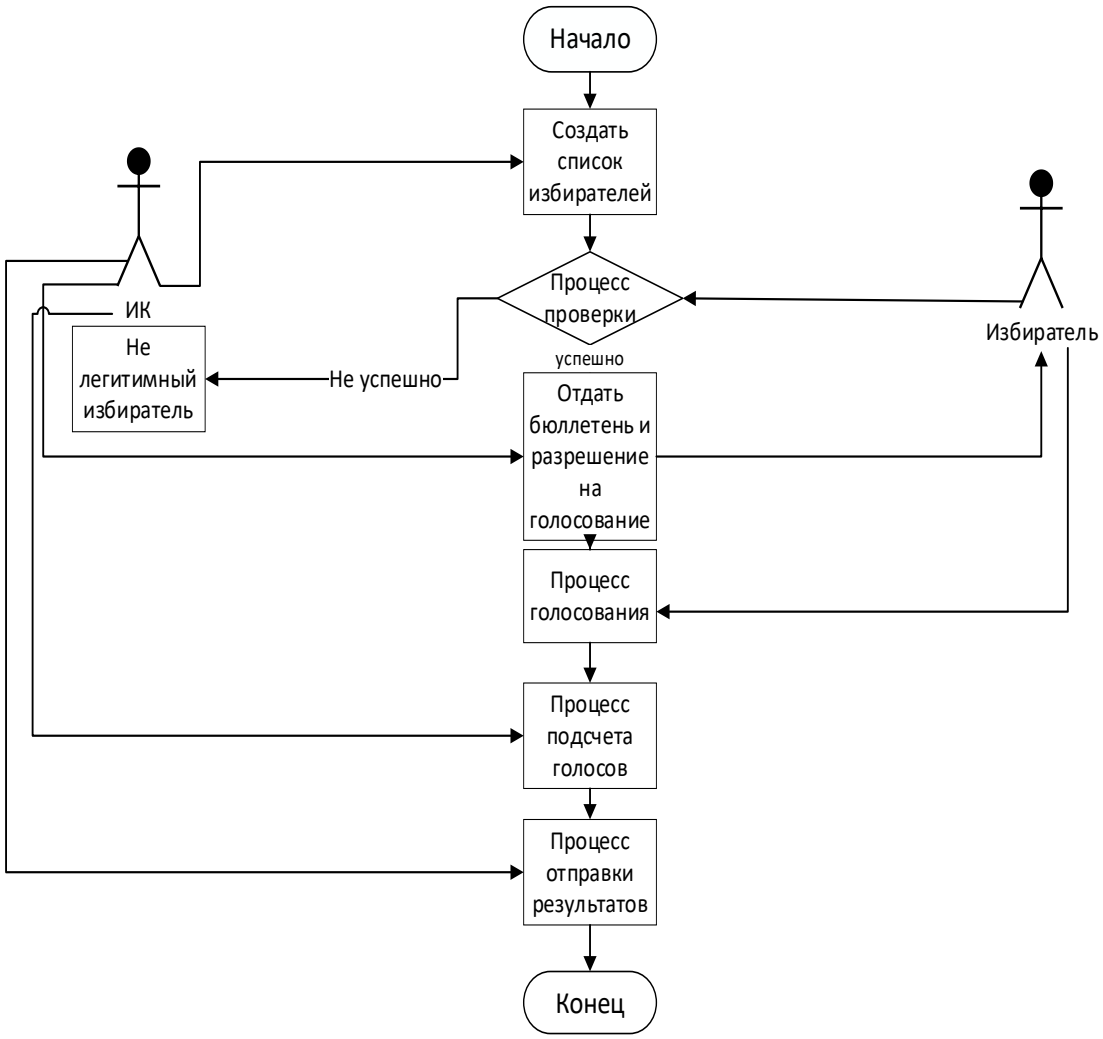

Рис. 1.3. Алгоритм иракской системы голосования 2021г.

Этап регистрации и подготовка списков избирателей

На выборах 2021 года избирательной комиссией была использована технология биометрической регистрации и верификации. Избиратель должен был лично прийти на указанный избирательный участок по месту жительства, где им заполнялась регистрационная форма. Сотрудник избирательного участка с помощью специальных устройств снимал десять отпечатков пальцев избирателя и фотографировал его. После этого избиратель получал свою

личную биометрическую карту, данные которой хранятся в базе данных регистрации избирателей на указанном избирательном участке. Каждый избирательный участок должен был подготовить список избирателей за несколько дней до дня голосования [5].

Этап идентификации и аутентификации избирателя

ИК использует электронные устройства для проверки данных избирателей. Избиратель должен показать выданную ему биометрическую карточку участковому сотруднику. После чего, сотрудник помещает карточку избирателя на электронное устройство проверки. В случае, если проверка прошла успешно, сотрудник просит избирателя приложить большой палец левой руки к месту, предназначенному для снятия отпечатков пальцев. Если отпечаток пальца идентифицирован правильно, то проводится вторая проверка (см. рисунок 1.4). Сотрудником проверяется имя избирателя в бумажном списке избирателей. При успешной проверке, избирателю выдаются бумажные бюллетени [5].

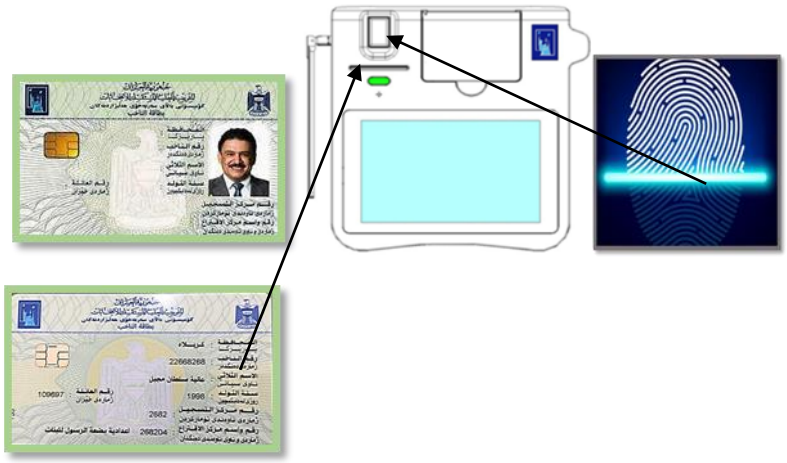

Рис. 1.4. Процесс проверки избирателя

Этап голосования

Выборы проводятся в один день с 7:00 утра до 6:00 вечера. Перед голосованием, руководитель избирательного участка вручает по 500 бюллетеней каждому руководителю избирательного округа. После успешного

завершения процесса проверки данных, избиратель отдает голос за своего кандидата и помечает бюллетень специальной ручкой. На этой специальной ручке нанесен логотип избирательной комиссии (см. рисунок 1.5). Затем, бюллетень помещается избирателем в специальное электронное устройство для подсчета голосов (сканер), после чего он опускает бумажный бюллетень в урну для голосования по избирательному округу. Далее, избиратель должен обмакнуть палец правой руки в чернила для того, чтобы он не смог голосовать дважды [5].

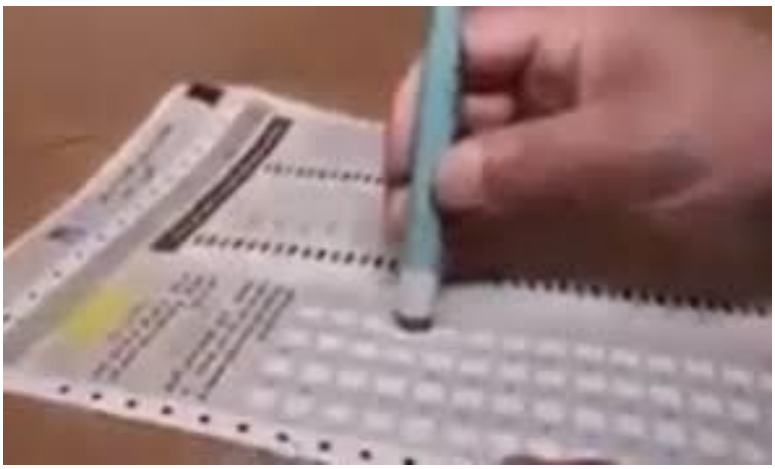

Рис. 1.5. Специальная ручка для голосования

Этап подсчета голосов и отправки результатов в ЦИК

После завершения голосования начинается процесс подсчета голосов. Для этого ИК используется электронное устройство. Процесс подсчета голосов на избирательном участке проходит в два этапа [5]:

- Электронный подсчет и сортировка голосов на избирательном участке с применением электронного устройства подсчета и сортировки (PCOS). Далее происходит отправка результатов из всех избирательных участков в центральный офис избирательной комиссии по каналам спутниковой связи с помощью устройства RTS (см. рисунок 1.6)

Рис. 1.6. Процесс электронного подсчета

- Ручной подсчет и сортировка голосов проводятся в каждом округе избирательного участка. Для этого, урна (ящик) для голосования вскрывается в присутствии представителей политических партий, наблюдателей или других лиц, которые заинтересованы в проверке процесса подсчета голосов. Сотрудник избирательного округа подсчитывает бумажные бюллетени внутри ящика. Общее число бюллетеней внутри ящика и не использованных бюллетеней должно быть равно количеству бюллетеней, полученных руководителем избирательного округа до начала голосования. Далее, подсчитываются действительные и недействительные бюллетени, а также проводится подсчет голосов, отданных за каждого кандидата. В случае обнаружения расхождений между количеством голосов, выданных электронным счетным устройством и количеством голосов, полученных при ручном подсчете, ручной подсчет бюллетеней производится повторно. Если при повторном подсчете будет

расхождение между электронным и ручным подсчетом более 5%, тогда об этом будет объявлено партиям и наблюдателям, где в итоге будут приняты результаты ручного подсчета.

Этап объявления результатов

После окончания голосования, каждый избирательный округ объявляет результаты голосования на доске объявлений и отправляет их с помощью электронного устройства в центральную избирательную комиссию. В ЦИК происходит сортировка, анализ голосов, а окончательные результаты голосования объявляются на веб-сайте ЦИК и по телевидению [5].

Как видно из вышеизложенного, на выборах 2021 года использовались современные технологии, что позволило улучшить избирательный процесс и устранить недостатки, имевшие место на предыдущих выборах. Стоит отметить, что избирательные системы менялись в зависимости от ситуации в стране.

В следующем разделе проанализируем угрозы и недостатки системы голосования, использованной на выборах 2021 года.

1.2. Анализ угроз и недостатков существующей системы голосования

По результатам голосования были выявлены следующие нарушения и недостатки:

Нарушения требований законодательства:

а) Было установлено, что сотрудники избирательных участков могут принять участие в фальсификации результатов выборов для конкретной партии или партии назначают своих собственных сотрудников на избирательных участках, которые могут изменить результаты голосования[3].

[3]URL: https://al-ain.com/article/iraq-percentage-legislative-elections

b) Результаты, объявленные центрами, отличаются от предварительных результатов, полученных на избирательных участках при ручном подсчете голосов.

c) Имели место случаи использования голосов тех законных избирателей, которые не захотели (не смогли) принимать участие в голосовании[4].

d) Были случаи кражи или уничтожения ящиков для голосования с целью изменения результата голосования за определенного кандидата.

Недостатки:

1. В системе использовались бумажные бюллетени для голосования, это потребовало существенных затрат на их изготовление.
2. Более 295 электронных машин для голосования перестали работать "временно", что привело к лишению избирательных прав большого числа избирателей[5].
3. 152 наблюдателя были исключены из списков наблюдателей из-за нарушения ими правил поведения наблюдателей[6].
4. Почти 4 миллиона граждан Ирака не имели биометрической карты, что не дало им право принять участие в выборах (это увеличивает уровень фальсификаций на выборах)[7].
5. 34 избирательных участков нарушили время завершения голосования в 18:00[7].
6. В 35 участках были возражения против объявленных результатов голосования[7].
7. Было замечено, что большинство кандидатов и политических сил заявили о своей победе еще до оглашения результатов избирательной комиссией[7].

[4]URL:https://www.alquds.co.uk/%D8%A7%D9%84%D8%A7%D9%86%D8%AA%D8%AE%D8%A7%D8%A8%D8%A7%D8%AA-%D8%A7%D9%84%D8%B9%D8%B1%D8%A7%D9%82%D9%8A%D8%A9-%D8%AE%D8%B1%D9%88%D9%82%D8%A7%D8%AA-%D8%A8%D8%A7%D9%84%D8%AC%D9%85%D9%84%D8%A9-%D9%88/
[5]URL: https://futureuae.com/ar-AE/Mainpage/Item/6736
[6] URL:https://www.orsam.org.tr/ar/2021-irak-parlamento-secimlerinin-degerlendirilmesi/
[7] URL:https://al-ain.com/article/iraq-percentage-legislative-elections

8. Отмечено присутствие сотрудников партии вблизи избирательных участков, с целью влияния на решение избирателя[7].

В [1] авторы проанализировали существующую систему голосования в республике Ирака с 2003 по 2010 годы. Был сделан вывод, что голосование с использованием бумажных бюллетеней имеет такие недостатки: дорогое из-за использованных бумажных бюллетеней, долго подсчитывается результат голосования, возможна манипуляция и фальсификация результатов, инвалиды и пожилые люди не всегда могут прийти на избирательные участки для голосования. Было предложено вместо существующей бумажной избирательной системы внедрить электронную систему голосования, которая использует несколько типов электронных устройств, таких как электронная система прямой записи - (DRE), (для подачи бюллетеней избирателями и подсчета поданных голосов); экран монитора (LCD screen) для мониторинга; считыватель отпечатков пальцев и смарт-карт (для проверки личности избирателя и аутентификации). Недостатки этой системы в том, что избиратель по-прежнему должен приходить на избирательный участок и использовать бумажные бюллетени для голосования.

В [2] авторы проанализировали различные методы, используемые в системе голосования, такие как электронная прямая запись (DRE), оптическая система сканирования и интернет-голосование в киоске и на избирательном участке). Были сформулированы требования, которые должны соблюдаться в системе электронного голосования: аутентификация избирателей, уникальность, точность, тайна голосования. Признано целесообразным перейти на электронную систему голосования без бумажных бюллетеней, дополнительно использовать криптографические преобразования (хеширование) с целью обеспечения информационной безопасности, но конкретных предложений сделано не было.

Эти предложения безусловно позволяют улучшить систему голосования в республике Ирак и устранить ряд отмеченных недостатков традиционной

системы, обусловленных влиянием человеческого фактора и технологией обработки бумажных бюллетеней.

Однако, такие решения, на наш взгляд, являются не полными и не отражают возможностей и достижений в области создания современных систем голосования, которые могут быть получены при переходе к системам дистанционного электронного голосования (ДЭГ).

1.3. Особенности избирательных систем в арабских государствах с парламентской правовой системой

Перечень арабских стран включает 22 государства - члены Лиги арабских государств, это Алжир, Бахрейн, Джибути, Египет, Иордания, Ирак, Йемен, Катар, Коморские острова, Кувейт, Ливан, Ливия, Мавритания, Марокко, Объединенные Арабские Эмираты, Оман, Саудовская Аравия, Сирия, Сомали, Судан, Тунис и Палестина, а также ряд стран Африки (Джибути, Коморские острова, Мавритания, Сомали, Судан) [6,7].

В проведенном нами исследовании были изучены избирательные процессы арабских стран с парламентской правовой системой.

В целом организация и проведение выборов в арабских странах совпадает с общемировой практикой, однако им присущи свои специфические особенности, связанные с культурными и цивилизационными особенностями. В 2011 году начался процесс восстановления конституционных институтов и их трансформации с учетом изменившейся политической ситуации. Так, по конституционным поправкам были проведены референдумы в Египте, в Марокко и в Тунисе. Результатом конституционной реформы в вышеперечисленных странах стала победа исламских партий на парламентских выборах, проведенных на многопартийной основе [6]. В таблице 1.2 приведены характеристики избирательной систем некоторых арабских стран с парламентской правовой системой.

Таблица 1.2. Характеристика избирательной систем арабских стран с парламентской правовой системой

№	Страна	Кол. членов парламента	Избирательная системы	Население	Системы голосования
1	Сирия	250	Смешанная	18 млн.	Бумажное голосование
2	Ливан	128	Пропорциональная	5 млн.	
3	Марокко	395	Пропорциональная	37 млн.	
4	Тунис	130 мест для членов мужского пола, 24 места для женщин, 7 свободных мест.	Мажоритарная	12 млн.	
5	Алжир	407	Пропорциональная	46 млн.	
6	Йемен	301	Пропорциональная	31 млн.	
7	Бахрейн	40	Мажоритарная	18млн.	

Анализируя законодательства арабских государств с парламентской правовой системой и опыт проведения выборов в них, можно отметить следующие особенности избирательного процесса, которые должны быть учтены при построении современной системы электронного голосования:

1. На итоги голосования огромное влияние оказывают нарушения инструкций по голосованию со стороны членов избирательной комиссии.
2. Результаты голосования сильно зависят от влияния субъективного (человеческого) фактора: административного ресурса избирательной системы, религиозных организаций, мнения старейшин, менталитета избирателей,
3. Отличительной особенностью политической системы арабских стран является низкая роль партий в общественно-политической жизни, что обусловлено особенностями социальной структуры традиционного общества.

1.4. Актуальность внедрения системы дистанционного электронного голосования в разных странах

Использование системы ДЭГ при голосовании подразумевает физическое отсутствие избирателя на избирательном участке.

Системы ДЭГ дают право избирателям принимать участие в голосовании удаленно с любого компьютера или цифрового устройства, подключенного к сети общего пользования, такой как Интернет, из дома или с места работы [8, 9].

Основными преимуществами использования системы дистанционного электронного голосования являются [9 - 14]:

- Устранение угроз и недостатков, существующих в традиционном бумажном голосовании;
- Ускорение процесса подсчета голосов;
- Повышение точности результатов голосования;
- Обеспечение тайны голосования с помощью криптографических методов;
- Обеспечение анонимности избирателей с помощью криптографических методов;
- Увеличение числа участников выборов за счет удобства голосования из любой точки мира, в частности для тех, кто живет за границей;
- Расширенный доступ к процессу голосования для избирателей с ограниченными возможностями или имеющих другие физические трудности в присутствии на избирательном участке;
- Экономичность по сравнению с традиционным голосованием (нет необходимости печатать бумажные бюллетени, а также сокращение количества сотрудников в избирательной комиссии);
- Возможность исключить фальсификацию результатов голосования;
- Возможность проголосовать предоставляется только избирателям, имеющим право участвовать в выборах;
- Избиратели имеют право проголосовать только один раз;

- Сохранение здоровья избирателей, в том числе при распространении вирусных инфекций (пример, коронавирус был широко распространен в 2020 году и многие страны не смогли провести выборы);
- Возможность привлечения молодых избирателей к участию в выборах.

Как видно из вышеизложенного, системы ДЭГ имеют массу преимуществ, внедрение которых улучшает избирательный процесс на выборах, а также повышает доверие избирателей.

Далее, проведем краткий обзор использования ДЭГ в разных странах.

На рисунке 1.7. представлена статистика использования системы дистанционного электронного голосования, которое получило широкое распространение в России, Эстонии, Австралии, Венесуэле, Бразилии, Бельгии, Индии и других странах [15].

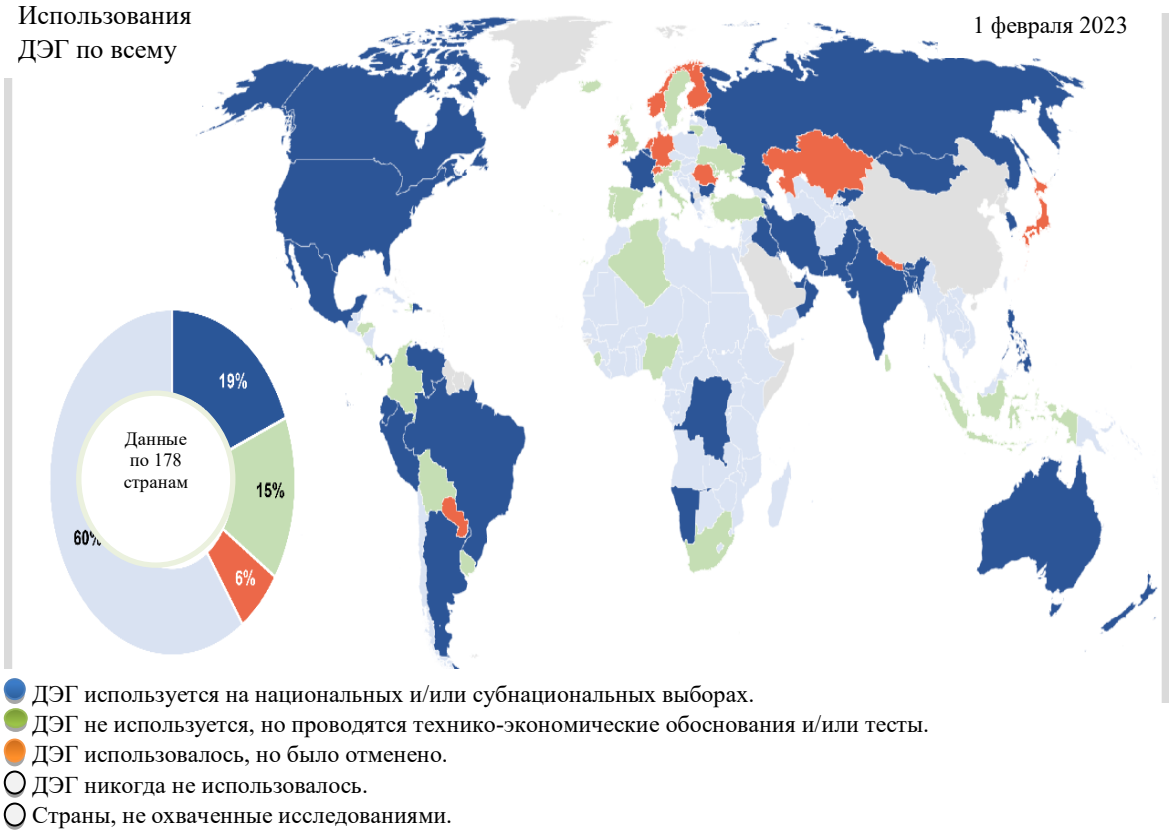

Рис. 1.7. Использование ДЭГ по всему миру[8]

[8] URL:https://www.idea.int/news-media/media/use-e-voting-around-world

В США, впервые ДЭГ применялось в 1964 году в штате Джорджия во время первого этапа президентских выборов [15]. Голосование проводилось с помощью специальных перфокарт: избиратель пробивал свой бюллетень с помощью специального устройства, а подсчет голосов осуществлялся компьютером.

Первое применение ДЭГ в Эстонии [15-17] было в 2005 году в качестве альтернативы традиционному волеизъявлению. Такая новая технология повысила явку избирателей, после чего руководство Эстонии приняло решение продолжить и расширить эту практику: так, во время парламентских выборов 2007 года избирателям предоставили возможность проголосовать досрочно (за четыре-шесть дней до официального дня голосования) через Интернет с использованием идентификационных смарт-карт [16]. Число избирателей, которые воспользовались дистанционным электронным голосованием на выборах 2007 года, увеличилось до 43,8 процента [15, 16].

В 2000 году на выборах в Бразилии использовалось ДЭГ с использованием машин с прямой электронной записью [15]. После этого начался процесс совершенствования процесса ДЭГ и использования новых технологий. В настоящее время, в Бразилии в действующую систему ДЭГ, для обеспечения ее безопасности, внедряются новые технологические решения, в частности биометрическая идентификация по отпечаткам пальцев, цифровая подпись и многие другие [17].

В Испании, в 2018 году был принят каталонский законопроект, который предусматривает распространение процедуры ДЭГ на всех избирателей. Голосование осуществлялось с помощью смс-сообщений или компьютера со считывателем смарт-карт и доступом в Интернет [17].

Первое ДЭГ в Канаде было проведено на муниципальных выборах в Онтарио в 2003 году, после этого оно стало использоваться и в других провинциях. На парламентских выборах 2018 года интернет-голосование уже проводилось в 194 из 444 муниципалитетов страны, и в 80% из них электронное голосование было единственным способом голосования граждан [17].

В США с 2015 года разрабатывается и тестируется блокчейн-голосование на платформе с приложением Web 3.0, которое подразумевает онлайн-регистрацию избирателей и голосование с использованием ID-выборов, ID-голосования и бюллетеня с QR-кодами [15, 18].

В Мексике первое ДЭГ было проведено на муниципальных выборах в Мехико в 2012 году. В настоящее время избиратели, проживающие за границей, могут голосовать дистанционно через Интернет [17].

В 2018 году первое ДЭГ на муниципальных выборах проводилось в Новой Зеландии, а также использовалось при проведении парламентских выборов для избирателей, проживающих за рубежом. На этих выборах для идентификации личности избирателя использовалась биометрическая система [15].

В Южной Корее ДЭГ с использованием технологии блокчейн было использовано на парламентских выборах в 2018 году [15].

Также в Японии в 2018 году в городе Ибараки было проведено ДЭГ с использованием технологии блокчейн. Для идентификации использовалась специальная карточка избирателя [15].

Первое ДЭГ в кантоне Женева в Швейцарии было проведено в 2003 году, а в 2004 году, в муниципалитете Аньерс в Женеве около 43,6% избирателей на муниципальных выборах проголосовали дистанционно [15]. Процесс голосования в Швейцарии осуществлялся на специальном веб-сайте для выборов. Для идентификации избирателя необходимо ввести уникальный идентификационный номер, который он получал по почте от избирательной комиссии [15, 17].

Первая система ДЭГ в России применялась на президентских выборах в 2000 году [15, 16, 19, 20]. Следует отметить, что во время парламентских и президентских выборов 2003-2004 годов на интернет-портал "Выборы" было совершено около 1800 кибератак (около 20% из-за рубежа).

В городе Новомосковске было проведено тестирование ДЭГ на выборах в 2008г. [15, 16]. Избирателям, пришедших проголосовать на избирательный

участок, желающим принять участие в новом эксперименте, выдавался специальный диск, с помощью которого они могли отдать свой голос из удобного места, оснащенного Интернетом. Тест оказался положительным: результаты, полученные при традиционном голосования, совпали с результатами электронного волеизъявления. В целях совершенствования технических средств, используемых при проведении выборов и подсчете голосов избирателей, на парламентских (2007 г.) и президентских (2008 г.) выборах, состоявшихся в России в пяти городах (Орел, Саратов, Великий Новгород, Суздаль и Рязань), были установлены комплексы электронного голосования, которые использовались на 21 избирательном участке [15, 19, 20]. Технология была реализована на базе сенсорного экрана, что позволило голосовать без использования традиционных бумажных бюллетеней через интерфейс устройства.

В 2009 году президент Д.А. Медведев поручил ЦИК России, региональным органам власти и Правительству Российской Федерации (РФ) подготовить и представить программу технического переоснащения российской избирательной системы [15, 19, 20]. Основной целью этой программы было обеспечение доступа субъектов Федерации к широкополосному Интернету для внедрения электронных средств подсчета голосов. Таким образом, руководствуясь положительной динамикой апробации дистанционного электронного голосования, на парламентских выборах 2011 года 5% избирательных участков Республики Татарстан было оборудовано комплексами дистанционного электронного голосования. На президентских выборах 2012 года аналогичными комплексами были оснащены уже 337 избирательных участков в семи субъектах РФ. Использование ДЭГ на выборах Президента России также получило поддержку [15].

На молодежном образовательном форуме 2015 г. «Территория смыслов» было отмечено, что реализацию концепции ДЭГ надо обсуждать со специалистами в области интернет-технологий, парламентариями обеих палат

российского парламента, представителями ЦИК России и иных избирательных комиссий [15].

Начиная с 2015 года практически все избирательные участки в стране были оснащены современными программно-техническими средствами, которые применялись в ходе парламентских (2016) и президентских (2018) выборов. Применение различных интернет-технологий сыграло одну из ключевых ролей в увеличении избирательной явки на последних президентских выборах в России, которая достигла 67,54% процента. В 2018 году прошли выборы с использованием избирательного блокчейна в Саратовский молодежный парламент [15]. Применение этой технологии привело к положительному результату, поскольку преимуществом технологии БЧ является высокая степень защиты данных, а именно, обеспечение нового, более высокого уровня «честности» и «прозрачности» избирательного процесса [15].

На выборах в Московскую городскую Думу в 2019 году, параллельно с традиционным голосованием, было принято решение использовать систему ДЭГ с использованием БЧ в трех избирательных округах Москвы [15, 19]. Для принятия участия в голосовании, избирателям было предложено воспользоваться сервисом "Мобильный избиратель", который позволял им подать заявку на участие в онлайн-голосовании. Во время выборов в региональный парламент, благодаря взлому тестовой системы криптографом из Франции П. Годри, были выявлены недостатки используемой технологии, [15]. Разработчики данной технологии учли замечания, сделанные Годри, что позволило усовершенствовать систему шифрования и электронные ключи, используемые избирателями для реализации своего волеизъявления. Как показала практика, в районах использования технологии БЧ явка избирателей значительно выросла, в том числе за счет тех, кто участвовал в голосовании впервые. Недостатком протестированной технологии было ее техническое несовершенство: в процессе голосования некоторые избиратели не имели доступа для входа в систему; более тысячи избирателей были вообще исключены из списков интернет-голосования, некоторые наблюдатели не

получили ключи для входа и т.д [15, 19]. В эксперименте приняли участие более 10 000 избирателей, это означает, что данная технология востребована избирателями [15].

В 2021 году была проведена масштабная общероссийская тренировка применения ДЭГ. В рамках тренинга голосование было проведено в 85 субъектах РФ [15, 19, 20]. По результатам тренировки и рассмотрения заявок избирательных комиссий ЦИК России принял решение организовать протестированное ДЭГ в 7 субъектах РФ на выборах 2021г. [15]. По данным ЦИК в общей сложности 2 535 978 избирателей проголосовали с помощью ДЭГ, что составляет четверть от численности населения, проживающих в этих субъектах избирателей, имеющих подтвержденные записи на портале госуслуг [15, 19, 20].

В 10 сентября 2023 в России завершился единый день голосования. Выборы прошли в 85 регионах, Выборы губернаторов прошли в 21 регионе, в том числе в Московской области (в Москве выбирали мэра). ДЭГ использовалось в 25 регионах (включая Москву). ДЭГ осуществлялось на региональной платформе ДЭГ (портал vybory.gov.ru), в Москве — через собственную региональную платформу (голосование проходит на сайте elec.mos.ru).

Были реализованы два пилотных проекта: "Мобильный УИК" и "Стоп-дубль". Приложение «Мобильная УИК» создано для членов избирательных комиссий, которые проводят поквартирные обходы и информируют граждан о выборах. С помощью этого приложения цифровой сервис ускоряет и облегчает работу членов участковых избирательных комиссий (УИК) по своевременному доведению до избирателей всей необходимой информации о выборах: дате голосования, возможных формах, кандидатах и партиях, уточнению списков избирателей. Проект «Стоп дубль» позволяет проверять избирателей и предотвращать многократное голосование. В этом году были также формально упразднены открепительные удостоверения[9].

[9] URL:https://www.rbc.ru/politics/11/09/2023/64f879ee9a7947cbe7bb2323

1.5. Функциональные требования к системе дистанционного электронного голосования

На основе анализа систем ДЭГ разного уровня и назначения, можно сформулировать следующие функциональные требования к системе ДЭГ, подробно изложенные в [21- 26]:

- Система ДЭГ должна состоять из распределенного идентичного аппаратно-программного комплекса узлов, расположенного в разных зданиях на территории избирательного участка с подключением к Интернету. Например, в ДЭГ России количество узлов составляет не менее одного на 5000 избирателей. Сбой менее чем в 25% узлов не должен нарушать работу всей системы.
- В системе ДЭГ список данных избирателей не может быть изменен. Кроме того, список должен совпадать со списком избирателей на этапе регистрации.
- Система должна иметь программное обеспечение и оборудование для наблюдения за работой системы в день голосования. Программы наблюдения размещены в каждом участке ДЭГ.
- В системе записывается и хранится следующая информация: текущие дата и время с точностью до одной секунды; дата и время внесения записи; число зарегистрированных избирателей; число избирателей, правильно прошедших идентификацию и аутентификацию; число избирателей, которые получили бюллетень; число избирателей, отправивших правильно заполненные бюллетени в систему ДЭГ.
- Штаб по наблюдению за выборами должен получать аналитическую информацию о работе системы в день голосования и во время подсчета голосов с задержкой не более 5 секунд.
- Предоставить избирательной комиссии инструменты для контроля доступа к информации, которая хранится и обрабатывается в системе

(например, список избирателей, данные избирателя, отметка о получении избирательного бюллетеня и т.д.).

- Обеспечивать стабильное интернет-соединение между избирателем и системой во время голосования.
- Обеспечивать устойчивость системы к взлому, включая программное и аппаратное обеспечение, встроенное в персональный компьютер избирателя.
- Наблюдатели и эксперты могут проверить работу системы, используя программное обеспечение и оборудование, которые были представлены избирательным комиссиям ранее, до дня голосования.

1.6. Требования по обеспечению информационной безопасности к системе дистанционного электронного голосования

В этом разделе, перечислим основные требования безопасности к системе ДЭГ, которые должны быть выполненные в разрабатываемой системе ДЭГ:

1. Тайна голосования. Результаты голосования каждого избирателя должны храниться в тайне от других участников, включая избирательную комиссию. Кроме того, ДЭГ должен быть организовано таким образом, чтобы обеспечивалась тайна передачи голосов на всех этапах процедуры голосования.
2. Анонимность избирателя. В системе ДЭГ не должно быть связи между поданным голосом и конкретным избирателем. В этом случае голоса остаются анонимными.
3. Аутентификация избирателя. Голосовать имеют право только уполномоченные избиратели. Списки избирателей составляются Избирательной комиссией (ИК) заранее.
4. Уникальность. Ни один избиратель не имеет право голосовать более одного раза.

5. Подтверждение голосования. Система голосования посылает электронное письмо избирателю, в качестве подтверждения того, что его голос корректно был принят системой.
6. Точность голосования. Система ДЭГ должна гарантировать соответствие количества электронных голосов количеству избирателей. Если избиратель попытается проголосовать еще раз или изменить свой выбор, система должна предотвратить это.
7. Проверка корректности заполнения избирательного бюллетеня. Система должна обеспечить контроль правильности заполнения бюллетеня избирателем, исходя из возможных значений (ЗА и ПРОТИВ) без ознакомления с выбором избирателя.
8. Система должна иметь возможность предотвращать угрозу нарушения тайны волеизъявления и анонимности голосующего со стороны административного ресурса.

Также в системе ДЭГ должны выполняется дополнительные требования:

9. Целостность. Никто не имеет право изменить голос, отданный за соответствующего кандидата.
10. Должны быть приняты меры по недопущению фальсификации голосов законных избирателей, которые не хотели и не могли принять участие в голосовании.
11. Надежность. В случае возникновения какой-либо технической причины (например, отсутствия подключения к Интернету), система должна оставаться надежной и не допуская потери голосов.
12. Проверяемость. Наблюдатели или те, кто заинтересован, могут проверять работу системы и процесс подсчета голосов.
13. Тайна сведений об избирателе. В системе ДЭГ должны обрабатываться и храниться только те личные данные, которые необходимы для ДЭГ в течение конкретного времени. Списки избирателей и общение с ними через систему электронного голосования должны быть доступны только уполномоченным лицам.

14. Личное голосование. Система ДЭГ должна осуществлять проверку участия в выборах только избирателей, подавших заявки на участие в выборах, а также позволять членам комиссии и наблюдателям проверять, что все избиратели из списка избирателей лично подали заявки на участие в голосовании.
15. Система ДЭГ должна распознавать голоса, подвергшиеся несанкционированной обработке.

Как видно из вышесказанного, к системе ДЭГ предъявляется обширный список требований. В нашем исследовании сосредоточимся на основных требованиях по обеспечению информационной безопасности.

1.7. Постановка задачи исследования

Проведенный выше анализ показал, что системы дистанционного электронного голосования имеют важные преимущества перед существующими системами бумажного голосования. Их внедрение в республике Ирак и других арабских государствах с парламентской формой управления является актуальной задачей, решение которой позволит реализовать все преимущества внедрения ДЭГ. Это увеличение скорости подсчета результатов голосования, снижение затрат, повышение точности результатов, предоставление удобства голосования для избирателей с ограниченными возможностями, а также увеличение числа молодых избирателей. Поскольку система ДЭГ основана на интернет-платформе, она подвержена рискам нарушения ее защищенности. Поэтому она должна обеспечивать выполнение многих требований информационной безопасности, наиболее значимыми из которых являются обеспечение тайны голосования и анонимности избирателей. Эти требования могут быть решены только на основе криптографических методов.

Целью работы является обеспечение защищенности от угроз безопасности информации в системах дистанционного электронного голосования на парламентских выборах в республике Ирак и других арабских государствах.

Для достижения цели исследования в работе решена научная задача: разработка научно-методического аппарата для создания безопасной системы дистанционного электронного голосования на парламентских выборах в арабских государствах, с учетом особенностей избирательного процесса на основе использования гомоморфного шифрования с распределенным дешифрованием.

К таким особенностям следует отнести необходимость учета следующих специфических факторов:

- Принятие большого количества избирателей, желающих принять участие в выборах, в том числе тех, кто живет за границей;
- Предотвращать (блокировать) угрозы, связанные с влиянием субъективного фактора: администрации избирательных комиссий, мнения религиозных деятелей и старейшин;
- Учитывать особенности менталитета избирателей, осознающих свою идентичность, как части арабского мира, имеющих общую историю, языковое и культурное родство;
- Блокировать кибер-атаки на инфраструктуру системы ДЭГ. (При традиционном бумажном голосовании аналогом такой атаки были случаи кражи избирательных ящиков);
- Учитывать особенности социальной структуры традиционного общества, характер политической системы арабских стран.

Для решение научной задачи необходимо решение частных задач:

– исследование принципов построения современных систем ДЭГ;
– анализ угроз в системе ДЭГ и способов их предотвращения (блокирования), обоснование требований к системам ДЭГ;
– разработка модели перспективной системы дистанционного электронного голосования с учетом специфики голосования в арабских странах;

- разработка протокола перспективной системы дистанционного электронного голосования с учетом специфики голосования в арабских странах;
- исследование методов защиты от угрозы преднамеренного или случайного неправильного заполнения бюллетеня избирателем в системе дистанционного электронного голосования;
- разработка метода проверки корректности заполнения избирательного бюллетеня в целом.

Выводы по 1-й главе

1. Проведен анализ существующей системы голосования в Республике Ирак, применяемой на выборах 2021 года, отмечены присущие ей угрозы и недостатки. Недостатки и угрозы традиционной системы голосования в основном обусловлены влиянием субъективного фактора и технологией обработки бумажных бюллетеней. Такие недостатки могут быть преодолены с переходом к системам дистанционного электронного голосования (ДЭГ).
2. Рассмотрены и изучены особенности избирательных систем в других арабских странах с парламентской правовой системой. Законодательные органы власти арабских стран формально строятся на демократической основе, а именно на основе всеобщего, равного и прямого избирательного права при тайном голосовании. В целом организация и проведение выборов в арабских странах совпадает с общемировой практикой, однако им присущи свои специфические особенности, связанные с культурными и цивилизационными особенностями,
3. Проведен анализ методов построения систем дистанционного электронного голосования и опыта их внедрения в разных странах. В результате проведенного исследования можно сделать вывод, что

разработка надежных систем ДЭГ являются предметом интереса многих стран.

4. Сформулированы функциональные требования и требования информационной безопасности к перспективной системе ДЭГ для республики Ирак. Выделена группа основных требований безопасности информации в системе ДЭГ: тайна голосования; анонимность; аутентификация избирателя; уникальность; точность и подтверждение голосования, которые определяют структуру и протоколы системы ДЭГ.

ГЛАВА 2. МОДЕЛЬ ПЕРСПЕКТИВНОЙ СИСТЕМЫ ДЭГ ДЛЯ АРАБСКИХ ГОСУДАРСТВ С ПАРЛАМЕНТСКОЙ ПРАВОВОЙ СИСТЕМОЙ, В ТОМ ЧИСЛЕ ДЛЯ РЕСПУБЛИКИ ИРАК НА ОСНОВЕ РАСПРЕДЕЛЕННОЙ СЕТИ БЛОКЧЕЙН-УЗЛОВ С ИСПОЛЬЗОВАНИЕМ СМАРТ-КОНТРАКТОВ

2.1. Анализ принципов построения современных систем ДЭГ

В данном разделе анализируются и предлагаются способы построения современных систем ДЭГ, с учетом выполнении требований информационной безопасности.

Современная система ДЭГ в общем случае включат в себя следующие компоненты:

– Избирателей;
– Избирательную комиссию (ИК);
– Избирательный бюллетень (ИзБ);
– Сервер (серверы);
– Доску объявлений и/или блокчейн (БЧ);
– Наблюдателей;
– Сайт выборов.

Функционирование системы осуществляется поэтапно, как показано на рис.2.1:

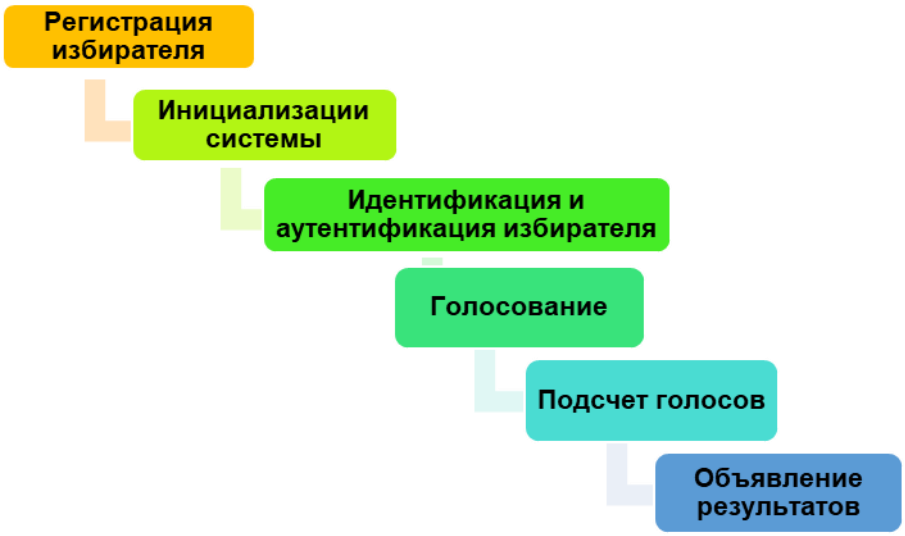

Рис. 2.1. Этапы работы системы ДЭГ

При построении системы ДЭГ обязательно должны быть выполнены требования информационной безопасности в первую очередь: обеспечение тайны волеизъявления избирателя и его анонимности. Рассмотрим способы построения систем ДЭГ с учетом выполнения этих требований.

2.1.1. Система ДЭГ на основе микс-сети

В 1981 году Чаум [35] представил метод, основанный на криптографии с открытым ключом, который позволяет системе электронной почты скрывать содержание сообщения, а также с кем общается участник.

Это достигается применением микс-серверов и микс-сетей. Целью использования микс-сети является скрытие связи между элементами во входных данных и элементами в выходных данных [35].

Как показано на рисунке 2.2, отправитель хочет передать сообщение получателю с помощью микс-сервера (допустим, существует только один микс сервер).

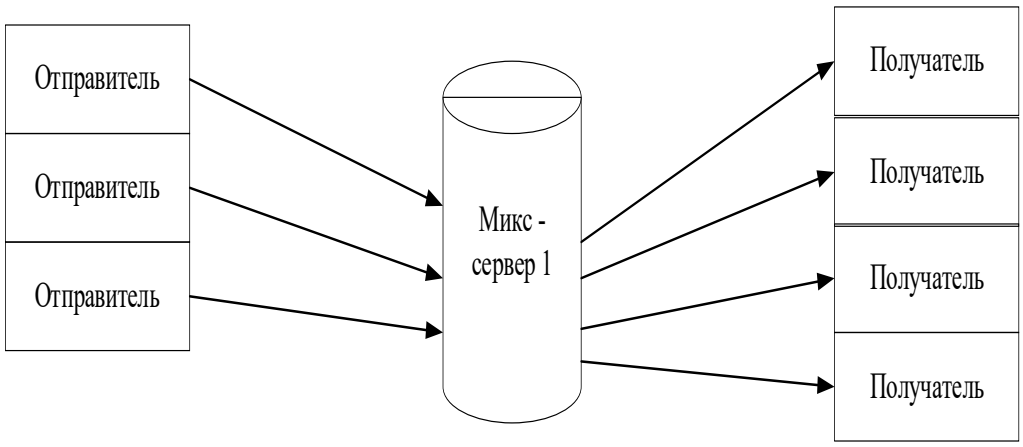

Рис. 2.2. Простое описание метода микс- сети

Микс-сервер (МС) обрабатывает каждое почтовое сообщение от отправителя его перед доставкой получателю [33, 34].

Принцип работы МС, представленный Чаумом, заключается в следующем [35]:

- Отправитель и микс-сервер используют криптографическую систему с открытым ключом (например, РША [39]) для генерации своей пары ключей (открытого *h* и закрытого *s*). Открытый ключ публикуется на доске объявлений, а закрытый ключ остается секретным на сервере.

- Отправитель *A* подготавливает сообщение *M*, которое он хочет отправить пользователю *B*, добавляет к сообщению случайное значение R_o и шифрует его открытым ключом адресата h_b. Затем, добавляет адрес *B*, и результат шифрует открытым ключом микс-сервера h_{mk1}, Криптограмма имеет следующий формат:

$$h_{mk1}(R_1, h_b(R_0, M), B). \quad (2.1)$$

Число R_0 необходимо для того, чтобы злоумышленник не мог угадать сообщение М.

После, получения зашифрованного сообщения микс-сервер, использует свой секретный ключ *s* и расшифровывает его. Внутри сообщения он находит адрес получателя *B* и зашифрованное сообщение, привязанное к *B*. Случайная строка R_1отбрасывается, как видно из выражения (2.1).

Аналогично, сервер поступает с криптограммами, полученными от других отправителей.

- Микс-сервер расшифровав с помощью закрытого ключа входные данные (криптограммы отправителей) перемешивает их. Затем, отправляет сообщения получателю *B*.

- После этого, получатель *B* расшифровывает полученное зашифрованное сообщение, используя свой закрытый ключ.

Цель перемешивания сообщения состоит в том, чтобы было невозможным для посторонних лиц установление связи между входными и выходными данными микс-сети.

Для предотвращения сговора между сервером и получателем используется не один сервер, а несколько серверов. В этом случае сервера

передают сообщения друг другу, а последний сервер передает сообщения получателю [35].

Анонимность передачи сообщения обеспечивается, если хотя бы один сервер микс-сети будет честным.

Этот метод можно использовать в системах тайного голосования в Интернете. В этом случае необходимо обеспечить анонимность голосования не только от посторонних лиц, но и от членов избирательной комиссии.

Чтобы разорвать связь между данными избирателей и их бюллетенями, то есть обеспечить анонимность избирателей используется свойство рандомизированности криптограмм в криптосхеме Эль-Гамаля [36].

Предположим, что ключи шифрования и дешифрования для КС ЭГ сгенерированы, этап идентификации и аутентификации избирателя пройден успешно.

Этап голосования

- Избиратель выбирает своего кандидата.

- Шифрует бюллетень по схеме Эль-Гамаля с использованием открытого ключа *h*:$C = (A, B) = (g^r, h^r \cdot G^v)\ mod\ p.$ (2.2)

где $v \in \{0,1\}$ - голос избирателя, r – случайное число, *G* – примитивный элемент над полем Галуа GF(p), *h*- открытый ключ.

- Микс-сервер рандомизирует зашифрованные бюллетени *Ci* и перемешивает их. Затем, выходные, зашифрованные бюллетеня, могут быть переданы другому микс-серверу, снова рандомизированы и перемешаны.

Для рандомизации зашифрованного текста он умножается на криптограмму C_1, представляющую зашифрованное сообщение равное 0.

$$C_1 = (A_1, B_1) = \left(g^{r'}, h^{r'} \cdot G^0\right)\ mod\ p. \quad (2.3)$$

После перемножение двух криптограмм получаем криптограмму:

$$(A, B) \cdot (A_1, B_1) = (g^{r+r'}, h^{r+r'} \cdot G^v). \quad (2.4)$$

Перехват этой криптограммы не позволяете нарушителю установить связь между входными и выходным данными микс-сервера.

Последний сервер отправляет зашифрованные бюллетени в избирательную комиссию.

Этап расшифровки бюллетеня и подсчет голосов

ИК расшифровывает полученные зашифрованные бюллетени, используя свой закрытый ключ, и подсчитывает голоса. Зашифрованные бюллетени ИК получает после того, как микс-серверы рандомизировали и перемешали их, поэтому после расшифровки бюллетеня ИК не может установить связь между результатами голосования избирателей и отправителями бюллетеней.

2.1.2. Система ДЭГ на основе слепой подписи

Слепая подпись (СП) — это криптографическое преобразование, которое применяется в таких ситуациях, когда отправитель хочет, чтобы получатель подписал полученное сообщение, без ознакомления с его содержанием [30, 32, 38]. СП предложена в 1983 году Д. Чаумом.

СП применяется в различных областях, включая анонимные голосования, договоры и соглашения, а также в цифровых документах, где обязательны условия обеспечения тайны голосования, анонимности и аутентификации избирателя [39,40,41].

Рассмотрим этапы работы системы ДЭГ, основанные на технологии СП [27, 30, 40 - 42]:

Этап инициализации системы

- ИК готовит список легитимных избирательных и публикует его на ДО.

- Также ИК генерирует свои открытый $h_{ИК}$ и закрытый ключи $s_{ИК}$ и публикует $h_{ИК}$ на ДО;

- Каждый избиратель генерирует свою пару ключей $(h_{И}, s_{И})$ по схеме асимметричного шифрования и публикует открытый ключ на ДО;

- Также он генерирует свой идентификационный номер (ИН) – I;
- Затем, он маскирует свой идентификационный номер I:

$$I_m = m^{h_{ик}} \cdot I \; mod \; n_{ик}. \quad (2.5)$$

где $h_{ик}$ - открытый ключ ИК, m – случайно сгенерированное целое число из диапазона $(1, 2, \dots, n_{ик} - 1)$, являющееся взаимно простым с $n_{ик}$, т. е. выполняется условия $\gcd(m, n_{ИК}) = 1$.

- Для того, чтобы ИК подписала каждому легитимному избирателю по одному идентификационному номеру, ИК должна знать, что они являются легитимными. Поэтому каждый избиратель зашифровывает свой номер n и маскированный идентификационный (т.е I_m) своим секретным ключом $s_И$, т. е. он направляет ИК по открытому каналу следующее сообщение:

$$M_1 = \left(n, E_{s_И}(n, I_m)\right). \quad (2.6)$$

где $s_и$ - закрытый ключ избирателя, n – порядковый номер избирателя в списке легитимных избирателей.

- ИК публикует все полученные сообщения M_1 на ДО. Далее, ИК расшифровывает криптограмму, содержащую в сообщении M_1, используя для этого открытый ключ избирателя $h_И$ с номером n, опубликованный на ДО. Если значение n, содержащееся в открытой части сообщения M_1 и в расшифрованной криптограмме совпадут, то ИК может быть уверена, что данное сообщение действительно получено от n-го избирателя.
- ИК подписывает маскированный ИН избирателя

$$I_{sm} = I_m^{s_{ик}} \; mod \; n_{ИК}. \quad (2.7)$$

и отправляет I_{sm} по открытому каналу к n-му избирателю и помещает (вместе с номером n) на общедоступном сайте.

- Избиратель демаскирует подписанный ИН следующим образом:

$$(I_{sm})/m \; mod \; n_{ик} = {(m^{h_{ик}} \cdot I)^{s_{ик}}}/{m} \; mod \; n_{ик} = \frac{m^{h_{ик} \cdot s_{ик}}}{m} \cdot I^{s_{ик}} mod \; n_{ик} = I^{s_{ик}}. \quad (2.8)$$

В итоге избирателе получил идентификатор, подписанный ИК, но ИК не знает какому избирателю она пописала идентификатор.

Этап голосования

- Избиратель создает бюллетень с результатом своего голосования,

Зашифровывает его: $M_2 = (P, E_{h_И}(I, I_s, v)$ (2.9)

где P – любое число, v- голос избирателя.

и отправляет в ИК по анонимному каналу.

- ИК публикует M_2 (в зашифрованном виде) на ДО;

- Избиратели посылают в ИК по анонимному каналу сообщение M_3, содержащее ключ расшифровки криптограммы M_2 по анонимному каналу:

$$M_3 = (P, s_И, n_И). \quad (2.10)$$

Этап расшифровки избирательного бюллетеня и подсчет голосов

- ИК с помощью ключа $(s_И, n_И)$ расшифровывает M_2.

Расшифровав M_2, ИК может учесть голос легитимного, но не известного ей избирателя поскольку его идентификатор был е подписан ИК.

Далее выполняется подсчет голосов, поданных за каждого кандидата, и объявляются итоги голосования.

Система обеспечивает анонимность избирателя за счет использования маскированного идентификатора подписанного СП ИК. Однако для полной анонимности в этой системе требуется использование дополнительного анонимного канала.

2.1.3. Система ДЭГ на основе гомоморфного шифрования

2.1.3.1 Аддитивный и мультипликативный гомоморфизм

Под гомоморфным шифрованием (ГШ) понимается криптографический примитив, представляющий собой функцию шифрования, удовлетворяющую дополнительному требованию гомоморфности относительно каких - либо алгебраических операций над открытыми сообщениями [30, 43, 48].

Гомоморфное шифрование (ГШ) позволяет производить операции над зашифрованными данными, не расшифровывая их и не раскрывая секретный ключ [44 - 49].

ГШ имеет особое значение для сферы информационной безопасности, поскольку оно позволяет проводить обработку и анализ данных, не нарушая их конфиденциальность. ГШ может быть использовано в различных областях, таких как обработка данных в облаке, финансовые технологии, медицинские исследования, анализ социальных сетей, системы ДЭГ и многое другое [50 - 53].

ГШ относится к новым направлениям в криптографии и является активно развивающейся областью науки и технологий. Однако, из-за вычислительной сложности и низкой производительности ГШ наиболее подходит для операций, не требующих большого объема вычислительных ресурсов [51].

Система ГШ обладает свойством гомоморфизма по отношению к операциям сложения или умножения [29, 30, 43 - 54]:

$$Dec\big(Enc(m_1) + Enc(m_2)\big)\, mod\, p = m_1 + m_2\ . \quad (2.11)$$

$$Dec\big(Enc(m_1)\ \times\ Enc(m_2)\big)\, mod\, p = m_1 \times m_2\ . \quad (2.12)$$

$$Dec\big(Enc(m_1)\ \times\ Enc(m_2)\big)\, mod\, p = m_1 + m_2\ . \quad (2.13)$$

$$Dec\big(Enc(m_1) +\ Enc(m_2)\big)\, mod\, p = m_1 \times m_2\ \ . \quad (2.14)$$

где *Enc()* - функция шифрования; *Dec()* - функция дешифрования*; m*- открытый текст.

Существуют два типа ГШ: полностью гомоморфное шифрование и частично гомоморфное шифрование [28, 51, 54, 55].

Полностью ГШ позволяет производить любые операции над зашифрованными данными, включая сложение, вычитание, умножение и другие математические операции. Однако, эта технология до сих пор находится в стадии разработки и имеет высокую вычислительную сложность, а также требует большого объема памяти для работы [55].

Частично ГШ позволяет производить только определенные операции или их небольшие комбинации. Данная технология гомоморфного шифрования распространена и широко используется в различных предметных областях. К таким системам относятся криптосистема RSA, криптосистема Эль-Гамаля [36],

криптосистема Гольдвассер-Микали, криптосистема Пэйе [57] и криптосистема Бенало [56].

В нашем исследовании рассматриваются частично гомоморфные системы на примере схемы Эль-Гамаля [36, 37].

Схема Эль-Гамаля

Криптосистема с открытым ключом (ЭГ) предложена Тахером Эль-Гамалом в 1985 году [36]. Её стойкость основывается на сложности вычисления дискретных логарифмов в конечном поле [36]. Дискретное логарифмирование – это задача нахождения числа x из заданного конечного поля $GF(p)$, такого что

$$g^x \equiv y \ (mod\ p), \tag{2.15}$$

где g, y - известные элементы поля $GF(p)$, p - простое число.

Схема состоит из трех шагов: генерация ключа, шифрование сообщения и дешифрование криптограммы.

Шаг 1: Генерация ключей

- Генерируется случайное простое число p;
- Выбирается целое число g — первообразный корень p;
- Выбирается случайное целое число s, $1 < s < p - 2$;
- Вычисляется $h = g^s \ mod\ p$. (2.16)

Открытым ключом в схеме ЭГ является числа (h, g, p), закрытым ключом число s.

Шаг 2: Шифрование

Сообщение M шифруется следующим образом:

- Выбирается случайное число r, $1 \leq r \leq p - 1$;
- Вычисляются числа $A = g^r mod\ p$ и $B = h^r M\ mod\ p$. (2.17)

где числа (A, B) – образуют криптограмму.

Шаг 3: Дешифрование

Выполняется по формуле: $M = B \cdot A^{-s}\ mod\ p$, (2.18)

где s – секретный ключ получателя сообщения,

Далее, рассмотрим систему ДЭГ на основе схемы шифрования ЭГ с аддитивным гомоморфизмом [43 – 47, 49 - 54].

Система ДЭГ включает в себя: избирателей, сервер, доска объявления (ДО) и ИК (см. рис. 2.3).

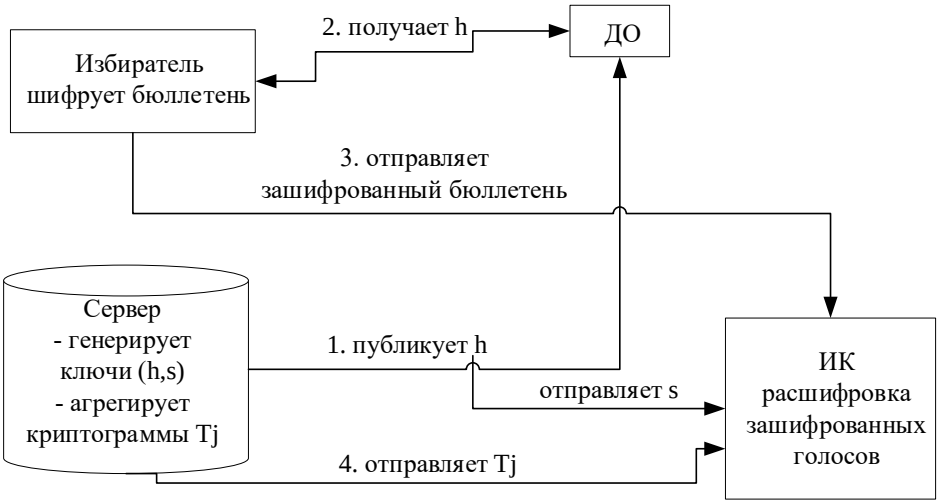

Рис. 2.3. Схема ДЭГ, основанная на гомоморфном шифровании

Этап инициации

- Доверенный сервер генерирует открытый и закрытый ключи криптосистемы ЭГ (шаг 1). Открытый ключ h публикуется на ДО.
- Избиратель загружает открытый ключ h из ДО. Секретный ключ s хранится на сервере или может быть разделен на доли и находиться у хранителей ключа до окончания выборов (шаг 2).

Этап голосования

- Каждый избиратель выбирает кандидата (кандидатов) из списка кандидатов;
- Шифрует свой голос v_i с помощью открытого ключа и отправляет его в ИК (шаг 3).
- $C_i = (A_i, B_i) = (g^{r_i}, h^{r_i} \cdot G^{v_i})$.

Этап расшифровки избирательного бюллетеня и подсчет голосов

- После завершения голосования, сервер осуществляется агрегирование криптограмм всех избирателей, отданных за кандидата j:

$T_j = \prod_{i=1}^{n} C_{nj} \; mod \; p,$

$$T_j = C_{1j} \cdot C_{2j} \cdot \ldots \cdot C_{nj} = (A_1 \cdot A_2 \cdot \ldots \cdot A_n, B_1 \cdot B_2 \cdot \ldots \cdot B_n) \bmod p, \quad (2.19)$$

$j = 1, 2, .., k$ и отправляет криптограмму T_j в ИК;

- ИК, используя ключ дешифрования s, осуществляет дешифрование агрегированных бюллетеней и подсчет голосов.

$$\frac{h^{(\Sigma r_i)} \cdot G^{\Sigma v_i}}{g^{\Sigma r_i s}} = \frac{g^{(\Sigma r_i)s} \cdot G^{\Sigma v_i}}{g^{(\Sigma r_i)s}} = G^{\Sigma v_i} \; mod \; p, \quad (2.20)$$

- Подсчет голосов

Для гомоморфной схемы ЭГ сумма всех голосов, отданных за j-го кандидата, вычисляется как: $\sum_{i=1}^{n} v_{ij} = \log_G G^{\Sigma v_{ij}} \; mod \; p,$ (2.21)

Логарифм вычисляется по таблице, которая составляется до начала выборов, с учетом количества избирателей, как представлено в таблице 2.1. После этого ИК объявляет итоги выборов.

Таблица 2.1. Общий вид таблицы возможных результатов голосования

$\sum v_{ij}$	$G^{\Sigma v_{ij}} \; mod \; p$
0	$G^0 \; mod \; p$
1	$G^1 \; mod \; p$
2	$G^2 \; mod \; p$
…..	
n	$G^n \; mod \; p$

Анонимность голосов избирателей при использовании гомоморфной криптосистемы обеспечивается за счет того, что ИК после расшифрования получает сумму голосов, поданных за кандидата, из которой не видно, как проголосовал отдельный избиратель.

В таблице 2.2 представлен сравнительный анализ систем ДЭГ, использующих разные методы их построения [30, 32, 52, 53, 58, 59].

Таблица 2.2. Сравнение методов построения современных систем ДЭГ

Методы / Свойство	Микс-сети	Слепая подпись	Гомоморфное шифрование
Выполнение требований безопасности	Обеспечивается тайна голосования; анонимность за счет перемешивания бюллетеней и невозможности установить связь между бюллетенем и его отправителем; аутентификация избирателя.	Обеспечивается тайна голосования и анонимность избирателя, за счет слепой подписи ИК идентификационного номера избирателя; аутентификация избирателя.	Обеспечивается тайна голосования и анонимность голосования избирателя за счет того, что происходит расшифровка сразу всех агрегированных бюллетеней; аутентификация избирателя.
Преимущества	-Разрушает связь между источником сообщения и получателем, затрудняя перехват сообщения, так как каждый узел знает только информацию о предыдущем узле и адрес следующего получателя.	-Особенность такой схемы заключается в том, что подписавший не знает содержание подписанного документа (не знает идентификатор избирателя)	-Эффективный подсчет голосов; -Простота реализации;
Недостатки	-Ненадежность узлов; -Медленно осуществляется подсчет голосов.	-Необходимо выполнить дополнительные процедуры, связанные с со слепой подписью	-Выполнение интенсивных вычислений больших чисел с зашифрованными данными требует

		идентификатора избирателя; -Процесс подсчета голосов идет медленно; -Требуется дополнительный анонимный канал.	дополнительных вычислительных затрат. -Могут использоваться только криптосистемы, поддерживающие гомоморфное шифрование.

Как видно из таблицы 2.2, метод ГШ имеет значительные преимущества перед другими методами. Вследствие этих преимуществ гомоморфной системы для обеспечения безопасности избирательного процесса будем использовать ее в качестве основы для разрабатываемой модели.

2.2. Система ДЭГ на основе технологии блокчейн

Блокчейн — это распределенная база данных, способная хранить и обрабатывать данные в равной степени на множестве компьютеров. Принцип работы БЧ основан на создании блоков информации и последующем их цепочном связывании с помощью криптографических методов [60 – 67, 99]. Краткие сведения об технологии блокчейн приведены в Приложении 1. Основные отличия и преимущества технологии БЧ по сравнению с обычной распределенной базой данных заключаются в следующем [69]:

- база данных, требует наличия администратора для управления, а децентрализованный БЧ в этом не нуждается;
- база данных основывается на архитектуре клиент/сервер. БЧ использует архитектуру распределенного леджера;
- в БЧ изменения в блок данных вносятся на основе консенсуса доверенных узлоа, в базе данны этого нет;

- в базе данных, в отличие от БЧ, хранящиеся данные могут быть изменены или удалены.

БЧ является хорошим вариантом для использования в системах голосования и в последнее время технология БЧ начала использоваться в избирательных процессах для повышения безопасности системы голосования в первую очередь как средства децентрализованного и надежного хранения информации всех участников избирательного процесса без возможности ее изменения посторонними лицами [67].

Рассмотрим классификацию систем ДЭГ, основанных на системе БЧ [60, 62, 67]:

- Система голосования на основе криптовалюты. Бюллетени кандидату выдаются на основе оплаты, которую он/она получает от избирателей. Проблема с такими системами заключается в том, что злонамеренные избиратели с целью сохранения денег, могут отказаться “платить” кандидатам.
- Система голосования на основе смарт-контрактов, которая поддерживает только двух кандидатов, а голосование ограничено определенным числом участников.
- Использование БЧ в качестве урны для голосования с целью поддержки целостности бюллетеней.

Для того, чтобы технология БЧ была применена на выборах, необходимо ответить на следующие вопросы:

1. Какой тип блокчейн-сети будет использован?

Существуют различные типы блокчейн-сетей: публичный; частный и консорциума. При выборе типа сети нужно учитывать такие факторы: уровень децентрализации; информационная прозрачность; комиссия за транзакцию или скорость добавления транзакции в сеть.

2. Какой алгоритм консенсуса используется в БЧ?

3. С каким сервером или программой может интегрироваться БЧ?

БЧ должен иметь возможность интегрироваться с сервером проверки личности избирателя, сервер регистрация и др.

4. Как может поддерживаться необходимый уровень анонимности?

Многие из существующих систем голосования, основанных на блокчейне, полагаются на неинтерактивные доказательства с нулевым разглашением в качестве меры для достижения правильного баланса между тайной голосования и проверке результатами голосования.

После ответов на эти вопросы можно выбрать тип блокчейна, который может применения на системы ДЭГ. Таким образом при выборе блокчейна для системы ДЭГ необходимо принять во внимание следующие характеристики:

- тип блокчейна - частная сеть с разрешенным доступом (к примеру: блокчейн – консорциума [70]);
- алгоритм консенсуса: доказательство власти;
- доступ только через персональный ключ (PIN);
- обеспечение анонимности;
- публичная проверяемость (все заинтересованные стороны избирательного процесса, включая людей, наблюдающих за процессом голосования, могут проверить всю процедуру и результат выборов;
- блокчейн должен интегрироваться с другим программным обеспечением или сервером, используемых в системе голосования.
- только легитимные избиратели могут получить доступ к блокчейну.

В таблице 2.3 представлены страны, в системах ДЭГ которых применялась в разной степени технология блокчейн [71].

Таблица 2.3. Примеры использования технологии Блокчейн на выборах в разных странах [71]

Страна/Город	**Описание**	**Комментарий**
Россия	Система ДЭГ применялся в 7 регионах Российской Федерации: в городах Москве и Севастополе, а также в Курской,	17- 19 сентября 2021 года

	Мурманской, Нижегородской, Ростовской и Ярославской областях.	
Корея Проект сообщества южнокорейской провинции Кенгидо	Провинция использовала систему голосования на основе блокчейн для сбора голосов по общественным проектам.	Корейский финансово-технологический стартап Block разработал Блокчейн-платформу
Эстония	Эстонская биржа Nasdaq протестировала e-voting — систему голосования в кругу акционеров компании, которая работает по блокчейн-технологии.	В 2017г.
Сьерра-Леоне	Впервые в истории Сьера_Леогне прошли выборы Президента с применением технологии блокчейн.	На выборах в 2018г.

Рассмотрим обобщенную схему использования БЧ в системе ДЭГ [60 - 67] (рис. 2.4).

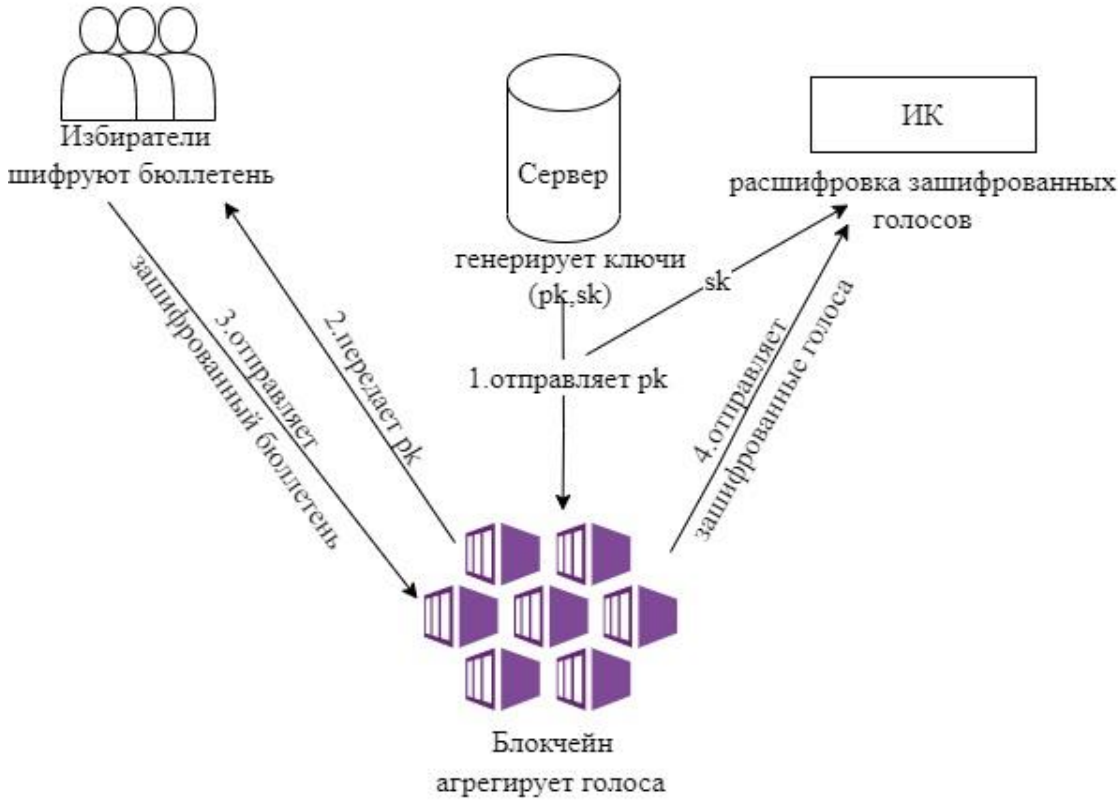

Рис. 2.4. Система ДЭГ на основе БЧ

Предположим, что ключи уже созданы.

1. Запрос о голосовании. Избиратель должен войти в систему голосования, используя свои учетные данные (имя пользователя и пароль). Система проверяет введенную информацию. В случае, если проверка прошла успешно, то избиратель может проголосовать.
2. Голосование. Избиратель выбирает своего кандидата. Голосование осуществляется через пользовательский интерфейс.
3. Шифрование голосов. Выбор избирателя шифруется с использованием схемы ГШ и криптограмма (транзакция) отправляется в БЧ.
4. Добавление голосов в БЧ. Блок создается в БЧ. После создания блока и в зависимости от выбранного кандидата информация записывается в БЧ.

Первой транзакцией, добавленной в блок, будет специальная транзакция, представляющая кандидата и содержащая его имя. Она будет служить базовым

блоком, а каждый голос за конкретного кандидата будет помещен поверх него. В отличие от других транзакций, эта транзакция не будет участвовать в подсчете голосов и будет содержать только имя кандидата. Зашифрованный бюллетень (новая транзакция) будет записан в блок. Каждый блок привязывается к ранее поданному голосу.

Системы голосования, основанные на блокчейне, имеют ряд преимуществ перед обычными, например, голоса избирателей не будут храниться на одном сервере, никто не сможет узнать результаты голосования до завершения голосования, и голос избирателя не изменится при сохранении в блокчейне [60, 65].

2.2.1. Квантово-устойчивый блокчейн (квантовый бдокчейн)

Технология БЧ может оказаться уязвимой для взлома после появления квантовых суперкомпьютеров. Вычислительная мощность таких компьютеров практически не ограничена, с их помощью можно взламывать современные системы асимметричного шифрования, подделывать электронные подписи, вычислять хэш-коды, которые практически невозможно взломать с помощью суперкомпьютеров пятого поколения с высокой и сверхвысокой производительностью (более 10^{18} операций в секунду). Злоумышленники при большом желании и достаточных ресурсах могут незаметно вносить изменения в БЧ или препятствовать его использованию другими участниками сети [73 - 75].

В настоящее время ведутся работы по разработке эталонной модели корпоративных блокчейн систем устойчивых как к обычным атакам, так и атакам с помощью квантового компьютера. В этих работах принимают участие следующие организации [78].

- Международная организация по стандартизации (ИСО)[10]. В 2016 году был создан специальный комитет ИСО/ТК 307 «блокчейн и технологии распределенных реестров».
- Международный союз электросвязи (ITU). В 2017 году учреждена фокус-группа по применению технологий распределенного реестра (FG DLT).
- Европейские организации по стандартизации (ESO). CEN-CENELEC и ETSI, в 2018 году подготовила рекомендации по успешному внедрению новых технических стандартов для технологий распределенного реестра/блокчейна в Европе.
- Профессиональная техническая организация по развитию технологий Институт инженеров электротехники и электроники (IEEE).

Их исследования находят отражение в публикуемых проектах, отчетах, материалах проводимых ими научных форумов.

В 2017 году ученые из Российского квантового центра создали концептуальную модель устойчивого-блокчейна (сокращенно квантового блокчейна) - неразрушимую распределенную систему хранения данных, защищенную от атак с помощью квантового компьютера и использующую квантовую систему передачи данных [74].

Квантовый блокчейн отличается от обычных типов блокчейнов тем, что в нем используются методы криптографии устойчивые к атакам с использованием квантового компьютера и квантовые системы передачи данных. И такие методы (криптографические примитивы) уже разработаны и находятся в стадии оформления проектов международных стандартов.

По итогам третьего раунда открытого конкурса лучших постквантовых алгоритмов асимметричного шифрования, электронной подписи и распределения ключей, проведенного Национальным институтом стандартов и технологий (National Institute of Standards and Technology NIST) в 2016-2023 г. были рекомендованы следующие основные алгоритмы [77]:

[10] URL:https://www.iso.org/ru/standard/73771.html?browse=tc

a) Алгоритмы асимметричного шифрования:

1. Classic McEliece – основан на теории кодирования и кодах, исправляющих ошибки и является обобщением крпптосхемы Мак-Элис, предложенной в 1979 году и криптосхемы Нидеррайтера, предложенной в 1984 году, которые и хорошо изучены. Показано, что при использовании кодов Гоппы обе схемы остаются стойкими к различным, в том числе квантовым атакам. Classic McEliece обладает малыми размерами шифротекстов, но большим размером ключа. Рекомендуется к использованию для решения ряда специфических задач.
2. CRYSTALS-Kyber – основан на теории решеток. Криптоанализ сводится к решению задачи Module-LWE. Для обеспечения стойкости к атакам с адаптивно подобранными шифротекстами используется преобразование Фуджисаки – Окомото. Имеет хорошую производительность и безопасность, но по мнению NIST Module-LWE еще малоизученная проблема и требует более детального криптоанализа.
3. NTRU – основан на теории решеток. За основу взята схема NTRUEncrypt, предложенная более 20 лет назад. Проблема NTRU, в отличие от Module-LWE (и других модификаций), была хорошо изучена, что является важным фактором.
4. SABER - основан на теории решеток. Криптоанализ сводится к проблеме MLWR (Module-LWE, где вместо сложения с вектором ошибки – округление по меньшему модулю). Используется преобразование Фуджисаки – Окамото, как и в CRYSTALS - Kyber.

b) Алгоритмы цифровой подписи [77]:

1. CRYSTALS - Dilithium – основан на теории решеток. За основу взят протокол Фиата-Шамира с прерываниями. Криптоанализ сводится к решению задач Module-LWE и Module-SIS. Имеет хорошую

производительность и может быть эффективно реализован на малоресурсных устройствах.

2. FALCON – основан на теории решеток. За основу взят фреймворк GPV- Криптоанализ сводится к задаче SIS на NTRU-решетках. Главным недостатком этой схемы является сложная программная и аппаратная реализация. Схема использует вычисления над числами с плавающей запятой что сильно усложняет анализ стойкости к атакам по сторонним каналам и делает трудной реализацию для малоресурсных устройства.

3. Rainbow – основан на мультивариативных преобразованиях. За основу взят схема UOV. Главным преимуществом является размер цифровой подписи. Но из-за большого размера ключа эту схему рекомендуется использовать только для специфических задач, где размер ключей некритичен.

Кроме того, отобрано восемь альтернативных схем, которые основываются не только на кодах, исправляющих ошибки или целочисленных решетках, а используют преобразования на многочленах от многих переменных; криптографических хэш-функциях; изогениях суперсингулярных эллиптических кривых и другие.

В России перспективное направление постквантовой криптографии сопровождает Технический комитет 26 по стандартизации «Криптографическая защита информации» (ТК26) и рабочая группа РТ 2.5 «постквантовые криптографические механизмы» [78]. В ТК 26 разработаны методические рекомендации для стандарта постквантовой электронной подписи [76].

В квантов-устойчивом блокчейне необходимо использовать [73-75]:

- постквантовые цифровые подписи -для проверки блокчейн-транзакций;
- квантовое распределение ключей;
- квантовые каналы связи;

- оценки стойкости квантовой криптографии (например, алгоритмы Шора, Гровера [81]);
- протокол квантового консенсуса.

К квантовому блокчейну проявляют интерес прежде всего банковский и финансовый секторы. Такие разработки безусловно важны и полезны в общественной сфере в том числе в системах ДЭГ, где информационная безопасность имеет решающее значение [75].

Из сказанного выше можно сделать вывод, что квантовый компьютер безусловно представляет угрозу традиционным криптосистемам с открытым ключом, а следовательно, и информационным системам, где асимметричные криптоалгоритмы используются. Однако, имеющийся задел в построении квантово-устойчивых криптоалгоритмов и их международная стандартизация в ближайшей перспективе дают уверенность в том, что эта проблема будет преодолена и применение квантово-устойчивых криптоалгоритмов в системах ДЭГ обеспечат необходимый уровень информационной безопасности.

2.3. Практические системы ДЭГ

Рассмотрим несколько практических схем ДЭГ, использующих приведенные выше методы.

А) Система Apollo США [80] - система дистанционного электронного голосования, созданная для Массачусетского технологического института (MIT) в 2016 году. Система включает в себя: избирателей, избирательную комиссию (ИК), регистраторов, серверы, центр сбора зашифрованных голосов, центр доверия. В данной системе используется криптосхема Пэйе для генерации ключей (открытый и закрытый ключ), шифрования и дешифрования бюллетеня. Методы доказательства с нулевым разглашением секрета применяются для проверки правильности заполнения избирательного бюллетеня [88] и для проверки корректности расшифровки бюллетеня.

На первом этапе ИК отправляет на сервер списки избирателей и кандидатов. Затем, регистратор делает запрос в центр доверия на генерацию открытого и закрытого ключа. Центр доверия публикует открытый ключ. Далее, начинается процесс голосования. Сначала, избиратель шифрует свой бюллетень с помощью открытого ключа и посылает зашифрованный голос регистратору и центру доверия. Он также отправляет доказательство корректности заполнения своего бюллетеня. Центр доверия убеждается в правильности заполнения бюллетеня избирателем. В случае успешной проверки, голос избирателя засчитывается. Последний этап - подсчет голосов и объявление результатов выборов. ИК сообщает центру доверия через регистратора о завершении голосования. Центр доверия запрашивает центр сбора голосов, который агрегирует зашифрованные голоса и передает результат в центр доверия. Центр доверия расшифровывает криптограммы с помощью закрытого ключа и отправляет результат в избирательную комиссию. Избирательная комиссия публикует результаты выборов на своем веб-сайте. Система обеспечивает анонимность и тайну голосования. Apollo реализован на Python 3.5, как веб-приложение Flask, размещенное на Heroku. Исходный код можно найти по адресу https://github.mit.edu/vmohan/Apollo, а пример выборов, проводимых на платформе Apollo - по адресу https://apollo-voting.herokuapp.com. Для использования сайта требуется действительный сертификат MIT.

В) Система Helios США [81- 83]. Первая доступная реализация системы веб-голосования с открытым аудитом разработана в Гарвардском университете, подходит, например, для выбора членов студенческого совета и для мало масштабных выборов. В этой системе используется сочетание нескольких типов ДЭГ: шифрование бюллетеня, основанное на подходе Бенало [56]; схема Эль Гамаля [36], применяемая для

генерации ключей, шифрования и дешифрования бюллетеня; схема микс-сети [35]), используемая для перемешивания зашифрованных бюллетеней, неинтерактивная схема доказательств с нулевым разглашением секрета [84, 85] для доказательства правильности заполнения избирательного бюллетеня, а также для доказательства корректности дешифровки.

Сначала, сервер генерирует бланк – бюллетень. Далее, избиратель выбирает своего кандидата из значений {0,1} и сервер шифрует выбор избирателя, используя открытый ключ. После этого, сервер посылает все зашифрованные бюллетени в микс-сервер. Микс-сервер маскирует и перемешивает их. Микс-сервер также должен доказать правильность перемешивания бюллетеней.

Helios является веб-приложением, написанным на языке программирования Python, работающее внутри сервера приложений CherryPy 3.0 с веб-сервером Lighttpd. Все данные хранятся в базе данных PostgreSQL. Система обеспечивает анонимность, тайну голосования и проверяемость (возможность избирателя проверить, учтен ли его голос). В [81] представлены результаты оценки времени выполнения операций для этого протокола, количество избирателей составляет 500 (таблица 2.4).

Таблица 2.4. Оценки времени

Операция	Время
Шифрование бюллетеней в браузере (вычисления выполняются по модулю p=1024 бита)	300ms
Перетасовка (на стороне сервера)	133 s
Доказательство перемешивания (на стороне сервера)	3 часа
Расшифровка (на стороне сервера)	71 s
Доказательство расшифровки (на стороне сервера)	210 s
Полный аудит (со стороны избирателя)	4 часа

C) Система Bronco Vote США [62]. Это система ДЭГ с использованием технологии Блокчейн (Ethereum) и смарт-контрактов для американских

университетов. Она использует схему Пэйе [57] для генерации ключей, шифрования и дешифрования бюллетеня. Система включает в себя: администратора, избирателя, портал голосования и сервер. Сначала, избиратель должен пройти регистрацию (используя электронную почту и номер студенческого билета) на сайте регистрации. После этого, данные избирателей отправляются на портал голосования. Портал голосования проверяет данные избирателей и, в случае успешной проверки, ему разрешается проголосовать. Избиратель выбирает своего кандидата, шифрует результат голосования и отправляет его в БЧ. Далее, БЧ агрегирует зашифрованные голоса и отправляет их на сервер для расшифровки. Затем, сервер расшифровывает голоса. Система обеспечивает анонимность, тайну голосования. Система состоит из трех смарт-контрактов, написанных на языке Solidity Ethereum, двух скриптов, написанных на JavaScript, и одной HTML-страницы. Исходный код можно найти по адресу https://goo.gl/nqBpzM.

D) Система Provotum (Швейцария) [87]. Это система ДЭГ с использованием технологии БЧ. Система состоит из: избирателей, провайдера идентификации IdP, ИК, сервера и блокчейна. Она использует схему Эль-Гамаля для генерации ключей, шифрования и дешифрования бюллетеня. Метод доказательства с нулевым разглашением секрета также используется для проверки правильности заполнения избирательного бюллетеня [88] и проверки корректности его расшифровки [90]. В данном протоколе применяется метод разделения данных при распространении закрытого ключа [89].

ИК генерирует свой собственный открытый и закрытый ключи для создания учетной записи в блокчейне и регистрирует свой открытый ключ на сервере. После этого, сервер дает разрешение ИК на доступ к блокчейну. В этом протоколе смарт-контакт рассматривается как бюллетень для голосования. Затем, БЧ формирует общий открытый

ключ для голосования. После чего начинается этап голосования. Избиратель выбирает своего кандидата из значений {0,1}, шифрует свой голос с помощью гомоморфной криптосистемы шифрования и формирует доказательство корректности заполнения бюллетеня и выкладывает их в смарт-контракте.

На основе смарт-контракта БЧ убеждается в корректности заполнении избирательного бюллетеня. В случае успешной проверки, зашифрованный голос сохраняется в БЧ. После окончания голосования осуществляется подсчет голосов и объявление результатов. Исходный код можно найти по адресу http://provotum.ch. Система обеспечивает анонимность, тайну голосования и проверяемость (возможность избирателя проверить, учтен ли его голос).

Е) Российская система КриптоВече [92]. Платформа для проведения онлайн-голосований, с использованием технологии БЧ. Данная система разработана СПбГУ специально для дистанционных голосований. Она позволяет участникам проголосовать дистанционно и гарантирует легитимность их голосов. Система обеспечивает анонимность, тайну голосования, точность и автоматический прозрачный подсчет результатов. Использование технологии БЧ делает процесс голосования прозрачным и повышает доверие к его результатам. Система поддерживает 4 типа пользователей [92]:

- Секретарь;
- Голосующий;
- Наблюдатель;
- Член счетной комиссии.

Система представлена двумя основными пользовательскими приложениями:

- Панель администратора/наблюдателя/члена счетной комиссии - эта часть системы служит для управления всем, что связано с

пользователями, голосованием и организациями. Для доступа к ней нужно обладать особыми правами;

- Панель пользователя-голосующего - эта часть отвечает за процесс волеизъявления, с ее помощью пользователь может оставить свой голос по повестке. Для доступа особых прав не нужно.
- Панель голосующего обеспечивает возможность входа в систему для пользователей – голосующих.

Сначала, голосующий должен отправить в администрацию системы заявку о том, что он хочет участвовать в выборах. Далее, для регистрации избиратель может перейти по ссылке, содержащейся в письме-приглашении от администратора. Для входа в систему, голосующий должен ввести адрес электронной почты, на который пришло письмо, и созданный пароль, а затем нажать кнопку "Войти" или войти в систему через ЕСИА (Единая система идентификации и аутентификации). После этого, произойдет автоматическое перенаправление обратно в систему голосования, а голосующий будет считаться авторизованным. Затем, голосующий создает новое голосование и выбирает его параметры. По окончанию голосования голосующий может увидеть количество зарегистрированных на голосование, узнать явку и посмотреть распределение голосов.

Отметим, что в описании системы не указаны используемые криптоалгоритмы.

Система интересна с точки зрения практической организации выборов с учетом множества возможных вариантов, а именно интерфейсы разработаны в деталях и голосующий может проголосовать не только на ПК, но и с помощью смартфона.

F) Система ДЭГ России [93]. Система разработана на основе криптосистемы с открытым ключом по заказу ЦИК при поддержке Министерства цифрового развития РФ, реализована на базе блокчейн-платформы [91].

Участники протокола:

- Избиратель. Гражданин Российской Федерации подает заявление в электронной форме для участия в ДЭГ, включенный в списки участников ДЭГ.
- Организатор (Комиссия ДЭГ). Организует процесс ДЭГ. Генерирует ключевую пару и разделяет ключ шифрования бюллетеня. Подсчитывает голоса избирателей.
- Наблюдатель. Наблюдение за процессом голосования и аудит результатов голосования.
- Регистратор. Функции: составление списка участников ДЭГ, идентификации и аутентификации пользователей с помощью ЕСИА; поддержка портала ДЭГ, предоставляющего участникам ДЭГ право получения бюллетеня путем использования подписи вслепую.
- Избирательный ящик - сервис анонимного волеизъявления, выдающий участникам бюллетень и принимающий обратно зашифрованный бюллетень.
- Счетчик - Блокчейн - участник, представляющий собой хранилище транзакций (бюллетеней участников ДЭГ и других данных) и осуществляющий подсчет итогов, к которому есть постоянный доступ на запись и/или чтение у участников протокола, а также у избирательных комиссий, организующих выборы (определяющих результаты выборов на территории), которые проводят подготовку исходных данных в ГАС «Выборы» (текст бюллетеня, форма протокола) для передачи Организатору.

  Организатор голосования (Комиссия ДЭГ) и БЧ генерируют ключевые пары (ключи шифрования и расшифрования бюллетеней). На БЧ формируется итоговый открытый ключ шифрования, который передается Регистратору и избирателю. Закрытый ключ разделяется

на доли. Избиратель генерирует ключевую пару электронной подписи. Избиратель и Регистратор выполняют протокол формирования подписи вслепую для ключа проверки электронной подписи избирателя. Избиратель заполняет бюллетень из значений 1 – «за» и 0 – «против», шифрует их с помощью ключа шифрования бюллетеней, формирует доказательство корректности содержимого бюллетеня, состоящее в том, что его выбор соответствует либо 0, либо 1. Также формируется доказательство корректности заполнения бюллетеня в целом.

В системе используются следующие криптографические методы: схема слепой подписи, основанная на RSA [39]; схема Эль Гамаля на эллиптических кривых для генерации ключа, шифрования и дешифрования бюллетеня [95 - 97]; схема Шамира [94] для разделения ключа дешифрования; схемы доказательства корректности заполнения избирательного бюллетеня [88, 98, 106]; схема обязательств (commitment) и Waves enterprise блокчейн [99].

Подводя итог вышеперечисленным практическим системам ДЭГ, рассмотрим криптографические методы, используемые в этих системах (таблица 2.5).

Таблица 2.5. Криптографические методы

Системы	Криптографические методы
Apollo (США)	Гомоморфное шифрование (схема Пэйе)
Helios (США)	Микс-сети и гомоморфное шифрование (Эль-Гамаля)
Bronco Vote (США)	Гомоморфное шифрование
Provotum (Швейцария)	Гомоморфное шифрование
КриптоВече (Россия)	Блокчейн
ДЭГ (Россия)	Блокчейн. Гомоморфное шифрование (Эль-Гамаля на эллиптической кривой), слепая подпись на основе RSA

Таким образом, из таблицы 2.5 следует, что современные практически реализованные системы ДЭГ используют гомоморфное шифрование и технологию блокчейн.

Исходя из приведенного выше анализа можно сделать вывод, что перспективную систему ДЭГ Ирака (арабских государств) целесообразно строить на основе гомоморфного шифрования и технологии БЧ [70], принимая во внимание особенности избирательного процесса в этих государствах и угрозы безопасности избирательной системы, которые частично обсуждались в главе 1. Рассмотрим эти особенности и угрозы более подробно.

2.4 Анализ особенностей избирательного процесса и угроз при построении системы ДЭГ для республики Ирак и арабских государств и определение основных требований информационной безопасности

1. Основной особенностью избирательного процесса является сильное влияние субъективного (человеческого) фактора, которое выражается в следующем:

- Нарушение членами избирательных комиссий инструкций по порядку подготовки и проведения голосования;
- Влияние на действия членов избирательных комиссий заинтересованных лиц и организаций (в том числе подкуп);
- Влияние на избирателей путем использования религиозного (исламского) фактора;
- Влияние мнения старейшин на выбор избирателей;
- Особенности менталитета избирателей, осознающих свою идентичность, как части арабского мира. которая подчеркивает цивилизационное единство, общую историю, языковое и культурное родство.

2. Применение кибер-атак на инфраструктуру системы ДЭГ. (При традиционном бумажном голосовании аналогом такой атаки были случаи кражи избирательных ящиков).
3. Влияние политической системы арабских стран, проявляющейся в низкой роли партий в общественно-политической жизни, что

обусловлено особенностями социальной структуры традиционного общества.

4. Необходимость приема традиционно большого количества избирателей, в том числе находящихся за границей;

Наиболее опасными угрозами для системы дистанционного электронного голосования, которые разрабатываемая модель должна предотвращать или блокировать, на наш взгляд, являются:

1. Со стороны посторонних лиц:
   - Нарушение тайны голосования;
   - Нарушение анонимности;
   - Вброс голосов;
   - Голосование за лиц, не пришедших на выборы.
2. Со стороны избирателя:
   - Неправильное заполнение бюллетеня;
   - Повторное голосование.
3. Со стороны избирательной комиссии:
   - Нарушение тайны голосования;
   - Нарушение анонимности, в том числе после окончания выборов;
   - Вброс голосов;
   - Получение информации о результатах выборов до окончания голосования.

Рассмотрим детально угрозу потенциального влияния субъективного фактора на результаты голосования через администрацию системы ДЭГ. Возможность реализации такой угрозы объясняется тем, что администрация владеет закрытым ключом. Есть способ блокировать эту угрозу, когда закрытый ключ делится на доли, которые распределяются между доверенными участниками системы голосования [5]. Однако, такое разделение полностью не решает проблему ограничения влияния административного ресурса на результаты голосования. Во-первых, нет гарантии, что ИК не предоставит части

закрытого ключа полностью независимым участникам выборов. Во-вторых, уже после голосования, когда ключ расшифрования восстановлен из долей, ИК может сделать копию этого ключа и, имея этот ключ, ИК может осуществить атаку, связанную с нарушением анонимности отдельно отслеживаемых избирателей. Рассмотрим подробно организацию такой атаки.

Предположим, что нарушитель следит за работой отдельного (приоритетного) избирателя и может подключиться к выходу компьютера, на котором осуществляется голосование. Тогда, не зависимо от того использовалась ли слепая подпись или анонимный канал, нарушитель знает, что передается зашифрованный бюллетень от данного избирателя. Далее, используя ключ расшифрования, нарушитель (уже после выборов) расшифровывает бюллетень. Это не влияет на результат голосования и подсчет голосов, однако анонимность избирателя может быть нарушена.

В разрабатываемой модели эта уязвимость предотвращается тем, что мы используем принцип шифрования единым для всех избирателей открытым ключом, а ключ расшифрования является изначально распределенным по нескольким независимым объектам [5, 100].

Другими словами, наша модель основана на гомоморфном шифровании с распределенным дешифрованием, и отличается от существующих систем тем, что предполагает наличие нескольких серверов, каждый из которых генерирует свои собственные открытый и закрытый ключи. Затем формируется общий открытый ключ, который передается всем голосующим. Расшифровка осуществляется частично каждым сервером, поэтому общий ключа расшифровки в полном объеме не формируется, что защищает от возможной атаки со стороны системной администрации. Предполагается, что серверы независимы от ИК, например, они принадлежат разным партиям, участвующих в выборах [100].

С учетом проведенного анализа можно сформулировать следующие требования к безопасности информации, разрабатываемой системы ДЭГ и путях их достижения [5, 10, 11]:

- Тайна голосования. Обеспечивается за счет шифрования бюллетеня по криптосхеме с открытым ключом, которая при выборе соответствующих параметров является вычислительно стойкой. За счет разделения ключей расшифрования никто не может узнать результаты текущего голосования до закрытия процедуры голосования.
- Анонимность избирателя. Достигается за счет использования гомоморфного свойства используемой криптосистемы. В этом случае осуществляется расшифрование агрегированных голосов. После расшифрования становится известной сумма голосов, поданных за кандидата, но никто не может узнать, как проголосовал отдельный избиратель. Кроме того, обеспечивается дополнительное усиление анонимности избирателя при атаках со стороны административного ресурса.
- Аутентификация избирателя. Осуществляется путем подтверждения учетной записи избирателя, имя которого заранее включено в список избирателей. Сервер идентификации и аутентификации сверяет данные избирателя, полученные от избирательной комиссии, с данными избирателя, отправленными с сервера регистрации. Если проверка прошла успешно, то ему будет предоставлен доступ к серверу голосования.
- Уникальность. Достигается за счет того, что избиратель может зайти на сайт выборов со своей учетной записью только один раз. Если он попытается войти в систему снова, ему будет сообщено, что он уже проголосовал, тогда он не сможет проголосовать более одного раза.
- Подтверждение голосования. Достигается за счет того, что избиратели получают сообщение о том, что их голос был учтен и принят системой правильно.
- Точность голосования. Достигается за счет проверки корректности заполнения бюллетеня.

2.5. Разработка модели перспективной системы ДЭГ в республике Ирак (арабских государствах) с учетом условий и особенностей избирательного процесса

Обобщая сказанное выше и учитывая особенности избирательного процесса в республике Ирак и арабских государствах, предлагается в основу построения системы ДЭГ положить следующую модель (рис. 2.5).

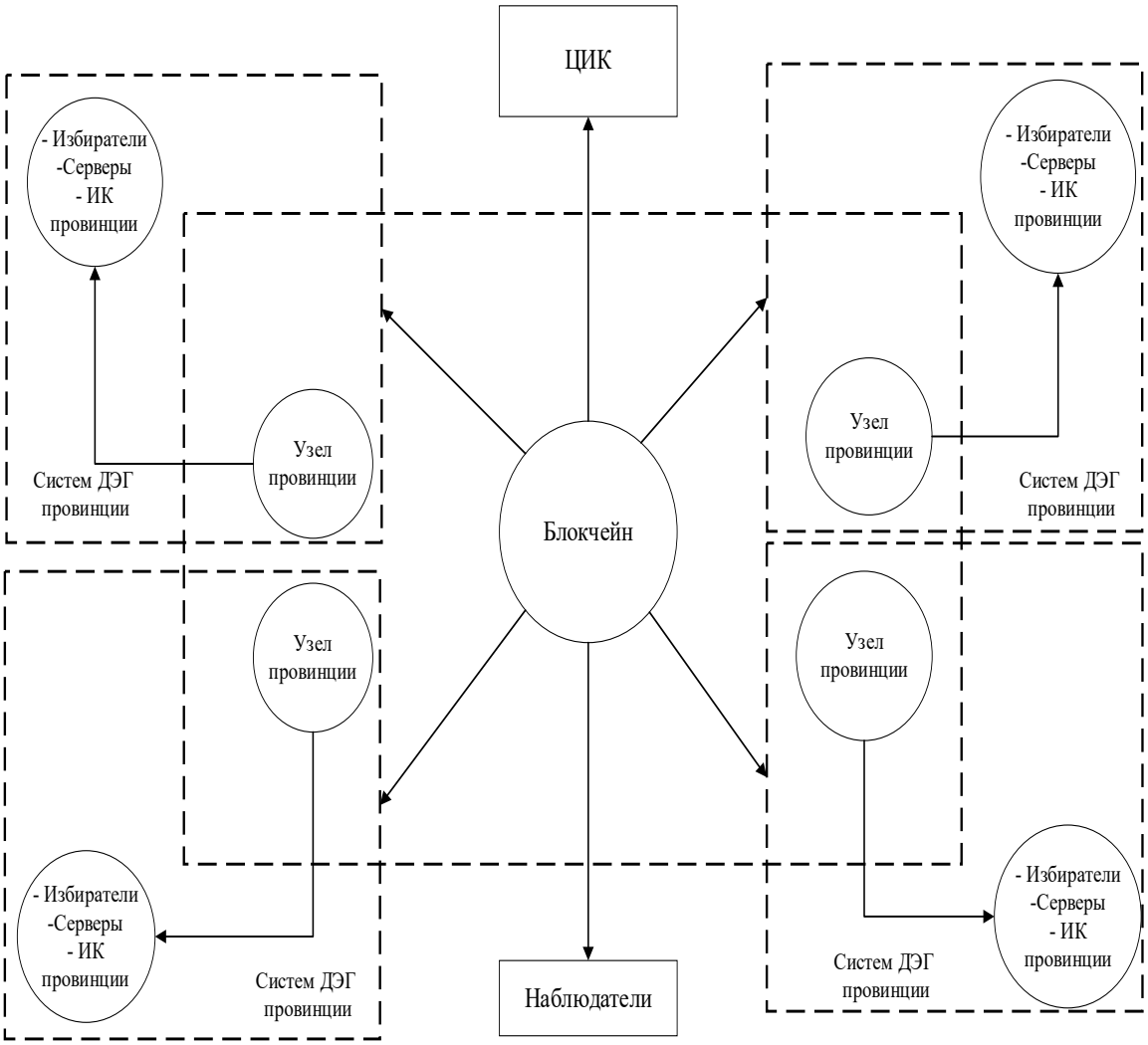

Рис.2.5. Общая перспективная схема ДЭГ для республики Ирак

Систему ДЭГ республики Ирак предлагается создавать в виде объединения подсистем ДЭГ 18 провинций. Технологически такое объединение выполняется по принципу блокчейн- консорциума с использованием смарт-контрактов.

Блокчейн-консорциум представляет собой блокчейн, управляемый несколькими предопределенными участниками или "членами консорциума". В отличие от общедоступных блокчейнов, таких как, например, биткоин, блокчейн-консорциум обеспечивает больший контроль над уровнем доступа и конфиденциальностью. Также блокчейн-консорциум может разрабатывать общие стандарты и протоколы для использования в блокчейн-сети. Это важно для обеспечения совместимости между различными системами и приложениями, использующими эту сеть. Работа блокчейн-консорциума направлена на создание устойчивой и эффективной блокчейн-сети, способной удовлетворять потребности и цели участвующих в ней организаций [70].

Мы выбрали этот тип блокчейна (блокчейн-консорциум), потому что он больше подходит для нашей модели и достижения целей.

В каждой провинции создается узел голосования провинции, на который замыкаются избирательные участки и округа провинций. В таблице 2.6 представлено количество избирательных участков и округов в Республике Ирак по данным выборов 2021 года [5].

Таблица 2.6. Количество избирательных участков и округов в Республике Ирак [5]

Провинция	Количество Избират. Участков	Количество избирателбных округов	Провинция	Колич. Избират. участок	Колич. Избират. Округов примерно
Багдад	17	1000	Эль-мутанна	2	200
Эль-Анбар	4	350	Эль-кут	3	304
Каркук	3	300	Эль-дивания	3	300
Мосул	8	700	Карблаа	3	240
Эль-сулимания	5	500	Эль-Наджаф	3	303
Эль-басра	6	514	Дияла	4	500
Эль-насерия	5	400	Салах Эль-ден	3	310
Майссан	3	250	Духок	3	200
Вавилон	4	407	Ирбил	4	500

Система ДЭГ провинции строится на основе распределенной сети узлов блокчейна (Рис. 2.5). Узел голосования провинции включает в себя серверную

платформу, состоящую из сервера регистрации; сервера аутентификации; нескольких серверов голосования ведущих партий. К нему подключаются узлы блокчейна провинции [5].

Как описано в первой главе п.1.1. по всей территории республики Ирак устанавливается 83 избирательных участка в 18 провинциях республики. Каждый избирательный участок состоит из нескольких местных избирательных округов, где каждый избирательный округ обслуживает примерно 450 избирателей.

Исходя из этого, можно определить количество основных узлов в БЧ - 83 и запасных узлов - 9 (10% от количества основных узлов). Максимальное количество местных избирательных округов составляет не более 1000. Взаимодействие ИКП и избирательных участков в провинции предлагается осуществляет с использованием смарт-контрактов. Их количество определяется количеством избирательных участков в провинции. В смарт-контрактах хранятся зашифрованные голоса избирателей избирательного участка, что гарантирует полноту подсчета голосов, сокращает время подсчета голосов и снижает нагрузку на блокчейн-сеть.

Смарт-контракты — это программы, которые автоматизируют и исполняют условия соглашения без участия третьих сторон. Они выполняются на блокчейне и обеспечивают доверие между сторонами. Для обеспечения безопасности смарт-контрактов используется криптографические методы [69]. Создание блокчейн-консорциума с использованием смарт-контракта для дистанционного электронного голосования представляет собой инновационное решение, которое может улучшить прозрачность и безопасность процесса голосования.

При создании блокчейн-консорциума в системе дистанционного электронного голосования следует учитывать следующее [70]:

1. При выборе участников консорциума сформировать группу участников, которые будут активно работать в консорциуме. Это могут быть представители правительственных органов,

технологических компаний, академических учреждений и других заинтересованных сторон.

2. При выборе технологии блокчейн: решить, какую блокчейн-технологию использовать. Наиболее популярными в настоящее время являются Ethereum, Hyperledger Fabric, Corda и некоторые доугие.
3. Смарт-контракты следует разработать с ориентацией подсчета голосов. Эти смарт-контракты должны обеспечивать безопасность, своевременность и надежность.
4. Предоставить ресурсы и возможность обучения участников консорциума, чтобы они могли эффективно использовать систему.

Участники системы ДЭГ в провинции

Пользователи ДЭГ [5]:

- Избиратель - гражданин Ирака, который имеет биометрическую карту и включен в списки избирателей ДЭГ. Он должен зарегистрироваться на сайте электронной регистрации до дня голосования.
- Избирательная комиссия провинции (ИКП) — независимый коллегиальный орган, формируемый в соответствии с избирательным законодательством, организующий и обеспечивающий подготовку и проведение выборов различного уровня, в том числе выдвижение и регистрацию кандидатов и политических партий (из списков кандидатов). Она подготавливает список избирателей и организует процесс ДЭГ.
- Наблюдатель – участник, осуществляющий наблюдение за процессом голосования и аудит результатов голосования.

Компоненты системы ДЭГ:

- Серверы голосования партий (Серверы голосования) - выделенные или специализированные компьютеры для генерации пары ключей (открытый и закрытый ключ) и управления процессом голосования на провинциальном уровне. С помощью этих серверов осуществляется

распределенное дешифрование бюллетеней избирателей. Предполагается, что серверы принадлежат разным партиям, имеющими установленную квоту в парламенте. Количество серверов для голосования в каждой провинции составляет 4-5, один сервер для ИКП, а остальные - для основных партий.

- Электронный бюллетень – избирательный бюллетень, для голосования на выборах. Бюллетень в электронном виде представляет собой строку символов (1,0), где 1 - голос «ЗА» и (0) – голос «ПРОТИВ», подаваемые за каждого кандидата. В зависимости от правил выборов могут быть различные варианты голосования. Например, на парламентских выборах в республике Ирак избиратель должен проголосовать только за одного кандидата.
- Сервер регистрации – отвечающий за регистрацию избирателей в электронной форме. Чтобы иметь возможность участвовать в электронных выборах, избиратели до дня голосования должны зарегистрироваться онлайн на веб-сайте электронной регистрации посредством создания учетной записи. ИК провинции отправляет список избирателей на сервер регистрации.
- Сервер идентификации и аутентификации – осуществляющий идентификацию и аутентификацию избирателей.
- Узел блокчейн провинции – участник, представляющий собой хранилище транзакций. В нашей системе будет применяться блокчейн-консорциум. Каждая провинция имеет свой собственный узел на блокчейн-консорциум, содержащий информацию о голосовании на избирательных участках и округах для данной провинции.

Следует отметить, что структура модели перспективной иракской системы голосования сохраняет преемственность с традиционной структурой, используемой на выборах в Ираке, которая подходит для парламентских выборов в арабских странах.

Далее, рассмотрим функционирование системы ДЭГ на провинциальном уровне (см. рисунок 2.6).

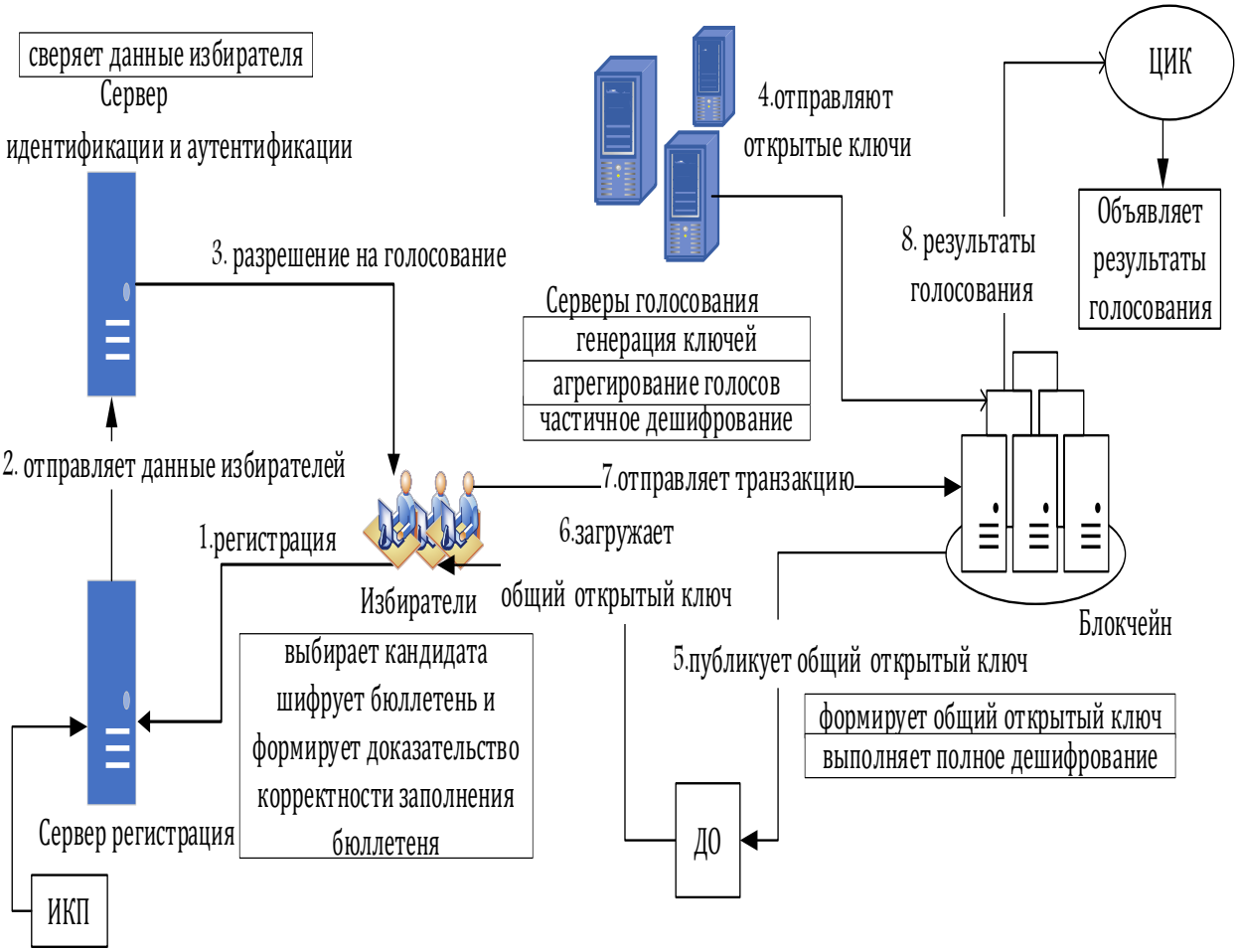

Рис. 2.6. Структура системы ДЭГ провинции

Описание работы схемы

Отметим, что в нашей модели используется схема Эль-Гамаля для генерации ключей, шифрования и дешифрования бюллетеня.

1) Избиратель, желающий принять участие в выборах, должен зарегистрироваться на веб-сайте регистрации.
2) После завершения процесса регистрации сервер передает данные избирателей на сервер идентификации и аутентификации.

3) Процесс проверки данных избирателей начинается на сервере. Если проверка проходит успешно, то избиратель получает доступ к голосованию.
4) Серверы голосования отправляют свои открытые ключи в блокчейн для формирования общего открытого ключа.
5) БЧ публикует общий открытый ключ на доске объявлений.
6) Избиратель загружает общий открытый ключ с ДО. Затем, шифрует свой выбор с помощью общего открытого ключа и формирует доказательство корректности заполнения бюллетеня.
7) Он отправляет зашифрованный бюллетень и доказательство в БЧ.
8) После завершения голосования, БЧ отправляет первую часть криптограмм на сервер голосования, который выполняет частичную расшифровку всех криптограмм, используя свойство аддитивного гомоморфного шифрования. Затем, серверы отправляют результаты частично расшифрованных бюллетеней в блокчейн. Полная расшифровка с использованием вторых частей криптограммы осуществляется на БЧ. Он отправляет результат расшифровки в ИКП, которая передает результат голосования в ЦИК.
9) ЦИК объявляет результаты голосования.

Детальное описание функционирование системы ДЭГ будет приведено в следующей главе при рассмотрении протокола ДЭГ.

2.6. Определение характеристик блокчейн, используемого в предлагаемой модели

В данном разделе определяются характеристики БЧ в предлагаемой модели. Как было отмечено ранее (см. п.2.3), существуют различные типы БЧ, которые могут быть применены в разных информационных системах.

В нашей модели предлагается использовать блокчейн–консорциум с использованием смарт-контрактов, а именно Hyperledger Fabric (HF)). HF — это блокчейн-фреймворк с открытым исходным кодом, разработанный Linux Foundation и предназначенный для корпоративного использования, направленного на обеспечение эффективных и безопасных транзакций между участвующими сторонами [79].

HF включают в себя [79]:

- Сеть разрешений. HF позволяет организациям контролировать доступ и участие в сети, обеспечивая конфиденциальность. Участники должны пройти аутентификацию перед доступом к блокчейну.
- Каналы. HF поддерживает создание нескольких каналов внутри сети, позволяя множествам участников проводить частные и конфиденциальные транзакции.
- Смарт-контракты. HF предоставляет программную модель для построения смарт-контрактов, известную как "цепной код". Цепной код может быть написан на различных языках программирования, что позволяет разработчикам использовать свои существующие навыки и инструменты.
- Модульность. Архитектура HF является модульной, что позволяет организациям выбирать компоненты, соответствующие их требованиям. Она предоставляет подключаемые согласованные протоколы, позволяющие организациям выбирать алгоритм, который наилучшим образом соответствует их потребностям в безопасности и производительности.
- Производительность и масштабируемость. HF разработан для поддержки высокой пропускной способности и эффективности транзакций. Это достигается за счет использования параллельного выполнения смарт-контрактов, что позволяет обрабатывать несколько транзакций одновременно.

- Конфиденциальность. HF предоставляет функции конфиденциальности, такие как приватные транзакции и каналы, которые позволяют участникам безопасно совершать транзакции, сводя к минимуму объем данных, передаваемых в сеть.
- В блокчейн используется алгоритм консенсуса - доказательство власти (Proof-of-Authority (PoA)) — который полагается на заранее определенные доверенные органы или валидаторы для установления легитимности и авторитетности транзакций в сети БЧ. Предоставляя доказательства своих полномочий, валидаторы могут обеспечить целостность и безопасность сети, одновременно ускоряя время подтверждения транзакций. Основная идея PoA заключается в гарантии того, что валидаторы заинтересованы в поддержании целостности и безопасности сети. Это достигается путем требования от них предоставить ту или иную форму подтверждения своих полномочий, например, быть доверенным лицом, занимать определенную должность в компании или организации, быть известным физическим лицом или иметь определенный уровень репутации в сети [61, 68].
- Скорость обработки транзакций от 1000 до 2000 транзакций в секунду.

В таблице 2.7 приведены количественные параметры предлагаемой модели ДЭГ.

Таблица 2.7. Количественные параметры предлагаемой модели

Параметры	Количество
Избиратели на уровне местных избирательных округов	Не более 450
Узел сети	83 узлов в 18 провинциях республики Количество узлов в каждой провинции соответствует количеству избирательных участков.
Серверы на уровне провинции	По 4-5 серверов в каждой провинции. Один для ИКП, а остальные для основных партий.

Выводы по 2-й главе

1. Проанализированы принципы построения современных систем дистанционного электронного голосования (ДЭГ), на основе микс-сетей, слепой подписи, гомоморфного шифрования и блокчейн. Проведено их сравнение. Результаты анализа показывают, что гомоморфное шифрование обладает рядом преимуществ и поэтому эта схема взята за основу в предлагаемой модели системы ДЭГ для обеспечения безопасности избирательного процесса.
2. Выполнен анализ практических систем ДЭГ в разных странах. Сделан вывод о том, что рассматриваемые системы зачастую либо не обеспечивают анонимность избирателя, либо представляют из себя коммерческий продукт без полного и открытого описания принципа работы системы, что приводит к недоверию к результатам со стороны участников голосования. Система ДЭГ должна обладать полностью понятными принципами работы, обеспечивать выполнение требований законодательства, учитывать реальные угрозы и особенности избирательного процесса в стране применения. В результате можно сделать вывод, что разработка надежных систем ДЭГ являются предметом интереса многих стран.
3. Разработана модель системы дистанционного электронного голосования (ДЭГ) для арабских государств с парламентской правовой системой, основанная на распределенной сети блокчейн-узлов, объединяющей подсистемы ДЭГ провинций, построенные по принципу блокчейн–консорциума с использованием смарт-контрактов, в которых хранятся зашифрованные голоса избирателей избирательного участка хранятся на узле голосования провинции с использованием смарт-контрактов, что гарантирует полноту подсчета голосов, сокращает время подсчета голосов и снижает нагрузку на блокчейн-сеть.

4. Определены характеристики блокчейн, используемого в предлагаемой модели. Выбранный тип БЧ соответствует структуре традиционной системы голосования в Республике Ирак и арабских государствах с парламентской правовой системой.

ГЛАВА 3. РАЗРАБОТКА ПРОТОКОЛА ФУНКЦИОНИРОВАНИЯ ПЕРСПЕКТИВНОЙ СИСТЕМЫ ДЭГ НА ОСНОВЕ ГОМОМОРФНОГО ШИФРОВАНИЯ С РАСПРЕДЕЛЕННЫМ ДЕШИФРОВАНИЕМ

3.1. Обоснование выбора криптосистемы гомоморфного шифрования для протокола голосования в перспективной системе ДЭГ республики Ирак

В предыдущей главе был сделан вывод, что в перспективной системе ДЭГ целесообразно использовать гомоморфное шифрование с распределенным дешифрованием в сочетании с технологией блокчейн. Однако само гомоморфное шифрование может быть выполнено с использованием разных криптосхем. Наиболее распространенными и часто применяемыми в системах ДЭГ являются криптосхемы Эль-Гамаля [36], Бенало [56], Пэйе [57].

Схема Эль-Гамаля была подробно рассмотрена в предыдущей главе в целях конкретизации описания принципов построения систем ДЭГ на основе микс-сетей, слепой подписи и гомоморфного шифрования.

В данном параграфе, проанализируем еще два типа гомоморфных схем шифрования (Бенало и Пэйе), так как они также являются часто используемыми гомоморфными криптосистемами [48].

В приложении № 3, приведены примеры построения систем Бенало и Пэйе, а также систем ДЭГ, использующих их гомоморфные свойства.

3.1.1 Криптосхема Бенало

В 1994 году Джош Бенало [56], предложил гомоморфную схему шифрования, которая является вероятностным асимметричным алгоритмом для криптографии с открытым ключом.

Генерирование ключей [48]*:*

1. Выбираются два больших простых числа p, q и размер блока сообщения r. (r-максимальное значение сообщения, представленного в виде числа). Число r выбирается таким образом, чтобы выполнялись условия:

$$(p-1) mod\, r = 0,\ \gcd\left(r, \left(\frac{p-1}{r}\right)\right) = 1,\ \gcd(r, q-1) = 1. \quad (3.1)$$

2. Вычисляется $n = pq$. (3.2)
3. Выбирается $y \in Z_n^*$, так, чтобы $y^{\varphi/r} \neq 1\ mod\ n$, где $\varphi()$- функция Эйлера от n. $\varphi(n) = (p-1)(q-1)$.
4. Вычисляется $x = y^{\varphi/r}\ mod\ n$. (3.3)

Тогда полагаем: (y, r, n)- открытый ключ, (φ, x)- закрытый ключ.

Шифрование сообщения:

Пусть сообщение $m \in Z_r$:

1. Выбирается произвольное число $u \in Z_n^*$,
2. Вычисляется криптограмма $c = y^m u^r\ mod\ n$. (3.4)

Расшифровывание криптограммы:

Получена криптограмма $c \in Z_n^*$:

1. Вычисляется $a = c^{\varphi/r}\ mod\ n$ (3.5)
2. Подбирается число *m* такое, что $m = \log_x a$. (3.6)

Действительно, для любых $m \in Z_r, u \in Z_n^*$, можно записать

$$a = (c)^{\varphi/r} \equiv (y^m u^r)^{\varphi/r} \equiv (y^m)^{\varphi/r}(u^r)^{\varphi/r} \equiv \left(y^{\varphi/r}\right)^m (u)^{\varphi} \equiv (x)^m (u)^0 \equiv x^m mod\ n$$

Криптосистема Бенало гомоморфное относительно операции сложения открытых тестов [56, 48]:

$$Enc(x_1) \times Enc(x_2) = (g^{x_1} u_1^r)(g^{x_2} u_2^r) = g^{x_1+x_2}(u_1 u_2)^r = Enc(x_1 + x_2) mod\ p,$$

где $Enc(x)$ является функцией шифрования от сообщения *x*.

3.1.2 Криптосхема Пэйе

Криптосхема Паскаля Пэйе [57], является вероятностным асимметричным алгоритмом для криптографии с открытым ключом. Она

основана на задаче вычисления n-го класса вычетов, которая считается трудновыполнимой [48].

Генерирование ключей:

1. Выбираются два больших простых числа p и q, удовлетворяющие условию $\gcd\big(pq,(p-1)(q-1)\big)=1$.
2. Вычисляются $n=pq$ и $\lambda=\mathrm{lcm}(p-1,q-1)$. (3.7)

где $\lambda(n)$- функция Кармайкла от n. $\lambda=\frac{(p-1)(q-1)}{\gcd(p-1,q-1)}$, (lcm-наименьшее общее кратное).

3. Выбирается $y, y\in Z_{n^2}^{*}$;
4. Вычисляется $x=\Big(L\big(y^{\lambda}\ mod\ n^2\big)\Big)^{-1}\ mod\ n$, где $L(u)=\left[\frac{u-1}{n}\right]$. (3.8)

Тогда полагаем (y,n) - открытый ключ, (λ,x) - закрытый ключ.

Шифрование сообщения:

Пусть сообщение $m\in Z_n$:

- Выбирается произвольное число $u\in Z_n^{*}$
- Вычисляется криптограмма $c=y^{m}u^{r}\ mod\ n^2$. (3.9)

Расшифровывание криптограммы:

Получена криптограмма $c\in Z_{n^2}^{*}$:

- Вычисляется $m=L\big(c^{\lambda}\ mod\ n^2\big)\times x\ mod\ n$. (3.10)

Гомоморфные свойства [48]:

1. Произведение двух шифротекстов будет расшифровано как сумма соответствующих их открытых текстов,
   $D\big(E(m_1,r_1)*E(m_2,r_2)\big)\ mod\ n^2=(m_1+m_2)\ mod\ n$.
2. Шифротекст, возведенный в степень, равную другому тексту будет расшифрован как произведение двух открытых текстов,
   $D\big(E(m_1,r_1)^{(m_2)}mod\ n^2\big)=m_1m_2\ mod\ n$.

3.1.3 Сравнение схем гомоморфного шифрования для построения систем ДЭГ

Сравнение криптосистем Эль-Гамаля, Пэйе и Бенало по некоторым свойствам приведено в таблице 3.1.

Таблица 3.1. Сравнение криптосистем Эль-Гамаля, Пэйе и Бенало

Схема / Свойство	Эль-Гамаль	Пэйе	Бенало
Стойкость	Основан на трудной задаче вычисления дискретных логарифмов в конечном поле.	Основана на трудно решаемой задаче о вычетах высокой степени.	Основана на задаче факторизации больших чисел
Удобство использования	Особенностью алгоритма является простота понимания и использования.		
Время выполнения операций	Для дешифрования криптосистема Эль-Гамаля в целом работает значительно быстрее, чем схема Бенало и требует на заключительном этапе решения задачи дискретного логарифмирования.	Для дешифрования криптосистема Пэйе в целом работает значительно быстрее, чем схема Бенало.	Операция дешифрования требует на заключительном этапе решения задачи дискретного логарифмирования для чисел относительно небольшого размера.
Недостатки, различия	- Удвоение длины зашифрованного текста по сравнению с начальным текстом. - Используется модуль n.	- Увеличение размера шифротекста по отношению к входному тексту. - Используется модуль n^2.	- Является более сложной и вычислительно более трудоемкой. - Используется модуль n.
Сходство	Используют шифрование с открытым ключом. Осуществляют рандомизацию шифртекста. Обладают свойством гомоморфизма.		

Сравнительный анализ показал, что между криптосистемами Эль-Гамаля, Пэйе и Бенало существует много общего: используют шифрование с открытым

ключом, обладают свойством гомоморфизма, обеспечивают конфиденциальность и анонимность избирателей. Схема Бенало требует выполнения большего объема математических вычислений при дешифровании криптограммы, что в свою очередь занимает больше времени. Поэтому на практике распространение получила криптосистемы Эль-Гамаль и Пэйе.

Отметим, что схема Пэйе работает с числами большого модуля $n^2 \gg n$.

В таблице 3.2 приведены результаты эксперимента по оценке времени генерации ключа, шифрования и дешифрования бюллетеня для трех криптографических схем.

Таблица 3.2. Сравнение гомоморфных алгоритмов

Схем / Параметры	Эль-Гамаля	Пэйе	Бенало
Время генерации ключа	0.0000274 мс	0.0561540 мс	1.7214342 мс
Время шифрования	0.0000073 мс	0.0157827 мс	0.0001516 мс
Время дешифрования	0.0000051 мс	0.0207673 мс	0.0001238 мс

Как видно из таблицы 3.2, схема Эль-Гамаля требует меньше времени для генерации ключей, шифрования и дешифрования бюллетеня по сравнению с другими рассматриваемыми схемами. Поэтому будем использовать эту схему в разрабатываемом протоколе функционирования системы ДЭГ.

В приложении № 3, приведены примеры построения систем Бенало и Пэйе, а также систем ДЭГ, использующих их гомоморфные свойства.

3.2. Разработка протокола функционирования системы ДЭГ провинции

В предыдущей главе была предложена модель системы ДЭГ, основанная на распределенной сети блокчейн-узлов с использованием смарт-контрактов. Описаны в общем виде основные этапы взаимодействия участников. В данной главе разработаем протокол функционирования перспективной системы ДЭГ на основе гомоморфного шифрования на основе криптосхемы Эль-Гамаля с распределенным дешифрованием, учитывающий специфические угрозы в системе ДЭГ арабских государств, которые были указаны в предыдущей главе

и обеспечивающий повышенную защищенность от угроз, связанных с субъективным (человеческим) фактором.

Предлагаемый протокол голосования включает в себя несколько этапов. Рассмотрим эти этапы поочередно, поясняя взаимодействие участников рисунками, которые могут быть объединены в единую схему. Участники протокола голосования были определены в п.2.5. На рисунке 3.1 представлено взаимодействие участников системы ДЭГ.

Этап инициализации системы. На этом этапе осуществляется генерирование ключей. ИК внедряет смарт-контракт в блокчейне, который выполняет процессы: проверки доказательства заполнения бюллетеня и полную расшифровку. Предполагается, что в системе ДЭГ будет использована криптографическая схема с распределенным ключом дешифрования. Для этого каждый сервер генерирует пару ключей: открытый – h_i и закрытый – s_i. Открытые ключи отправляются к БЧ, где формируется общий ключ голосования h, после этого, БЧ помещает этот ключ на доску объявлений (ДО), где избиратели его получают. Секретные ключи хранятся на серверах. Заметим, что сервера принадлежат разным партиям, что делает маловероятным сговор всех партий сразу [5].

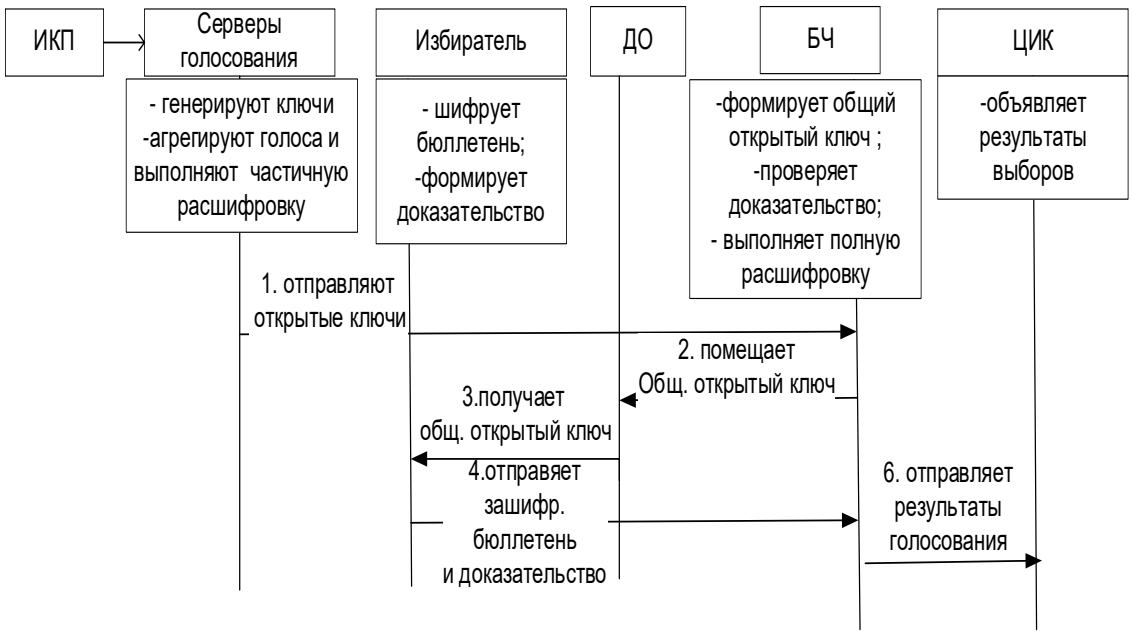

Рис. 3.1. Взаимодействие участники системы ДЭГ на этапе инициализации

Этап регистрация избирателей

Центральная избирательная комиссия Ирака (ЦИК) с 2015 года создает и поддерживает базу биометрических данных избирателей, содержащую отпечатки пальцев, полное имя избирателя, дату рождения и т.д., чтобы эти данные можно было использовать на выборах. Избиратель до дня голосования должен заполнить электронную биометрическую регистрационную форму, предоставить отпечатки пальцев и фотографию.

Для участия в дистанционном голосовании, избиратель, используя ПК (ноутбук, планшет или смартфон) должен зайти на сайт электронной регистрации (сервер регистрации) и зарегистрировать свои данные (полное имя избирателя, провинция и т.д.). Следует отметить, что перед каждыми выборами ИКП обновляет биометрическую базу данных избирателей [5].

Этап идентификации и аутентификации избирателей

Перед днем выборов ИКП передает список избирателей на сервер идентификации и аутентификации по защищенному каналу. Он сверяют данные избирателя, полученные от ИКП, с данными избирателя, отправленными с сервера регистрации. Если проверка прошла успешно, то избирателю будет предоставлен доступ к серверам голосования. На рисунке 3.2 показаны этапы регистрации, идентификации и аутентификации избирателей [5].

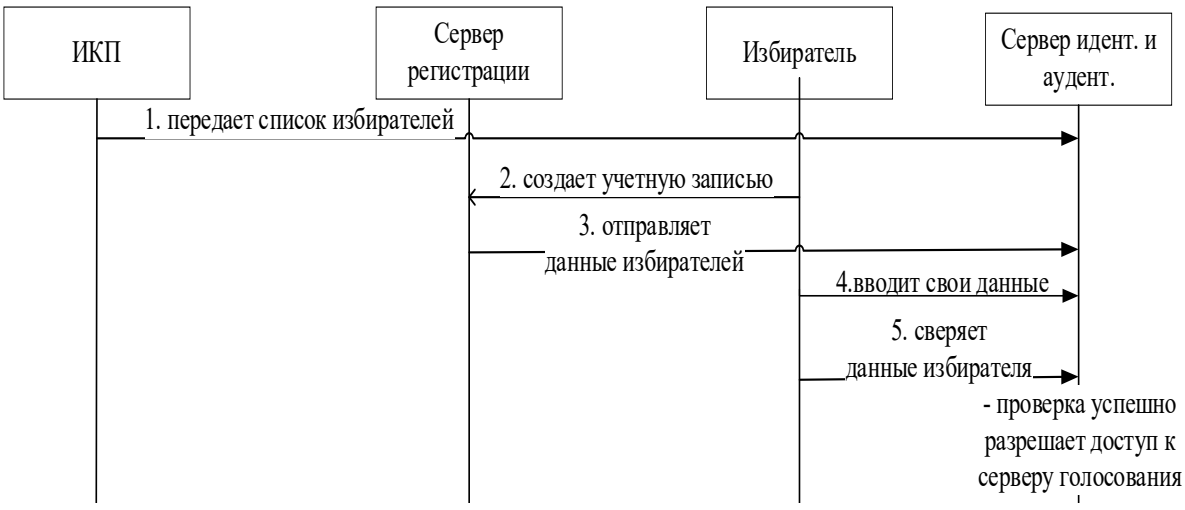

Рис. 3.2. Этапы регистрация, идентификации и аутентификации избирателей

Этап голосования

- Каждый избиратель с помощью программного обеспечения на своем устройстве выбирает кандидата (кандидатов) из списка кандидатов, шифрует свой голос (создает криптограммы (A_i,B_i) и доказательства корректности выполнения операции шифрования). После завершения голосования, избиратели отправляют бюллетени и доказательства корректности их заполнения в БЧ.

Этап расшифровки бюллетеней

БЧ проверяет доказательства и передает первые части криптограмм A_i, на сервера голосования. Они делают предварительную расшифровку своими секретными ключами, агрегируют эти расшифровки и отправляют их в БЧ. В БЧ хранятся вторые части криптограмм B_i и БЧ делает полную расшифровку агрегированных бюллетеней.

Этап подсчет голосов и объявление результатов выборов

Результат расшифрования БЧ передает в ИКП. ИКП направляет их в ЦИК. Она осуществляет окончательный подсчет голосов по всем провинциям и объявляет результаты выборов на сайте выборов [5].

На рисунке 3.3 показан этап голосования и объявление результатов выборов.

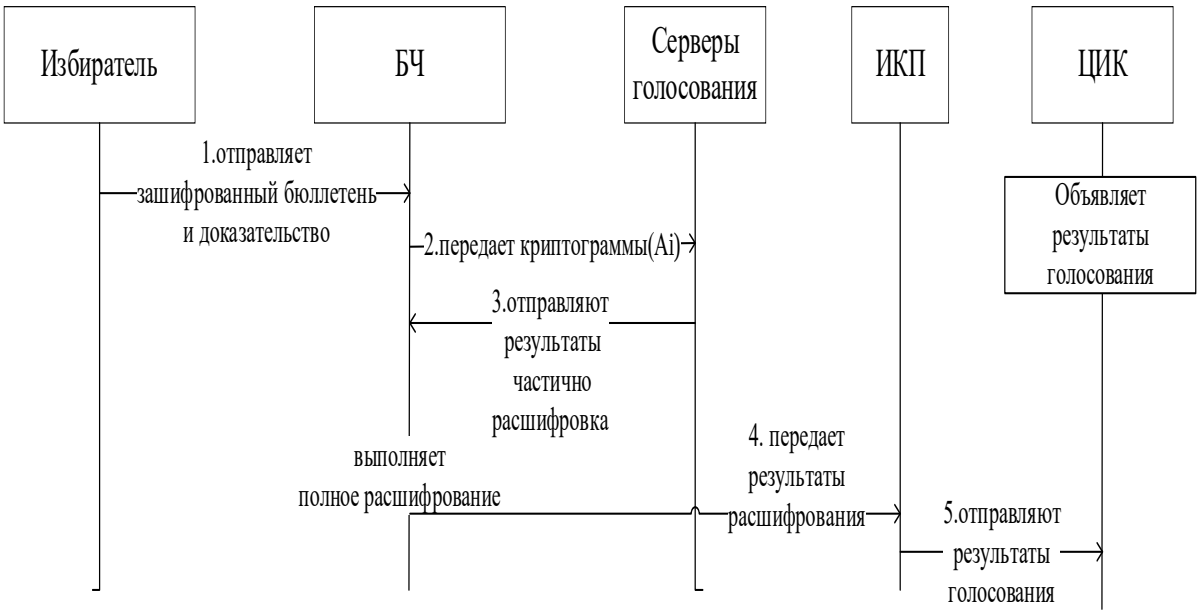

Рис. 3.3. Этап голосования и объявление результатов выборов

В следующем разделе дадим математическое обоснование разработанного протокола.

3.3. Математическая модель, используемая в протоколе ДЭГ, как основа выполнения требований безопасности

В рассматриваемой системе ДЭГ предлагается использовать гомоморфную криптографическую схему ЭГ [36] в поле GF(p) для генерации ключей, шифрования и дешифрования бюллетеней. (Аналогичным образом может быть рассмотрена схема ЭГ на эллиптической кривой [95- 97]). Обе схемы хорошо зарекомендовали себя при построении систем шифрования и электронной подписи [40 - 41].

Генерация ключей:

Шаг 1. Каждый сервер голосования партии (сервер голосования) E_t генерирует секретный ключs_t (случайное число) $1 < s_t < p-1$, затем формируют открытый ключ: $h_t = g^{s_t} \, mod \; p$, (3.11)

где p – простое число, g – примитивный элемент поля Галуа GF(p), $t = 1,2,\ldots,T$, Т-количество серверов.

Сгенерированные открытые ключи h_t передаются в БЧ, закрытые ключи s_t остаются на хранении на серверах до этапа расшифровки бюллетеней [5].

Шаг 2. БЧ формирует общий открытый ключ голосования [5, 100]:

$$h_{\text{общ.}} = g^{s_1} \cdot \; g^{s_2} \cdot \ldots \cdot \; g^{s_T} (mod \; p) = g^{s_1+s_2+\ldots+s_T} \, mod \; p \qquad (3.12)$$

БЧ помешает общий (итоговый) открытый ключ ($h_{\text{общ.}}$) на ДО. Для того чтобы уменьшить риск подделки или модификации переданного пользователю ключа, БЧ подписывает общий открытый ключ своей цифровой подписью, а избиратели, имея сертификаты открытого ключа БЧ, верифицируют подпись [5, 100].

Шифрование

Шаг 3. Избиратель V_i, голосуя за j-го кандидата, выбирает одно число из двух возможных значений: $v_{ij} = (0,1)$, где v_{ij}=1- «за» j-го кандидата, v_{ij}=0 -

«против» j-го кандидата, где $i = 1,2,\dots,n$. n – количество избирателей, $j = 1,2,\dots,k$. k – количество кандидатов и шифрует свой голос следующим образом [5, 100]:

$$(A_i, B_i) = \left(g^{r_i}, h_{общ.}{}^{r_i}.G^{v_{ij}}\right), \quad (3.13)$$

где r_i – случайное число, $1 \le r_i \le p-1$ и G – примитивный элемент над полем Галуа GF(p), (A_i, B_i) – первая и вторая части криптограммы (3.13) – зашифрованного бюллетеня избирателя.

Шаг 4. Избиратель V_i формирует доказательство корректности заполнения бюллетеня (этот вопрос рассматривается отдельно в главе 4).

Шаг 5. Зашифрованный бюллетень и доказательство корректности все избиратели направляют в БЧ. После этого, избиратель получает сообщение о том, что его голос принят и учтен [5, 100].

Частичное расшифровывание:

После того, как серверы голосования получат первую криптограмму из блокчейна, начнется процесс частичной расшифровки.

Шаг 6. Серверы делают предварительную расшифровку своими секретными ключами s_j [5, 100].

Шаг 7. Сервер E_t выполняет частичную расшифровку бюллетеней каждого избирателя по кандидату j, вычисляя [5, 100]:

$$W(j)_{1t} = A_1^{s_t},\ W(j)_{2t} = A_2^{s_t}, \dots, W(j)_{nt} = A_n^{s_t} \quad (3.14)$$

где $W(j)_{it}$ – частичная расшифровка бюллетеня по j-му кандидату, i – номер избирателя, t – номер сервера, s_t – закрытый ключ сервера t. Затем каждый сервер вычисляет произведение частичных расшифровок всех избирателей по j-му кандидату. [5, 100]:

$$X(j)_t = \prod_i W(j)_{it} \quad (3.15)$$

Заметим, что частичная расшифровка не дает серверу никакой информации о том, как проголосовал избиратель, поскольку расшифрование не окончено и поэтому никто не может узнать результаты текущего голосования до завершения процедуры голосования.

Шаг 8. Произведение $X(t)_t = \prod_i W(j)_{it}$ каждый сервер отправляет в БЧ [5, 100].

Полное расшифрование и подсчет голосов избирателей

Шаг 9. В БЧ вычисляется произведение величин $X(j)_t$ от разных серверов

$$X(j) = \prod_t X(j)_t,$$

где t – номер сервера.

Раскроем это произведение (номер кандидата опустим):

$$X(j) = (W_{11} \cdot W_{21} \cdot \ldots \cdot W_{n1}) \cdot (W_{12} \cdot W_{22} \cdot \ldots \cdot W_{n2}) \cdot \ldots \cdot (W_{1T} \cdot W_{2T} \cdot \ldots \cdot W_{nT}) \quad (3.16)$$

Перегруппировав множители в данном выражении, мы получим:

$$X = (W_{11} \cdot W_{12} \cdot \ldots \cdot W_{1T}) \cdot (W_{21} \cdot W_{22} \cdot \ldots \cdot W_{2T}) \cdot \ldots \cdot (W_{n1} \cdot W_{n2} \cdot \ldots \cdot W_{nT}) =$$
$$(g^{r_1 s_1} \cdot g^{r_1 s_2} \cdot \ldots \cdot g^{r_1 s_T}) \cdot (g^{r_2 s_1} \cdot g^{r_2 s_2} \cdot \ldots \cdot g^{r_2 s_T}) \cdot \ldots \cdot (g^{r_i s_1} \cdot g^{r_i s_2} \cdot \ldots \cdot$$
$$g^{r_i s_T}) \, mod \; p = g^{r_1 (s_1 + s_2 + \ldots + s_T)} \cdot g^{r_2 (s_1 + s_2 + \ldots + s_{Tt})} \cdot \ldots \cdot g^{r_i (s_1 + s_2 + \ldots + s_T)} \, mod \; p =$$
$$g^{(s_1 + s_2 + \ldots + s_T)} \cdot (g^{r_1 + r_2 + \ldots + r_n}) \, mod \; p = g^{\sum s_t} \cdot g^{\sum r_i} \, mod \; p \quad (3.17)$$

Шаг 10. Полное расшифровывание выполнятся в БЧ.

Сначала вычисляется $Y(j) = \prod_i B_i$:

$$Y(j) = B_1 \cdot B_2 \cdot \ldots \cdot B_n = \left(h_{общ.}{}^{r_1} \cdot G^{v_{1j}}\right) \cdot \left(h_{общ.}{}^{r_2} \cdot G^{v_{2j}}\right) \cdot \ldots \cdot \left(h_{общ.}{}^{r_n} \cdot G^{v_{nj}}\right) mod \; p$$
$$= h_{общ.}{}^{\sum r_i} \cdot G^{\sum v_i} (mod \, p) \quad (3.18)$$

Далее вычисляется:

$$\frac{Y(j)}{X(j)} = \frac{h_{общ.}{}^{\sum_{i=1}^{n} r_i} \cdot G^{\sum_{i=1}^{n} v_i} (mod \; p)}{g^{\sum_{i=1}^{n} s_t} \cdot g^{\sum_{i=1}^{n} r_i (mod \; p)}} = \frac{g^{\sum_{i=1}^{n} s_t \sum_{i=1}^{n} r_i} \cdot G^{\sum v_i}}{g^{\sum_{i=1}^{n} s_t} \cdot g^{\sum_{i=1}^{n} r_i}} = G^{\sum_{i=1}^{n} v_i} \, mod \, p. \quad (3.19)$$

Шаг 11. Подсчет голосов (вычисление суммы голосов, поданных за j-го кандидата): $\sum_{i=1}^{n} v_{ij} = log_G \, G^{\sum_{i=1}^{n} v_{ij}} \; mod \, p.$ (3.20)

Логарифм вычисляется по заранее составленной таблице, в которой до начала выборов, в зависимости от числа участников и параметра G, посчитаны возможные результаты голосования (см. табл.3.3) [5, 100].

Таблица 3.3. Общий вид таблицы возможных результатов голосования

$\sum_{i=1}^{n} v_{ij}$	$G^{\sum_{i=1}^{n} v_{ij}} \; mod \; p$
0	$G^0 \; mod \; p$
1	$G^1 \; mod \; p$
2	$G^2 \; mod \; p$

…..	
n	$G^n \bmod p$

ИКП отправляет результаты голосования в ЦИК. ЦИК осуществляет окончательный подсчет голосов по всем провинциям, готовит отчет о результатах выборов и объявляет результаты выборов на сайте выборов [5].

Стоит отметить, что предлагаемый протокол обеспечивает комплексную защиту от атак на разных уровнях и отвечает требованиям безопасности системы голосования: обеспечивается тайна голосования и анонимность голосующего; аутентификация избирателя; уникальность и точность голосования; подтверждение голосования.

В следующем разделе проведем анализ наиболее вероятных и опасных угроз, которые могут обнаруживаться и блокироваться в этой системе.

3.4. Анализ угроз в разработанной системе ДЭГ

В системах электронного голосования существует достаточно много угроз, связанных с действиями нарушителя и неправомерными действиями участников протокола голосования [5, 83]. В таблице 3.4 показано несколько наиболее опасных типов угроз, которые могут существовать в предлагаемой системе ДЭГ.

Таблица 3.4. Типы угроз для системы ДЭГ

Со стороны посторонних лиц	Со стороны избирателя	Со стороны ИК
Нарушение тайны голосования	Неправильное заполнение бюллетеня	Нарушение тайны голосования
Нарушение анонимности	Повторное голосование	Нарушение анонимности, в том числе после окончания выборов
Вброс голосов	-	Вброс голосов
Голосование за лиц, не пришедших на выборы		Получение информации о результатах голосования до окончания голосования

Рассмотрим способы предотвращения и блокирования угроз в предлагаемой системе ДЭГ [5].

Предотвращение нарушения тайны голосования обеспечивается за счет шифрования бюллетеня по схеме ЭГ, которая при выборе соответствующих параметров является вычислительно стойкой. В данной системе голосования применено распределение секретных ключей между серверами. С помощью этих ключей независимые сервера партий, участвующих в выборах, выполняют предварительное расшифрование бюллетеня. При этом частичная расшифровка одним или несколькими серверами не позволяет определить содержимое бюллетеня, если хотя бы один из T серверов является честным. Мы предполагаем, что сговор T серверов маловероятен. Единый ключ расшифрования никогда не формируется и нигде не хранится. Также сервера предоставляют доказательства корректности частичного расшифрования. За счет разделения ключей расшифрования никто не может узнать результаты текущего голосования до закрытия процедуры голосования [5].

Полная расшифровка в БЧ проводится для суммы голосов, поэтому результат голосования относительного каждого избирателя остается неизвестным для ИКП.

Анонимность голосования достигается за счет использования гомоморфного свойства криптосистемы Эль-Гамаля. Обеспечение анонимности голосования основываются на том, что выполняется следующее условие:

$$D_{\hat{E}}\left(Enc(v_1)\cdot Enc(v_2)\cdot \dots Enc(v_N)\right) = v_1 + v_2 + \dots + v_N, \qquad (3.21)$$

где $Enc(v_i)$ - зашифрованный голос v_i i-го избирателя, $D_{\hat{E}}(Enc)$ – результат дешифрования криптограммы, составленной из произведения криптограмм всех избирателей. Суть выражения (3.21) заключается в том, что результат дешифрования произведения зашифрованных голосов равен сумме этих голосов, а за счет того, что при расшифровании получается сумма всех голосов сразу, обеспечивается анонимность индивидуальных голосов. Этот вопрос был рассмотрен в п.2.1. Действительно, предположим, что за некоторым избирателем установлена слежка и его бюллетень анализируется отдельно. Так

как расшифрование проводится раздельными серверами и сговор всех серверов исключается, то бюллетень, не может быть расшифрован отдельными лицами [5].

Блокирование вброса голосов посторонними лицами достигается за счет того, что избиратели проходят процедуру двухфакторной аутентификации на этапе инициализации системы. Вброс голосов на последнем этапе (после расшифровки агрегированных голосов) избирательными комиссиями провинции и ЦИК также невозможен, поскольку все голоса помещены в транзакцию блокчейна, которая содержит доказательство корректности процедуры расшифрования [5].

Блокирование голосования за лиц, не пришедших на выборы, достигается за счет использования избирателем своей электронной подписи. При этом избиратель подписывает бюллетень своим секретным ключом перед передачей бюллетеня на (серверов голосования). Посторонние лица, в том числе ИКП не смогут сформировать подпись избирателя, поскольку никто не знает секретного ключа подписи избирателя и, следовательно, не сможет проголосовать за избирателя [5].

Блокирование неправильно заполненного бюллетеня избирателем достигается за счет использования метода доказательства корректности заполнения избирательного бюллетеня. Бюллетень в электронном виде представляет собой строку символов (1,0), где 1- голос «за» и 0 – голос «против», поданные за каждого кандидата. Любые отклонения от установленных вариантов голосования, например, использование числа 2 или -1, поданных за кандидата, будут означать некорректное заполнение бюллетеня. Для того, чтобы подтвердить корректность заполнения бюллетеня, необходимо использовать методы доказательства корректности заполнения бюллетеня. Сначала, избиратель шифрует бюллетень по схеме Эль-Гамаля, а затем формирует доказательство того, что он зашифровал свой бюллетень из значений {0,1} и отправляет значение доказательств в БЧ, который проверяет, что избиратель правильно заполнил свой бюллетень. Если проверка прошла

успешно, то голос избирателя принят. Существуют различные методы проверки корректности заполнения избирательного бюллетеня, например [88 - 89, 98, 105 -108, 110,111]. Подробно этот вопрос рассмотрен в следующей главе.

Блокирование повторного голосования достигается за счет того, что избиратель может зайти на сайт выборов со своей учетной записью только один раз, если он попытается войти в систему снова, ему будет сообщено, что он уже проголосовал, тогда он не сможет проголосовать более одного раза [5].

Блокирование получения информации о результатах голосования до окончания голосования достигается за счет того, что в данной гомоморфной системе расшифровка агрегированных бюллетеней происходит в два этапа: сначала сервера осуществляют предварительное расшифрование, а затем БЧ осуществляет полное расшифрование. Досрочное расшифрование невозможно, если хотя бы один из серверов выдержит регламент голосования и не начнет расшифрование раньше окончания выборов [5].

3.5. Научно - технические предложения по внедрению разработанной системы дистанционного электронного голосования

С целью демонстрации работоспособности, предложенной модели ДЭГ и элементов протокола, был разработан программный комплекс, состоящий из нескольких программ и интерфейсов для участников избирательного процесса. Общая схема взаимодействия программ внутри макета представлена на рисунке 3.4. Процесс голосования моделируется с помощью трех программ: сервера, избирателя и комиссии ДЭГ. С помощью программы сервера можно симулировать наличие нескольких серверов, сгенерировав несколько пар ключей внутри единой программы. С помощью программы избирателя в свою очередь можно стимулировать голосование нескольких участников, отправив несколько голосов за время единственной сессии [5].

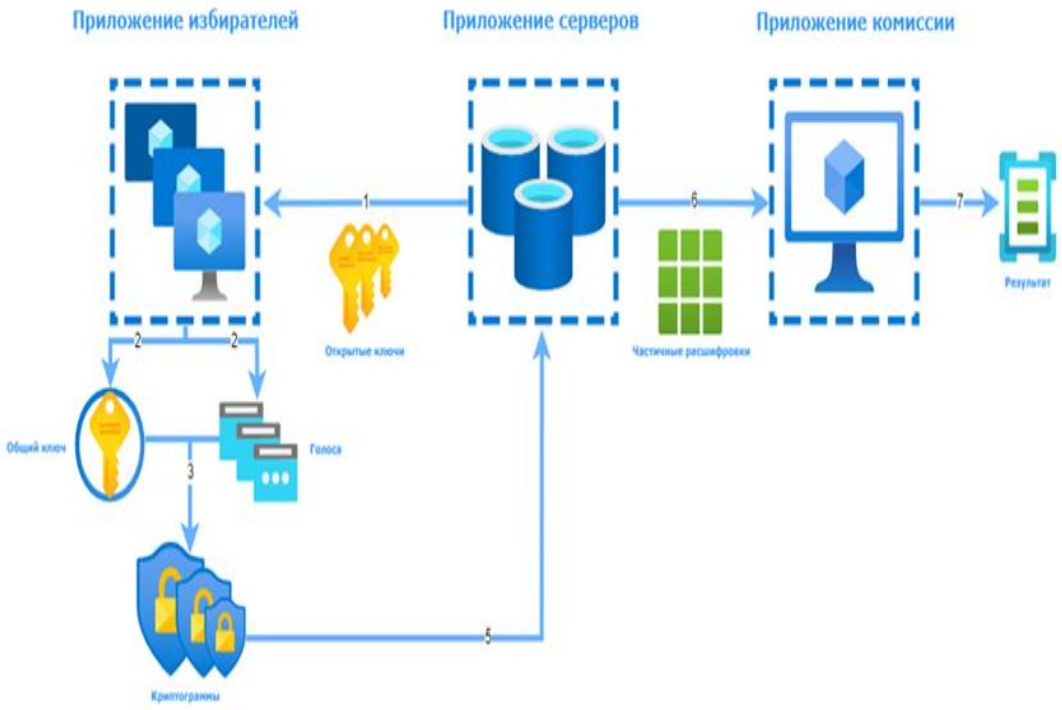

Рис. 3.4. Макет системы ДЭГ

Интерфейс сервера голосования представлен на рисунке 3.5, интерфейс избирателя на рисунке 3.6. [5, 100].

В верхней части окон отображаются общесистемные параметры. После нажатия кнопки генерации ключа, в текстовых браузерах отобразятся открытый и закрытый ключ. Закрытые ключи, советующие отправленным открытым ключам в файл записаны не будут, они будут храниться в памяти программы до того, как пользователи завершат шифрование голосов. При нажатии на кнопку отправки открытого ключа, открытый ключ будет записан в файл.

Для голосования, избирателю необходимо нажать кнопку «За» или кнопку «Против», а затем отправить голос (см. Рис. 3.6). При нажатии кнопки «Отправить» голос шифруется и записывается в файл [5].

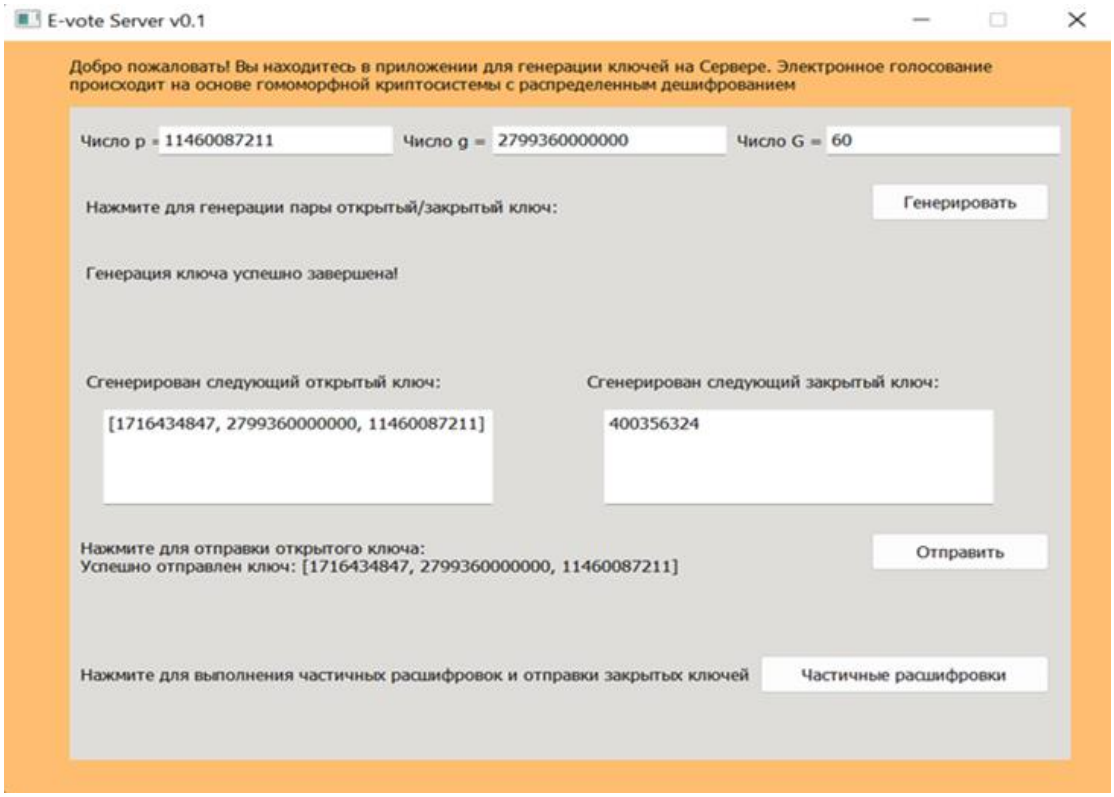

Рис.3.5. Интерфейс сервера голосования (генерация и отправка ключа)

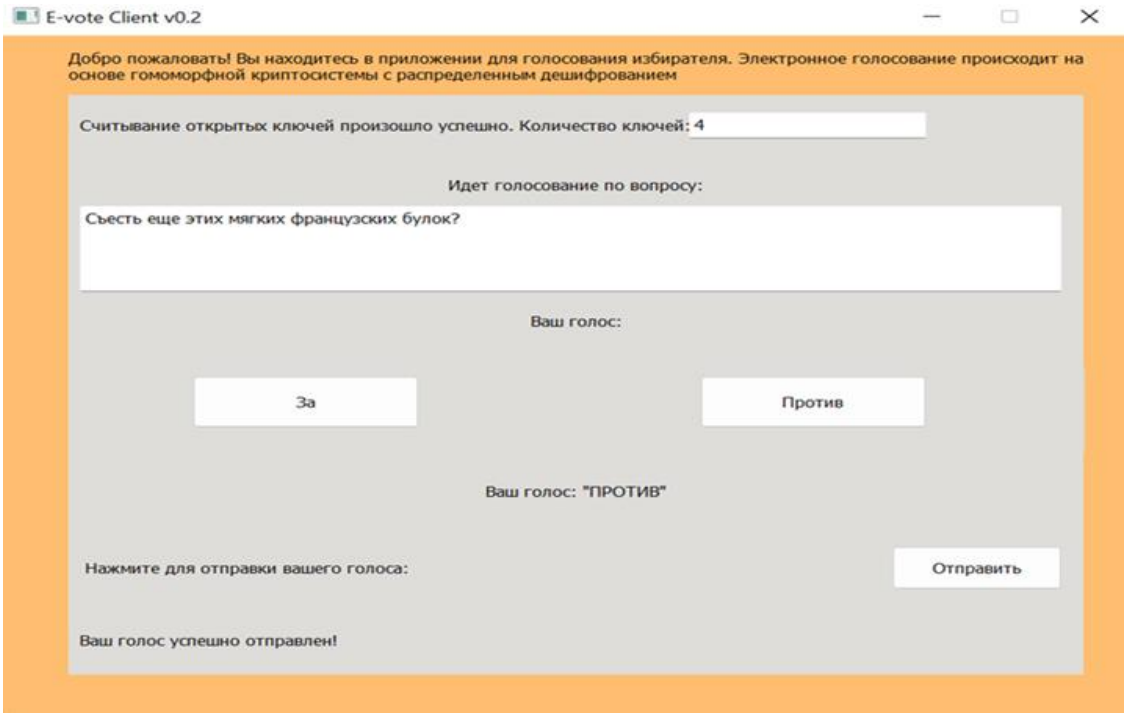

Рис.3.6. Интерфейс избирателя, отправка голоса

Кнопка «Расшифровать» выводит полную информацию об итогах голосования, включая рассчитанные частичные расшифровки X и Y, и расшифрует результаты голосования по каждому кандидата (см. Рис. 3.7) [5].

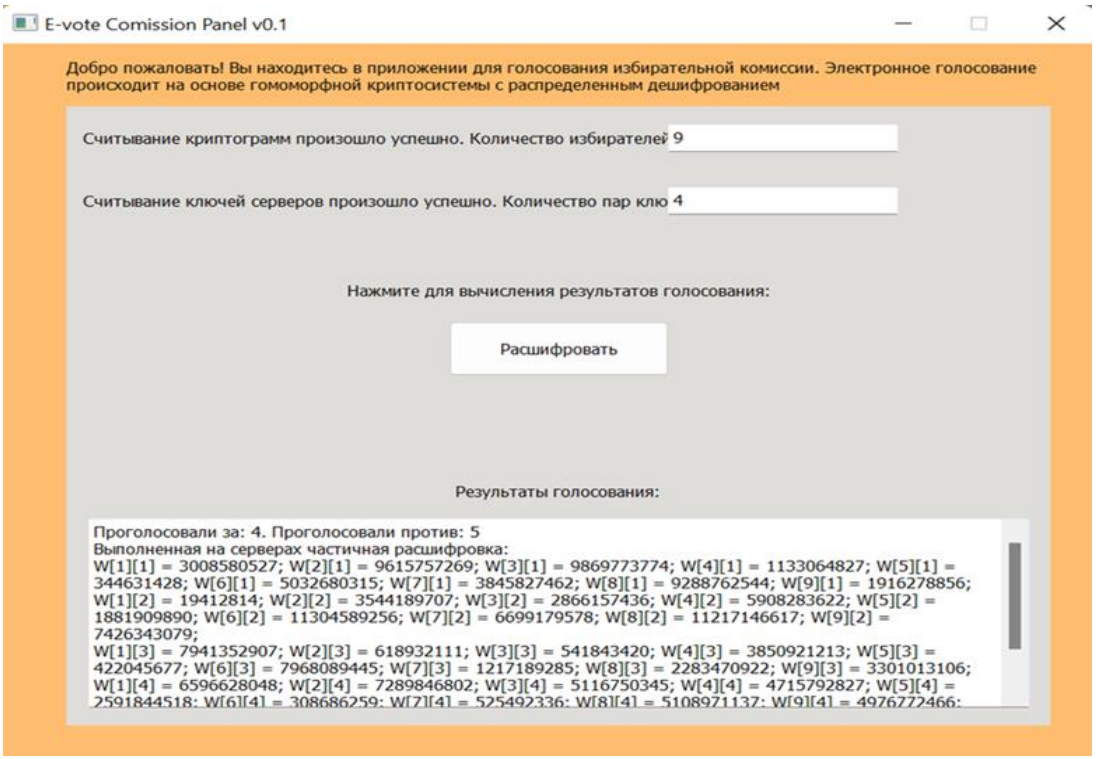

Рис.3.7. Интерфейс избирательной комиссии

Все приложения были разработаны на языке программирования *Python 3.10* с использованием библиотеки PyQt5 для создания графического интерфейса приложений [5].

При моделировании системы ДЭГ использованы следующие параметры: p= 11460087211; g= 2799360000000; G=60; N=100, k=3, с использованием 1024-битного ключа.

Моделирование процесса голосования проводилось на ноутбуке со следующими характеристиками ОС: 64-разрядная Windows 10; оперативная память: 4 ГБ; процессор: Intel (R) Core (TM) i5-8250 CPU при частоте 1,60 GHz, 1,0 GHz.

Открытый ключ занимает в среднем 127 байт дискового пространства, секретный ключ 72 байта. Зашифрованный голос занимает 8.192 байт дискового пространства. Заметим, что в данном макете блокчейн не был использован.

Тестирование было проведено на основе следующего параметра: количество серверов: 3, количество голосующих: 9, тип варианта голосования: да/нет.

Основываясь на результатах моделирования, можно сказать, что предложенный протокол, основанный на гомоморфном шифровании с распределенным дешифрованием, подтвердил свою работоспособность.

Отметим, что для использования предлагаемого протокола на реальных выборах параметры должны быть расширены.

Выводы по 3-й главе

1. Проведен анализ принципов построения гомоморфных криптосистем электронного голосования. Рассмотрены криптосхемы Пэйе, Бенало. Приведено сравнение эффективности гомоморфного шифрования для схем Пэйе, Бенало и Эль-Гамаля путем вычисления времени генерации ключа, шифрования и дешифрования бюллетеня. Результаты показали, что схема Эль-Гамаля требует меньше времени для выполнения этих процессов, поэтому эта схема выбрана в качестве основной для дальнейшего применения в протоколе системы ДЭГ.
2. Разработан протокол перспективной системы дистанционного электронного голосования, учитывающий особенности угроз системе ДЭГ в арабских странах, Протокол основан на гомоморфном шифровании и распределенном дешифровании, что обеспечивает выполнение требований безопасности информации: тайна волеизъявления; анонимность голосующего; аутентификация избирателя; уникальность и точность голосования, подтверждение факта голосования. Отличается от известных тем, что обеспечивает дополнительную защищенность от атаки, нацеленной на нарушение анонимности избирателя со стороны административного ресурса системы. Это достигается за счет применения распределенного

дешифрования, при котором никто из участников системы не имеет доступа к ключу дешифрования.

3. Проанализированы наиболее опасные угрозы, которые могут быть в системе ДЭГ и представлены доказательства возможности их предотвращения или блокирования. Отметим, что основные угрозы связаны с влиянием субъективного (человеческого фактора).
4. Разработан демонстрационный макет модели ДЭГ, состоящий из нескольких программ и интерфейсов для участников избирательного процесса. На основе моделирования процедуры голосования с использованием макета подтверждена функциональность протокола.

ГЛАВА 4. МЕТОД ЗАЩИТЫ ОТ АТАКИ НЕКОРРЕКТНОГО ЗАПОЛНЕНИЯ ИЗБИРАТЕЛЬНОГО БЮЛЛЕТЕНЯ В СИСТЕМЕ ДИСТАНЦИОННОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ, ОБЕСПЕЧИВАЮЩИЙ СКРЫТНОСТЬ ВОЛЕИЗЪЯВЛЕНИЯ ИЗБИРАТЕЛЯ ПО ОТДЕЛЬНЫМ КАНДИДАТАМ И ПО ВСЕМ КАНДИДАТАМ В ЦЕЛОМ

4.1. Анализ методов проверки корректности заполнения бюллетеня на основе проверки логарифмов

В последнее время большое внимание при построении систем электронного голосования уделяется защите от угрозы преднамеренного или случайного неправильного заполнения бюллетеня голосования избирателем. Эта задача не является тривиальной, так как контроль правильности заполнения бюллетеня должен осуществляться в зашифрованном виде, без раскрытия того, как проголосовал избиратель [112].

Бюллетень в электронном виде представляет собой строку символов (1, 0). В зависимости от правил выборов могут быть различные варианты голосования. Например, избиратель может проголосовать за одного кандидата из k кандидатов, или он может проголосовать за двух и более кандидатов $(t \text{ из } k)$, но он не может не голосовать. Могут быть и другие правила, установленные избирательной комиссией.

Возможны два вида атак на систему ДЭГ со стороны избирателя, которые могут проводиться умышленно или случайно. Первый вид атаки заключается в том, что избиратель указывает некорректное число, соответствующее его выбору ЗА или ПРОТИВ по конкретному кандидату. Любые отклонен ия от установленных вариантов голосования, например, использование чисел 2 или (-1), поданных за какого-то кандидата, будут означать некорректное заполнение бюллетеня [113].

Второй вид атаки заключается в нарушении избирателем, установленного ИК правила голосования по количеству поданных голосов ЗА в одном бюллетене. То есть помимо проверки корректности заполнения ИзБ по каждому кандидату, необходима проверка корректности заполнения ИзБ в целом.

Другими словами, число голосов m, поданных ЗА, должно быть в интервале: $m_{min} \leq m \leq m_{max}$, где m_{min}, m_{max} – минимальное и максимальное число кандидатов, за которых может проголосовать избиратель согласно правилу голосования, установленному ИК [113]. Пример правильного заполнения бюллетеня показан в таблице 4.1.

Таблица 4.1. Формирование правильного заполнения бюллетеня

Кандидаты	D_1	D_2	D_3	D_4	……	D_k
Выбор избирателя V_1	1	0	0	1	……..	0

Как видно из таблицы 4.1, избиратель отдал голос «за» за первого и четвертого кандидатов, и голос «против» – за остальных кандидатов. Таким образом, бюллетень должен содержать только значения (1, 0). Для того, чтобы подтвердить, что он действительно заполнил свой бюллетень правильно, необходимо использовать методы доказательства корректности заполнения ИзБ [113].

В следующем разделе, рассмотрим один из известных методов проверки заполнения ИзБ по каждому кандидату (предложен в [88] авторами Cramer R., Gennaro R., Schoenmakers B. - метод CGS).

Анализ метода проверки корректности заполнения бюллетеня по каждому кандидату при шифровании бюллетеня по схеме Эль-Гамаля в поле GF(p)

Избиратель выполняет следующие операции:

- Выбирает своего кандидата;

- Шифрует ИзБ, как показано ниже (см. таблицу 4.2);

- Формирует доказательство ИзБ за каждого кандидата, в соответствии с алгоритмом в таблице 4.2.

Таблица 4.2. Процедура формирования доказательства корректности заполнения избирательного бюллетеня

Избиратель: голосование и формирование доказательства		*Оценки сложности (при выборе v_i=1)*
Проголосовал «за» кандидата: $v_i = 1$.	«против» кандидата: $v_i = 0$.	
Избиратель случайным образом выбирает числа:		
$r_i, w, u_1, d_1 \in \mathbb{Z}_q$	$r_i, w, u_2, d_2 \in \mathbb{Z}_q$	*O (1)*
Осуществляет шифрование бюллетеня по каждому кандидату		
Вычисляет: $A_i = (g^{r_i}) \bmod p$ $B_i = h^{r_i} G^{v_i} \bmod p$	$A_i = (g^{r_i}) \bmod p$ $B_i = h^{r_i} / G^{v_i} \bmod p$	*1kM* *2kM*
Формирует доказательства корректности шифрования, вычисляя:		
Вычисляет: $a_1 = g^{u_1} A_i^{d_1} \bmod p$ $b_1 = h^{u_1} (B_i G^{v_i})^{d_1} \bmod p$ $a_2 = g^{w} \bmod p$ $b_2 = h^{w} \bmod p$	 $a_1 = g^{w} \bmod p$ $b_1 = h^{w} \bmod p$ $a_2 = g^{u_2} A_i^{d_2} \bmod p$ $b_2 = h^{u_2} (B_i / G^{v_i})^{d_2} \bmod p$	 *2kM* *3kM* *1kM* *1kM*
Вычисляет хэш-функцию $c = H(A, B, a_1, b_1, a_2, b_2) \bmod q$		
Вычисляет доказательство: $d_2 = c - d_1 \bmod q$ $u_2 = w - r_i d_2 \bmod q$	$d_1 = c - d_2 \bmod q$ $u_1 = w - r_i d_1 \bmod q$	*O(k)* *O(k)*
Всего		*10kM*

Далее, избиратель отправляет значения (A_i, B_i, a_1, b_1, a_2, b_2, d_1, d_2, u_1, u_2) проверяющему (в БЧ), где согласно алгоритму из таблицы 4.3 происходит проверка того, что избиратель правильно заполнил свой бюллетень.

Таблица 4.3. Алгоритм проверки корректности голосования за кандидата

Проверяющий (БЧ)		*Оценки сложности*
Вычисляет хэш-функцию c = $H(A_i, B_i, a_1, b_1, a_2, b_2)$		
Проверяет сравнения:	$c = d_1 + d_2 \bmod q$	*O(k)*
	$a_1 = g^{u_1} A_i^{d_1} \bmod p$	2M
	$b_1 = h^{u_1} (B_i g^{v_i})^{d_1} \bmod p$	2M
	$a_2 = g^{u_2} A_i^{d_2} \bmod p$	2M
	$b_2 = h^{u_2} (B_i / g^{v_i})^{d_2} \bmod p$	2M
	Всего	8 kM

где p, q: простые числа, $G \in G_q$, g – генератор G.

Проведем оценку сложности операций, требуемых для формирования доказательства корректности заполнения ИзБ и проверки этого доказательства. При этом будем учитывать только количество операций возведения числа в степень по mod p (операции сложения и умножения чисел учитывать не будем ввиду их меньшей сложности по сравнению с операцией возведения в степень). (Обозначим символом M операцию возведения числа в степень по mod p; k – количество кандидатов.

Таблица 4.2 показывает, что сложность формирования доказательства корректности заполнения бюллетеня для k кандидатов составляет 10kM. Наоборот, объем вычислений для проверки доказательства корректности заполнения бюллетеня на одного избирателя, проводимых в БЧ, составляет 8kM, как видно из таблицы 4.3.

В случае, рассмотренном выше, контролирующий орган (БЧ) может убедиться, что избиратель корректно проголосовал за каждого кандидата («за» или «против»). Отметим, что использование такого метода в системе ДЭГ важно для обнаружения атаки неправильного заполнение бюллетеня избирателем.

В рассмотренном методе проверка корректности заполнения бюллетеня, осуществляется путем анализа зашифрованного бюллетеня без раскрытия информации о том, как проголосовал избиратель. Для этого используется метод, «доказательства с нулевым разглашением секрета» (ZKP). В данном случае используется метод доказательства на основе равенства логарифмов, предложенный в [89], который в свою очередь основывается на методе цифровой подписи Чаума и Педерсена [89]. Рассмотрим суть метода доказательства подробно.

Пусть, Z_p – кольцо вычетов по модулю p. G_q - группа простого порядка q , g – генератор этой группы $q \mid p-1$. И пусть Gq- единственная подгруппа Z_p^* порядка q. Задача дискретного логарифмирования включает в себя

нахождение показателя степени $r \in Z_q$ такого, что $g^r = y\,(mod\,p)$ для заданного y.

Пусть $g, h \in Z_q$ удовлетворяют условию $A = g^r \bmod p$, $B = h^r \bmod p$.

Доказывающая сторона *P* хочет убедить проверяющую сторону *V*, в том, что она знает r, не раскрывая r [89].

Для этого *P* и *V* выполняют следующий протокол, в котором *P* доказывает *V*, что

$$\log_g A = \log_h B, \qquad (4.1)$$

не раскрывая r [90].

Таблица 4.4. Алгоритм доказательства на основе равенства логарифмов

P (доказывающий)	*V* (проверяющий)
знает $\{r, g, h, A, B\}$	знает $\{g, h, A, B\}$
1. выбирает $w \in Z_q$	
2. вычисляет $a = g^w \bmod p$; $b = h^w \bmod p$.	
3. передает (a, b)	(a, b) →
	4. выбирает $c \in Z_q$
	5. передает c P
	c ←
6. вычисляет $d = w + rc\,(mod\,q)$	
7. передает d	d →
	8.проверяет сравнения $g^d =^? a \cdot A^c$; $h^d =^? b \cdot B^c$.

Выполнение сравнений свидетельствуют о том, что равенство (4.1) выполняется.

Действительно, несложно проверить, что:

$g^d = g^{w+r\cdot c}, aA^c = g^w \cdot g^{r\cdot c} = g^{w+r\cdot c}$, и

$h^d = h^{w+r\cdot c}, b \cdot B^c = h^w \cdot h^{r\cdot c} = h^{w+r\cdot c}$.

Откуда и следует равенство логарифмов в (4.1).

В [88] доказано, что данный протокол обладает свойство ZKP, если проверяющая сторона *V* является честной.

Это условие выполняется в задачах проверки доказательства в предложенном протоколе ДЭГ, поскольку проверяющей стороной является доверенный участник протокола – блокчейн.

В [88] также показано, что данный протокол может быть не интерактивным, если доказывающая сторона будет формировать $c = H(A, B, a, b, g, h)$, где $H(.)$ – криптографическая стойкая хэш – функция.

Аналогичным образом может быть построена схема проверки корректности заполнения бюллетеня по каждому кандидату при шифровании бюллетеня по криптосхеме Эль -Гамаля на эллиптической кривой.

Рассмотрим этот метод. Сначала, рассмотрим основные этапы шифрования расшифрования бюллетеня применительно к гомоморфной системе ЭГ на ЭК.

Генерация ключей

Сервер генерирует эллиптическую кривую вида: $y^2 = x^3 + xa + b$. (4.2)

над полем Галуа $GF(p)$ и выбирает базовую точку $P \in E\big(GF(p)\big)$ порядка m.

Сервер случайным образом выбирает закрытый ключ d, $d \in \{1, \dots, m-1\}$. Далее вычисляется открытый ключ:

$$Q = dP \bmod p, \quad (4.3)$$

и вычисляется точка $M = vP \bmod p$, (4.4)

Параметры p, E, P, M, Q публикуются в БЧ. Секретный ключ d хранится на серверах в разделенном на доли виде.

Шифрование бюллетеня

Избиратель V_i, i = 1, 2, …, n, где n – количество избирателей, шифрует сообщение (бюллетень) v_i по схеме Эль-Гамаля с помощью открытого ключа и получает криптограмму:

$$\mathrm{Enc}(M_i) = C_i = (A_i, B_i), \quad (4.5)$$

где Enc () – функция шифрования; (A_i, B_i) – две части криптограммы C_i: первая часть: $A_i = rP \bmod p$, (4.6)

вторая часть: $B_i = (M + r_i Q) \bmod p$, (4.7)

r_i – выбирается случайным образом.

Дешифрование бюллетеня

Расшифрование криптограммы осуществляется с помощью закрытого ключа d: $\mathrm{Dec}(C_i) = B_i - dA_i \bmod p = M_i$, (4.8)

где Dec () – функция дешифрования.

Криптосистема ЭГ на ЭК обладает гомоморфным свойством.

Допустим, есть два шифртекста:

$C_1 = (A_1, B_1) = (r_1 P, M_1 + r_1 Q)$ и (4.9)

$C_2 = (A_2, B_2) = (r_2 P, M_2 + r_2 Q)$, (4.10)

Криптограммы могут быть агрегированы аддитивно:

$C_3 = C_1 + C_2 = \big((r_1 + r_2)P,\ (M_1 + M_2) + (r_1 + r_2)Q\big)$, (4.11)

Тогда при расшифровании C_3 получаем:

$\mathrm{Dec}(C_3) = M_1 + M_2$, (4.12)

Алгоритм голосования, формирование доказательства корректности заполнения ИзБ и их проверки включает следующие шаги 1 - 4, которые отображены в таблицах 4.5 и 4.6.

Шаг 1. Загрузка открытого ключа из БЧ.

Шаг 2. Выбор своего кандидата.

Шаг 3. Шифрование бюллетень по схеме ЭГ на ЭК [95 - 97].

Шаг 4. Формирование доказательства того, что он зашифровал свой бюллетень из значений $(1, 0)$.

Таблица 4.5. Формирование доказательства корректности заполнения бюллетеня

Избиратель: голосование и формирование доказательства			Оценки сложности (при выборе v= 1)
Голосует:	«за» кандидата – $v_i = 1$	«против» кандидата – $v_i = 0$	$O(1)$

Случайным образом выбирает числа $w, r_1, t_1, u_1 \in Z_q$.			$O(1)$
Осуществляет шифрование бюллетеня по каждому кандидату (вычисляет):	$A = (r_1 P) \bmod p$ $B = (\mathrm{M} + r_1 Q) \bmod p$	$A = (r_1 P) \bmod p$ $B = (r_1 Q) \bmod p$	1kM 2 kM
Формирует доказательство корректности голосования (вычисляет):	$a_1 = (t_1 P - u_1 A) \bmod p$ $b_1 = (t_1 Q - u_1 (B - v_i \mathrm{P}) \bmod p$ $a_2 = wP \bmod p$ $b_2 = wQ \bmod p$	$a_1 = \mathrm{wP} \bmod p$ $b_1 = wQ \bmod p$ $a_2 = (t_1 \mathrm{P} - u_2 \mathrm{A}) \bmod p$ $b_2 = (t_1 \mathrm{Q} - u_2 (\mathrm{B} - v_i \mathrm{P}) \bmod p$	2 kM 3 kM 1 kM 1 kM
Вычисляет хэш-функцию $c = H(A, B, a_1, b_1, a_2, b_2) \bmod q$			
Вычисляет доказательство:	$u_2 = c - u_1 \bmod q$ $t_2 = w - r_1 u_2 \bmod q$	$u_1 = c - u_2 \bmod q$ $t_1 = w - r_1 u_1 \bmod q$	$O(k)$ $O(k)$
	Всего		10 kM

Таблица 4.6. Алгоритм проверки корректности голосования за кандидата

Проверяющий (БЧ)		Оценки сложности
Вычисляет хэш-функцию с = $H(A, B, a_1, b_1, a_2, b_2)$		
Проверяет сравнения:	$c \bmod q =^{?} u_1 + u_2 \bmod q$ $t_1 P \bmod p =^{?} a_1 + u_1 A \bmod p$ $t_1 Q \bmod p =^{?} b_1 + u_1 (B - v_i P) \bmod p$	$O(k)$ 2kM 3kM
	Всего	5kM

В таблицах 4.5 и 4.6 приведены оценки сложности выполнения проверки корректности заполнения бюллетеня на основе проверки логарифмов. Символ M обозначает операцию умножения точки эллиптической кривой на целое число. Операции сложения точек не учитывались ввиду их меньшей сложности по сравнению с операцией умножения.

Рассмотрим метод проверка корректности заполнения бюллетеня в целом.

Анализ метода проверка корректности заполнения бюллетеня в целом для криптосистемы ЭГ в поле GF(p)

Рассмотрим следующий метод [89, 98], формирования доказательства корректности заполнения ИзБ для всех кандидатов:

Избиратель находит произведение всех криптограмм, содержащихся в ИзБ:

$$C = (\prod C_i) = (\prod A_i, \prod B_i) \quad (4.13)$$

и пусть $\sum v_i = m$ - сумма голосов «ЗА», фактически отданных избирателем за всех кандидатов.

Кроме того, выполняет следующие действия:

- Выбирает случайное число $t \in Z_p$, вычисляет:

$$X = h^t . \quad (4.14)$$

- Находит хэш-функцию

$$c = H(g, \prod A_i, \prod B_i, X, \mathrm{m}).$$

- Находит: $z = t + r \cdot c$ (4.15)

где $r = \sum r_i$, а r_i числа, ранее использованные при формировании криптограмм. Затем он посылает (X, z, m') в БЧ.

Если избиратель проголосовал неправильно, то есть совершил атаку на систему ДЭГ, то он указывает общее количество голосов "ЗА", отданных за всех кандидатов - m', которое отличается от фактической суммы отданных голосов m, $m \neq m'$.

БЧ выполняет проверку:

- Находит хэш-функцию следующим образом:

$$c = H(g, \prod A_i, \prod B_i, X, m');$$

- Проверяет сравнение

$$h^z =^? X \cdot \left(\frac{\prod_i B_i}{g^{m'}}\right)^c . \quad (4.16)$$

Рассмотрим правую часть сравнения

$$X \cdot \left(\prod_i B_i \Big/ g^{m'}\right)^c = h^t \cdot \left(\prod_i g^{v_i} h^{r_i} \Big/ g^{m'}\right)^c = h^t \cdot \left(g^m \cdot h^r \Big/ g^{m'}\right)^c \quad (4.17)$$

Если $m = m'$, то $h^{t+r \cdot c} = h^z$, значит сравнение (4.16) выполнятся. В основе этого метода, как и в методе проверки корректности заполнения бюллетеня индивидуально по каждому кандидату, используется доказательство с нулевым разглашением секрета, основанное на проверки логарифмов.

Оценка сложности методов проверки корректности заполнения бюллетеня

На основе анализа соотношений (4.13) - (4.17) несложно установить, что:

– количество операций по формированию доказательства корректности заполнения ИзБ на стороне избирателя – 1 М;

– количество операций проверки доказательства корректности заполнения ИзБ на стороне БЧ – 3 М.

Анализ метода проверка корректности заполнения бюллетеня в целом для криптосистемы ЭГ на эллиптической кривой

Пусть $m_{\max}$ – максимальное число голосов «за», при голосовании за k кандидатов. Будем считать, что ключи (открытый, закрытый) сгенерированы, избиратель выполнил следующие действия:

– Выбирает кандидатов;

– Шифрует бюллетень с помощью открытого ключа: $C_i = (A_i, B_i) \bmod p$,

где $A_i = r_i P \bmod p;\ B_i = F + r_i Q \bmod p$, где $F = b_{vi} P \bmod p$, b_{vi} – выбор избирателем кандидата i, $b_{vi} \in \{0,1\}$, $i = 1, 2, \ldots, k$.

– Формирует доказательство корректности голосования за каждого кандидата, как было описано выше.

Рассмотрим подробно формирование доказательства корректности заполнения бюллетеня в целом.

Избиратель вычисляет сумму криптограмм бюллетеня для всех кандидатов: $C_\Sigma = (A_\Sigma, B_\Sigma)$, (4.18)

где $A_\Sigma = \sum_{i=1}^{k} A_i\ , B_\Sigma = \sum_{i=1}^{k} B_i,\ r = \sum r_i, m = \sum m_i,\ m$ – сумма голосов «за», поданных избирателем в пользу всех кандидатов.

Выполняет следующий алгоритм:

- Находит: $T = t \cdot Q$, (4.19)

где $t \in Z_p$ – случайной число;

- Вычисляет хэш-функцию $c = H(Q, A_\Sigma, B_\Sigma, T, m)$, (4.20)

- Вычисляет: $z' = t + r \cdot c$, (4.21)

- Посылает в БЧ (T, z', m').

Избиратель с целью обмана может указать суммарное число голосов «за», поданных в пользу всех кандидатов m', отличное от фактического числа голосов m, если $m > m_{\max}$.

БЧ вычисляет: $c = H(Q, \sum A_i, \sum B_i, T, m')$, для чего используются криптограммы $C_i = (A_i, B_i)$ из бюллетеня.

Далее БЧ проверяет сравнение:

$$z'Q =^{?} T + c\left(\sum_{i=1}^{k} B_i - m'F_i\right), \quad (4.22)$$

Если сравнение выполнятся, то $m = m'$. Покажем, что это действительно так: $T + c\left(\sum_{i=1}^{k} B_i - m'F_i\right) = tQ + c\left(mF + r_\Sigma Q - m'F\right) =$

$$= tQ + r_\Sigma cQ + c(mF - m'F) = z'Q + c(mF - m'F) = z'Q, \quad (4.23)$$

Сравнение (4.22) выполняется.

Видим, что если $m = m'$ и $m' \leq m_{\max}$, то избиратель проголосовал правильно.

Сложность данного алгоритма формирования и проверки доказательства корректности заполнения ИзБ в целом можно оценить на основе вышеприведенных соотношений так:

– Количество умножений точки эллиптической кривой на число на стороне избирателя – 1М;

– Количество умножений точки эллиптической кривой на число в БЧ – 3М.

Анализ вышеприведенных методов проверки корректности заполнения бюллетеня показывает, что при их реализации происходит раскрытие общего количества голосов, поданных в ходе этой проверки. Рассмотрим эту уязвимость более подробно.

В первом варианте (шифрование в числовом поле GF(p)) избиратель передает проверяющему (X, z, m') во втором варианте (шифрование на ЭК $E_p(a,b)$ передает (T, z', m').

Таким образом, избиратель в этих сообщениях указывает общее количество голосов "ЗА", отданных за всех кандидатов - m'. На наш взгляд, это является недостатком методов проверки, поскольку позволяет посторонним лицам на основе анализа сумм голосов, содержащихся в избирательных бюллетенях, отслеживать интенсивность хода голосования.

Рассмотрим еще один метод проверки корректности заполнения бюллетеня на основе перемешивания криптограмм бюллетеня [108, 109, 114].

4.2. Анализ метода проверки корректности заполнения бюллетеня на основе перемешивания криптограмм бюллетеня

Данный метод рассмотрим применительно к криптосистеме ЭГ на ЭК.

Идея этого метода [109] заключается в следующем: Сервер или БЧ генерирует бланк – бюллетень, представляющий вектор C из зашифрованных следующим образом криптограмм:

$$C = (C_1, .., C_k), \tag{4.24}$$

Первая криптограмма вычисляется как [108, 109, 114]:

$$C_1 = (\rho_1 P, F + \rho_1 Q) \bmod p, \tag{4.25}$$

где P – базовая точка;

$$Q = dP \bmod p, \tag{4.26}$$

Q – открытый ключ,

точка $$F = M_i P \bmod p, \tag{4.27}$$

где $P, Q, F \in E_P(GF(P))$, ρ_1 – выбирается случайным образом, M – сообщение (метка для голоса избирателя).

Остальные криптограммы вычисляют как:

$$C_i = (\rho_i P, \rho_i Q) \bmod p, \tag{4.28}$$

где ρ_i выбирается случайным образом, $\rho_i \in Z_p$, $i = 2,3,\dots,k$.

Сервер публикует C_i и ρ_i на БЧ.

Избиратель для голосования считывает из БЧ бланк-бюллетень и выполняет следующее [112]:

1) Убеждается, что информация, полученная с БЧ, корректна; для этого избиратель проверяет, что $\rho_i P = A_i$ и вычисляет $\mathrm{Rev}_r(C_i) = B_i - \rho_i Q$ – в результате должно получиться либо точка *F*, либо точка $\mathcal{O}$;

2) Приступает к голосованию:

– Выбирает своего кандидата – *Ds*;

– Выбирает перестановку $\pi(s, i_1, i_2, \dots, i_{k-1})$;

– Перемешивает C в соответствии с выбранной перестановкой

$C_i \to C_\pi(i)$

– Маскирует бюллетень. Для этого:

а) Генерирует случайным образом набор целых чисел $r_i \in Z_p$;

б) Вычисляет:

$$C_i' = C_{\pi(i)} + (r_i P, r_i Q) = \left(A_{\pi(i)} + r_i P, B_{\pi(i)} + r_i Q\right) = \left((\rho_i + r_i)P, F_i + (\rho_i + r_i)Q\right) \bmod p \quad (4.29)$$

где $i = 1,2,\ ..,\ k$, причем $F_i = \mathcal{O}$ для $i = 2,\ ..,\ k$.

C_i' отправляет в БЧ;

– Формирует доказательство корректности перемешивания бюллетеня, для чего:

– Получает от БЧ выбранные случайным образом числа s_i и s_i', $s_i, s_i' \in \{0, 1, .., 2^L - 1\}$;

– Вычисляет числа $t_i = s_{\pi(i)}, t_i' = s'_{\pi(i)}$,

– Генерирует случайным образом набор целых чисел $r'_i \in Z_p$;

– Вычисляет

$$C_i'' = t_i C_i' + (r_i' P + r_i' Q) = (A_i'', B_i'') = (t_i A_i' + r_i' P, t_i B_i' + r_i' Q), \quad (4.30)$$

– Отправляет C', C'', t_i и t_i' в БЧ.

Проверка доказательства заключается в проверке выполнения сравнений [108, 109, 114]:

$$\sum_{i=1}^{k} \mathrm{Dec}(C_i) \times s_i =^{?} \sum_{i=1}^{k} \mathrm{Dec}(C_i') \times t_i, \quad (4.31)$$

$$\sum_{i=1}^{k} \mathrm{Dec}(C_i) \times s_i' =^{?} \sum_{i=1}^{k} \mathrm{Dec}(C_i') \times t_i', \quad (4.32)$$

$$\sum_{i=1}^{k} \mathrm{Dec}(C_i) \times s_i \times s_i' =^{?} \sum_{i=1}^{k} \mathrm{Dec}(C_i') \times t_i \times t_i', \quad (4.33)$$

где Dec ()- функция дешифрования.

Однако непосредственные проверка согласно (4.31 – 4.33) невозможна, так как для этого БЧ должен знать закрытый ключ *s*. Поэтому проверка доказательств осуществляется на основе NIZKP. Далее будем использовать обозначение ZP*(x|y)*, означающее доказательство (zero proof) того, что секрет *x* удовлетворяет условию *y*.

Доказательство (4.31) – (4.33) заключается в проверке следующих равенств [114]:

$$ZP(t_i, r_i' | C_i'' = (t_i C_i' + (r_i' P, r_i' Q)), \quad (4.34)$$

где $C_i = (A_i, B_i) = (\rho_i P, F_i + \rho_i Q)$,

$C_i' = ((r_i + r_i')P, F_i + (r_i + r_i')Q)$,

$C_i'' = (t_i A_i' + r_i' P, t_i B_i' + r_i' Q)$,

$$ZP(t_i, r_i' r_i | \sum_{i=1}^{k} t_i \left(C_i \cdot s_i + (r_i P, r_i Q)\right) + (r_i' P, r_i' Q) = \sum_{i=1}^{k} C_i''), \quad (4.35)$$

$$ZP(r_i, r_i', t_i, t_i' | \sum_{i=1}^{k} t_i' \left(C_i \cdot s_i' + (r_i P, r_i Q)\right) = \sum_{i=1}^{k} C_i' t_i'), \quad (4.36)$$

$$ZP(r_i, r_i', t_i, t_i' | \sum_{i=1}^{k} t_i t_i' \left(C_i \cdot s_i s_i' + (r_i P, r_i Q)\right) + t_i' (r_i' P, r_i' Q) = \sum_{i=1}^{k} C_i'' t_i), \quad (4.37)$$

Проверку сравнений (4.34 – 4.37) будем проводить отдельно для каждой части криптограммы $C_i'' = (A_i'', B_i'')$,

Для проверки (4.34) необходимо доказать:

$A_i'' = A_i' t_i + r_i' P, \ B_i'' = B_i' t_i + r_i' Q.$

Покажем это для A_i''.

Избиратель формирует доказательство следующем образом:

– Выбирает случайные числа $z_i, u_i \in Z_p$,

вычисляет: $L_i = z_i P \bmod p, J_i = u_i A'_i \bmod p,$ (4.38)

и находит хеш-функцию $c = H(A''_i, P, L_i, J_i)$.

– Вычисляет: $\theta_i = z_i + r'_i c_i \bmod q$; $\alpha_i = u_i + t_i c_i$,

$T_i = \theta_i P + \alpha_i A'_i \bmod p,$ (4.39)

– Пересылает в БЧ (T_i, L_i, J_i).

БЧ вычисляет хеш-функцию $c' = H(A''_i, P, L_i + J_i)$ и проверяет сравнение:

$$L_i + J_i + c' \cdot A''_i =^? T_i \,. \quad (4.40)$$

Покажем, что если перемешивание выполнено правильно и $c = c'$, то сравнение выполняется. Для этого вычислим левую часть $(L_i + J_i + c' \cdot A''_i)$:

$$L_i + J_i + c \cdot A''_i = z_i P + u_i \cdot A'_i + c(t_i A'_i + r_i P) =$$
$$= z_i P + c \cdot r'_i P + u_i \cdot A'_i + t_i \cdot c \cdot A'_i = \theta_i P + \alpha_i A'_i.$$

Правая часть (T_i).

Видно, что левая часть совпала с правой частью $T_i = \theta_i P + \alpha_i A'_i$. Сравнение (4.40) для A''_i доказано.

Затем БЧ проверяет *ZP* (4.35) для первых частей криптограмм C''_i.

Избиратель генерирует случайное число $w \in Z_p$. Далее вычисляет:

- $T = wP \bmod p,$ (4.41)

- $r_\Sigma = \sum_{i=1}^{k} r_i t_i + r'_i, U = r_\Sigma P \bmod p,$ (4.42)

- Хеш-функцию: $c = H(P, T, U, A''_1, A''_2, .., A''_k),$ (4.43)

- $z = w - r_\Sigma \cdot c \bmod q,$ (4.44)

После чего отправляет в БЧ (T, z).

БЧ вычисляет:

- $U' = \sum_{i=1}^{k} A''_i - \sum_{i=1}^{k} s_i A_i,$ (4.45)

- Хеш-функцию: $c' = H(P, T, U, A''_1, A''_2, .., A''_k),$ (4.46)

- $T' = zP + c'U'.$ (4.47)

Если $T = T'$, то (4.35) для первой части криптограмма C''_i доказано.

Покажем, что это действительно так:

$$U' = \sum_{i=1}^{k} A_i'' - \sum_{i=1}^{k} s_i A_i = \sum_{i=1}^{k} t_i A_i' + r_i' P -$$

$$- \sum_{i=1}^{k} s_i A_i = \sum_{i=1}^{k} t_i \left(A_{\pi(i)} + r_i P\right) + r_i' P - \sum_{i=1}^{k} s_i A_i =$$

$$= \sum_{i=1}^{k} t_i A_{\pi(i)} + \sum_{i=1}^{k} t_i r_i P + r_i' P - \sum_{i=1}^{k} s_i A_i =$$

$$= \sum_{i=1}^{k} t_i A_{\pi(i)} - \sum_{i=1}^{k} s_i A_i + \sum_{i=1}^{k} (t_i r_i + r_i') P =$$

$$- \sum_{i=1}^{k} s_{\pi(i)} A_i - \sum_{i=1}^{k} s_i A_i + \left(\sum_{i=1}^{k} t_i r_i + r_i'\right) P$$

Так как для перестановки π():

$$\sum_{i=1}^{k} s_{\pi(i)} A_{\pi(i)} - \sum_{i=1}^{k} s_i A_i = 0$$

то $U' = \left(\sum_{i=1}^{k} t_i r_i + r_i'\right) P = r_{\sum} P$ (4.48)

Далее $T' = zP + c'U' = \left(w - r_{\sum} c\right) P + c' r_{\sum} P$. Если $c' = c$, то $T' = wP$ и $T' = T$.

Аналогично проверяются сравнения (4.36) и (4.37).

Заметим, что подсчет голосов в такой системе осуществляется на сервере путем покомпонентного агрегирования координат векторов C_i', полученных от всех избирателей, принявших участие в выборах. В этом случае сумма $\sum_{i=1}^{n} C'_1 = \sum_{i=1}^{n} (C_1 v_{i1})$ – количество голосов (в зашифрованном виде), поданных за первого кандидата (v_{ij} = (1, 0)), $\sum_{i=1}^{n} C'_2 = \sum_{i=1}^{n} (C_1 v_{i2})$ – количество голосов, поданных за второго кандидата и т. д. Расшифрование агрегированных голосов осуществляется избирательной комиссией с использованием секретного ключа *s*.

На основе гомоморфного свойства схемы шифрования ЭГ получим расшифровку криптограмм, поданных, например, за *j*-го кандидата: $\mathrm{Dec}(\sum_{i=1}^{n} C'_j) = R_j$.

Логарифмируя это выражение, найдем сумму голосов (R_j), поданных за j-го кандидата. Победителем на выборах будет кандидат, набравший наибольшую сумму голосов – $\max(R_j)$.

В таблицах 4.7, 4.8 приведены оценки сложности выполнения проверки корректности заполнения бюллетеня на основе перестановок на стороне избирателя и в БЧ.

Таблица 4.7. Оценка сложности метода проверки корректности заполнения бюллетеня на основе перестановок

Операции, выполняемые избирателем	Оценка сложности для k-кандидатов
1) Проверка C_i, принятых от БЧ, $r_iP = A_i$ и вычисление $\mathrm{Rev}_r(C_i) = B_i - r_iQ$;	2kM
2) Вычисление: $C_i' = ((r_i + r_i')P, F_i + (r_i + r_i')Q)$ и $C_i'' = (t_iA_i' + r_i'P, t_iB_i' + r_i'Q)$;	6kM
3) Вычисление точек эллиптической кривой $L_i = z_iP, J_i = u_iA_i', T_i = \theta_iP + \alpha_iA_i'$ для доказательства (4.40) для первой части криптограммы A_i (аналогично для второй части B_i).	8kM
4) Вычисление точек эллиптической кривой $U = r_\Sigma P, T = wP$ для доказательства (4.34 – 4.37).	6M
Всего	16kM + 6M

Таблица 4.8. Оценка сложности процедуры проверки корректности перемешивания бюллетеня

Операции, выполняемые БЧ	Оценка сложности
1) Вычисление левой части сравнения (4.40) $L_i + J_i + c'A_i'' = T_i$	2 kM
2) Вычисление $U' = \sum_{i=1}^{k} A_i'' - \sum_{i=1}^{k} s_iA_i$ и левой части сравнения $zP + c'U' = T$.	1 kM 2 M
Всего	3kM + 2M

Заметим, что поскольку в данном методе избиратель перемешивает, криптограммы (C_1, C_2, …, $C_к$) заданные БЧ, то проверка правильности перемешивания обеспечивает и корректность заполнения бюллетеня в целом. То есть специальной проверки корректности заполнения бюллетеня в целом для данного метода не требуется.

Проведем сравнительный анализ сложности реализации рассмотренных выше методов проверки корректности заполнения бюллетеня избирателем в системе ДЭГ, основанных на проверки логарифмов и на проверке корректности перестановки. Будем полагать, что в обоих случаях для шифрования сообщений используются криптосистемы Эль-Гамаля на эллиптической кривой с одинаковыми параметрами (уравнение кривой, длины ключей, длины криптограмм, длины случайных чисел).

Результаты сравнения представлены в таблице 4.9.

Таблица 4.9. Сравнение методов доказательства корректности заполнения бюллетеня избирателем

	Метод на основе	
	сравнения дискретных логарифмов	проверки корректности перестановки
1) Количество операций, выполняемых на стороне избирателями. Шифрование бюллетеня	3kM	–
2) Количество операций формирования доказательства избирателем	7kM + 5M	16kM + 6M
Всего на стороне избирателя	10kM + 1M	16kM + 6M
Формирование зашифрованных криптограмм		4kM (один раз для всех избирателей)
3) Общее количество операций для проверки доказательства в БЧ	5kM + 3M	3kM + 2M
Всего на стороне БЧ для одного избирателя	5kM + 3M	3kM + 2M
Всего на стороне БЧ для *n* избирателей	*n* (5kM + 3M)	*n* (3kM + 2M) + 4kM

Таблица 4.9 показывает, что сложность формирования доказательства корректности заполнения бюллетеня для k кандидатов составляет 10kM + 1M операций умножения точки эллиптической кривой на число для первого метода и 16kM + 6M для второго метода. Это примерно на 60 % меньше для первого метода. Наоборот, объем вычислений для проверки доказательства корректности заполнения бюллетеня на одного избирателя, проводимых в БЧ, составляет 5kM + 3M операций умножения точки эллиптической кривой на число, для первого метода и 3kM + 2M для второго. Т. е. на проверку бюллетеня во втором методе требуется в 1,67 раза меньше вычислений, чем в первом. Заметим также, что для второго метода сложно организовать контроль правильности заполнения бюллетеня, если при голосовании допускается вариант, когда избиратель может выбирать k кандидатов в диапазоне $m_{min} < m < m_{max}$. Поэтому более универсальным мы можем считать метод проверки корректности заполнения бюллетеня на основе доказательства с

нулевым разглашением секрета, основанном на проверке равенства логарифмов.

Однако, как уже было отмечено выше (п.4.1) данный метод имеет уязвимость, заключающуюся в том, что посторонние лица могут получить информацию об общем числе голосов, отданных избирателем (без конкретизации выбора по кандидатам). Это, на наш взгляд, является недостатком метода.

В приложении 4 привелены Примеры формирования и проверки доказательства корректности заполнения бюллетеня по каждому кандидату на основе криптосхемы Эль -Гамаля на эллиптической кривой.

Разработаем метод проверки корректности заполнения ИзБ для всех кандидатов (проверка в целом) для системы ДЭГ, построенной на основе криптосистемы ЭГ, устраняющий вышеуказанный недостаток и расширяющий класс методов проверки корректности заполнения ИзБ.

4.3. Разработка метода проверки корректности заполнения избирательного бюллетеня в целом на основе доказательства с нулевым разглашением секрета, обеспечивающего скрытность общего числа голосов

Предположим, что ключи шифрования и дешифрования ИзБ сгенерированы, согласно схеме ГШ ЭГ. Избиратель сделал свой выбор, криптограммы (A_i, B_i) ИзБ сформированы и переданы в БЧ. Доказательство корректности ИзБ за каждого кандидата осуществляются так же, как в методе (см.п. 4.1.).

Рассмотрим метод проверки корректности заполнения ИзБ в целом, без раскрытия общего количества поданных голосов. В нем мы используем технику вычислений, применяемую в [110].

Перед процедурой голосования БЧ генерирует величину $A_{k+1} = g^{r_{k+1}}$, $r_{k+1} \in Z_p$, и число $f \in Z_p$ и посылает $(g^{r_{k+1}}, f)$ избирателю. Избиратель после выбора кандидатов и шифрования голосов по каждому кандидату формирует доказательство:

- используя первые части криптограмм $A_1 A_2 \dots A_k$, поданных за каждого кандидата, генерирует числа $y_i, i = 1, \dots, k$, $y_i = \frac{\prod_{j<i} A_j}{\prod_{j>i} A_j}$.

- вычисляет: $U_{D_i} = y_i^{r_i} g^{v_i}$. (4.49)

- находит произведение: $U'_{\sum} = \prod_{i=1}^{k} U_{Di} = \prod_{i=1}^{k} y_i^{r_i} g^{v_i}$. (4.50)

- вычисляет, где $e \in Z_p$, $X' = h^e$, $x = e + \sum_{i=1}^{k} r_i \cdot f$. (4.51)

- посылает в БЧ доказательство: $U'_{\sum}, X'$ и x.

БЧ выполняет проверку доказательства:

Первая проверка:

- вычисляет: $y_{k+1}^{r+1} = A_1 A_2 \dots A_k$. (4.52)

- находит: $U_{Dk+1} = y_{k+1}^{r_{k+1}} \cdot g^{v_{k+1}}$ (4.53)

- вычисляет: $U_{\sum} = U'_{\sum} U_{Dk+1} = g^{\sum_{i=1}^{k} v_i + v_{k+1}}$. (4.54)

Методом подбора находит такое v_{k+1}, при котором $U_{\sum} = 1$

- проверяет неравенство: $m_{min} \le \sum_{i=1}^{n} v_i \le m_{max}$.

Выполнение неравенства свидетельствует о том, что число поданных голосов лежит в заданном интервале.

Вторая проверка:

- проверяет сравнение: $h^x =^? X' \cdot V$. (4.55)

где $V = \left(\prod_{i=1}^{k} B_i \Big/ U_{\sum} \cdot g^{-v_{k+1}}\right)^f$.

Выполнение сравнения свидетельствует о том, что число при формировании доказательства U_{D_i} избиратель использовал те же величины v_i, что и при формировании криптограмм *Bi*.

Дадим пояснение к этой проверке

Запишем: $V = \left(\prod_{i=1}^{k} B_i \Big/ U_{\sum} \cdot g^{-v_{k+1}}\right)^f = \left(h^{\sum r_i} \cdot g^{\sum_{i=1}^{k} v_i} g^{-\sum_{i=1}^{k+1} v_i} \cdot g^{v_{k+1}}\right)^f$.

Если избиратель проголосовал правильно *(m=m')*, то

$\sum_{i=1}^{k} v_i - \left(\sum_{i=1}^{k+1} v_i\right) + v_{k+1} = m - (m' + v_{k+1}) + v_{k+1} = 0$, тогда $V = h^{(\sum r_i) f}$

и $X' \cdot V = h^e \cdot h^{(\sum r_i) f} = h^x$.

В этом методе число m' в явном виде не передается, а число v_{k+1} известно только БЧ, поэтому посторонний пользователь, в том числе ИК, не может узнать общее количество голосов ЗА, содержащихся в бюллетене, что, в свою очередь, повышает безопасность голосования в целом.

Сложность такого метода можно оценить на основе вышеприведенных соотношений, как показано в таблицах 4.10 и 4.11. При оценке сложности учитывались только операции возведения числа в степень по модулю [113].

Таблица 4.10. Оценка сложности формирования доказательства корректности заполнения бюллетеня предлагаемым методом на стороне избирателя

Избиратель		Оценки сложности
Количество операций при формировании доказательства за каждого кандидата:		10 k
Количество операций при формировании доказательства в целом:		
Вычисление:	$y_i = \frac{\Pi_{j<i} A_j}{\Pi_{j>i} A_j}$.	O(k)
	$U_{Di} = y_i^{r_i} g^{v_k}$.	2 k
	$\prod_{i=1}^{k} y_i^{r_i} g^{v_i}$	O(k)
	$X' = h^e$, $x = e + \sum_{i=1}^{k} r_i \cdot f$.	1 O(1)
Всего операций при формировании доказательства в целом:		2 k + 1
Всего операций по избирательному бюллетеню		12k + 1

Таблица 4.11. Оценка сложности проверки доказательства корректности голосования на стороне БЧ

Проверяющий (БЧ)		Оценки сложности
Количество операций по проверке доказательства ИзБ за каждого кандидата:		8 k
Количество операций по проверке доказательства ИзБ в целом		
Вычисление	$A_{k+1} = g^{r_{k+1}}$.	1
	$y_{k+1}^{r+1} = A_1 A_2 \dots A_k$	O(k)
	$U_{Dk+1} = y_{k+1}^{r_{k+1}} \cdot g^{v_{k+1}}$.	2
Проверка неравенства	$m_{min} \le \sum_{i=1}^{n} v_i \le m_{max}$	O(m_{max})
Вычисление V	$V = (\Pi_{i=1}^{k} B_i / U_{\sum} \cdot g^{-v_{k+1}})^f$	1
Проверка сравнения	$h^x =^? X' \cdot V$.	O(1)
Всего операций по проверке доказательства ИзБ в целом		4
Количество операций проверки ИзБ за каждого кандидата и в целом:		8 k+4

Следует отметить, что разработанный метод позволяет блокчейн убедиться в том, что избиратель корректно выбрал количество кандидатов из диапазона возможных значений и обеспечивает скрытность общего числа голосов, отданных избирателями, что повышает безопасность системы ДЭГ [113].

В следующем параграфе, проведем анализ сложности реализации рассмотренных выше методов проверки корректности заполнения бюллетеня избирателем в системе ДЭГ.

4.4. Сравнение сложности методов доказательства корректности заполнения избирательного бюллетеня

В таблице 4.12 представлены результаты сравнения сложности вычислений известного (X) [89, 98] и предложенного (Y) методов для избирателя (доказывающей стороны) и БЧ (проверяющей стороны). Оценка сложности вычислений проведена по наиболее трудоемкой операции – возведению числа в степень по mod p [113]. Для n избирателей, принимающих участие в выборах эти значения, очевидно нужно умножить на n.

Таблица 4.12. Сравнение сложности вычислений для двух методов доказательства корректности заполнения бюллетеня

Количество операций для контроля корректности заполнения бюллетеня в целом (для одного избирателя)	Методы	
	X	Y
формирование доказательства избирателем	$10\,k + 1$	$12\,k + 1$
проверки доказательства в БЧ	$8\,k + 3$	$8\,k + 4$

В таблице 4.13 приведены оценки сложности вычислений в БЧ для существующего и предлагаемого методов для разного количества кандидатов и избирателей [113].

Таблица 4.13. Оценки сложности способов контроля корректности заполнения бюллетеня в зависимости от количества кандидатов и избирателей

Количество избирателей	Оценка сложности			
	k=1	k=3	k=5	k=10
	X/Y	X/Y	X/Y	X/Y
1	22 / 25	58 / 65	94 / 105	184 / 205
n	22n / 25n	58n / 65n	94n / 105n	184n / 205n

Как видно из таблиц 4.12 и 4.13, предлагаемый способ на стороне избирателя приблизительно на 20 % сложнее известного, а на стороне БЧ они приблизительно имеют одинаковую сложность. Однако предлагаемый способ является более безопасным, так как в ходе проверки правильности заполнения ИзБ в целом не раскрывается для посторонних лиц [113].

Выводы по 4-й главе

1. Исследованы два метода защиты системы ДЭГ от угрозы неправильного заполнения бюллетеня избирателем. Первый метод основан на доказательстве с нулевым разглашением секрета и реализуется на основе проверки логарифмов. Второй метод проверки корректности заполнения бюллетеня основан на доказательстве корректности «перемешивания» криптограмм бюллетеня с нулевым разглашением секрета. Приведено детальное описание обоих методов при использовании криптосхемы Эль-Гамаля в числовом поле и на эллиптической кривой.
2. Получены оценки сложности вычислений при формировании доказательства корректности заполнения бюллетеня избирателем и оценки сложности проверки доказательства контролирующей стороной. Метод, основанный на доказательстве равенства логарифмов, имеет меньшую сложность вычислений на стороне избирателя по сравнению с методом, основанном на перемешивании голосов избирателей. В тоже время второй метод (метод перемешивания голосов) требует в 1,67 раза меньше вычислений в блокчейне, что становится существенным фактором выбора в пользу второго метода при большом количестве избирателей.

3. Разработан метод проверки корректности заполнения избирательного бюллетеня в целом, который в отличие от известных методов, позволяет контролирующему органу убедиться в том, что избиратель правильно выбрал количество кандидатов из диапазона возможных значений и при этом обеспечивается скрытность суммарного числа голосов в бюллетене, поданном избирателем, тем самым блокируется атака на систему ДЭГ, заключающаяся в анализе и оценке статистики хода голосования до окончания выборов. Проведено сравнение сложности вычислений известного и предложенного методов для избирателя (доказывающей стороны) и БЧ (проверяющей стороны). Сделан вывод, что разработанный метод при примерно одинаковой сложности вычислений в сравнении с известным методом повышает безопасность системы ДЭГ, поскольку в ходе проверки не раскрывается суммарное число голосов, отданных избирателем при голосовании за несколько кандидатов, тем самым обнаруживается и блокируется атака на систему ДЭГ, заключающаяся в анализе и оценке статистики хода голосования до окончания выборов.

ЗАКЛЮЧЕНИЕ

Во многих демократических странах выборы проводятся с использованием традиционных протоколов голосования на основе бумажных бюллетеней или электронных машин для голосования. Однако, такие методы имеют недостатки, особенно с точки зрения безопасности процесса голосования. Возможны такие угрозы: нарушение тайны голосования, нарушение анонимности избирателей, фальсификация результатов выборов, возможность избирательной комиссии использовать голоса избирателей, которые не участвуют в выборах и невозможно гарантировать точность результатов голосования.

Применение интернет технологий существенно изменило многие информационные обмены между людьми и организациями. За последние несколько лет проявился большой интерес к использованию Интернета для обеспечения безопасных и надежных выборов и постепенному переходу к системам дистанционного электронного голосования (ДЭГ). Использование таких технологий на выборах позволяет устранить перечисленные недостатки традиционных систем голосования, а также обеспечить возможность голосования людям из любой точки мира, сохранить свое здоровье, особенно в случае распространения любого типа вирусов.

В настоящее время в арабских государства и, в частности, в республике Ирак применяются традиционные (бумажные) системы голосования. Поэтому разработка принципиального нового подхода к построению системы ДЭГ в этих государствах, в частности, разработка модели и протокола системы ДЭГ является актуальной научной задачей.

Внедрение системы ДЭГ в арабских государствах позволяет устранить недостатки действующей системы голосования (высокая стоимость бумажных бюллетеней, неправильное заполнение бюллетеней, вбрасывание поддельных бюллетеней в удаленные урны для голосования, неудобство голосования для маломобильных инвалидов). Также ДЭГ улучшает избирательный процесс в

целом, повышает доверие избирателей, увеличивает число избирателей за счет тех, кто живет за границей и т.д.

В перспективной системе ДЭГ должны обеспечиваться такие требования безопасности избирательного процесса: аутентификация избирателя, уникальность, тайна голосования, анонимность избирателя, подтверждение голосования и точность голосования.

Перспективная система ДЭГ должна учитывать особенности избирательного процесса на парламентских выборах в арабских государствах, в частности предотвращать (уменьшать) угрозы, связанные с субъективным (человеческого) фактором: исходящим от администрации выборов, влиянием мнения старейшин и религиозны деятелей и т.д.

В диссертации решена актуальная научная задача – разработан научно-методический аппарат для построения современной защищенной системы ДЭГ для арабских государств с учетом особенностей избирательного процесса на основе использования гомоморфного шифрования с распределенным дешифрованием.

Цель исследования, состоящая в обеспечение защищенности от угроз безопасности информации в системе дистанционного электронного голосования на парламентских выборах в республике Ирак и арабских государствах достигнута.

Основные научные результаты диссертационной работы состоят в следующем:

1. При постановке задачи были рассмотрены основные преимущества внедрения ДЭГ на выборах, выделены особенности избирательного процесса на парламентских выборах в арабских государствах, а также перечислены наиболее опасные угрозы, существующие во всех системах ДЭГ.
2. Был проведен анализ существующей системы голосования в Республике Ирак, применяемой на выборах 2021 года, отмечены присущие ей угрозы и недостатки. Как правило, недостатки и угрозы

традиционной системы голосования в основном обусловлены влиянием субъективного фактора и технологией обработки бумажных бюллетеней. Такие недостатки могут быть преодолены с переходом к системам дистанционного электронного голосования.

3. Сформулированы функциональные требования и требования информационной безопасности к системе ДЭГ.
4. Проанализированы принципы построения современных систем дистанционного электронного голосования (ДЭГ), на основе микс-сетей, слепой подписи, гомоморфного шифрования и технологии блокчейн. Проведено их сравнение. Результаты анализа показали, что гомоморфное шифрование обладает рядом преимуществ и поэтому эта схема взята за основу для дальнейшего исследования.
5. Разработана модель перспективной системы дистанционного электронного голосования создана с учетом специфики голосования в арабских странах. В отличие от известных систем ДЭГ предложенная модель строится на основе распределенной сети узлов блокчейна-консорциума (БЧ) с использованием смарт-контрактов. Для каждой провинции создается узел голосования, включающий в себя серверную платформу, состоящую из сервера регистрации; сервера аутентификации; нескольких независимых серверов голосования, предназначенных для генерации ключей и частичного расшифрования бюллетеней. На каждый узел замыкаются избирательные участки и округа провинций. Также на узле голосования провинции есть несколько смарт-контрактов, в которых хранятся зашифрованные голоса избирателей избирательного участка. Такая архитектура системы ДЭГ позволяет реализовать на ней функционирование протокола голосования, обеспечивающего выполнение требований информационной безопасности процесса голосования.
6. Разработан протокол перспективной системы дистанционного электронного голосования разработан с учетом особенностей угроз

системе ДЭГ в арабских странах, основанный на гомоморфном шифровании и распределенном дешифровании, что обеспечивает выполнение требований безопасности информации: тайна волеизъявления; анонимность голосующего; аутентификация избирателя; уникальность и точность голосования, подтверждение факта голосования. Отличается от известных тем, что обеспечивает дополнительную защищенность от атаки, нацеленной на нарушение анонимности избирателя со стороны административного ресурса системы. Это достигается за счет применения распределенного дешифрования, при котором никто из участников системы не имеет доступа к ключу дешифрования.

7. Исследованы два метода защиты системы ДЭГ от угрозы со стороны избирателя, заключающиеся в неправильном заполнении бюллетеня избирателем. Оба метода основаны на алгоритмах «доказательства с нулевым разглашением секрета». Также приведено детальное описание обоих методов с использованием схемы шифрования Эль-Гамаля на основе эллиптической кривой и в поле *GF(p)*.
8. Разработан метод проверки корректности заполнения избирательного бюллетеня в целом, позволяющий контролирующему органу (блокчейну) убедиться в том, что избиратель корректно выбрал количество кандидатов из диапазона возможных значений. Разработанный метод при примерно одинаковой сложности вычислений в сравнении с известным методом, повышает безопасность системы ДЭГ, поскольку в ходе проверки не раскрывается суммарное число голосов, отданных избирателем за несколько кандидатов, тем самым блокируется атака на систему ДЭГ, заключающаяся в анализе и оценке статистики хода голосования до окончания выборов.
9. Перспективными направлениями дальнейших исследований являются

- Разработка программно-аппаратного комплекса для проведения исследований производительности предложенной системы голосования.
- Оценка устойчивости системы ДЭГ к атакам на основе квантового компьютера и разработка мер (методов) обеспечения безопасности системы ДЭГ в этих условиях.

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

ЦИК – центральная избирательная комиссия Ирака.

ИК – избирательная комиссия.

PCOS – электронное устройство для подсчета и сортировки бумажных избирательных бюллетеней.

RTS – электронное устройство для отправки результатов выборов.

ДЭГ – дистанционное электронное голосование.

QR – Штриховой код.

БЧ – блокчейн.

УИК – участковые избирательные комиссии.

МС – микс сети.

РША – криптосистема Райвеста-Шамира-Адлемана.

КС – криптосистема.

ЭГ – Эль-Гамаля.

СП – слепая подпись.

ДО – доски объявлений.

ИН – идентификационный номер.

ГШ – гомоморфное шифрование.

MIT – массачусетский технологический институт.

ЕСИА – единая система идентификации и аутентификации.

ПК – персональный компьютер.

ИКП – избирательная комиссия провинции.

HF – hyperledger fabric.

PoA – подтверждение полномочий.

GF – конечное поле или поле Галуа.

ИзБ – избирательный бюллетень.

ЭК – эллиптическая кривая.

ZKP – доказательствам с нулевым разглашением секрета.

NIZKP – Неинтерактивное доказательство с нулевым знанием.

СПИСОК ЛИТЕРАТУРЫ

1. Chalabi, M. H. E-voting framework for elections in Iraq: MS. Thesis / Chalabi Mohammed Hassan. – Malaysia. – 2014. – 135 p.
2. Rady K. A Passage towards E-voting in Iraq: Investigation for the verification and the security in the electronic voting systems / K. Rady, J. Ubena // SSRN Electronic Journal. – 2012. – pp. 37.
3. Official gazzete of iraq. Independent high electoral commission law [Электронный ресурс] // Al-Waqai Al-iraqiyya. Baghdad. – 2019. Режим доступа: https://www.moj.gov.iq/view.6986/.
4. Alshamary M. Iraq's struggle for democracy / M. Alshamary // Journal of democracy. – Vol. 34. – №. 2. – 2023. – pp. 150-162.
5. Салман В.Д. Модель и протокол перспективной системы дистанционного электронного голосования для Республики Ирак с учетом особенности избирателей системы / В.Д. Салман // Научно-аналитический журнал «Вестник санкт-петербургского университета ГПС МЧС России». – 2023. – № 2. – С. 91-101.
6. Сапронова М. А. Политический процесс в арабских странах: учебное пособие / М. А. Сапронова. – Москва. – 2017. – 312 с.
7. Сапронова М. А. Постреволюционные конституции и институты власти арабских стран (на примере Египта, Марокко и Туниса) / М. А. Сапронова // Политическая наука. – 2012. – №. 3. – С. 179-198.
8. Mursi M. F. On the development of electronic voting: a survey / M. F. Mursi, G. M. Assassa, A. Abdelhafez, K. M. A. Samra // International Journal of Computer Applications. – 2013. – Vol. 61. – №. 16. – pp. 1-12.
9. Hao F., Ryan P. Y. A. (ed.). Real-world electronic voting: Design, analysis and deployment / F. Hao, P. Y. A. Ryan // CRC Press. – 2016. – 461 p.
10. Ikonomopoulos, S. Functional requirements for a secure electronic voting system / S. Ikonomopoulos, C. Lambrinoudakis, D. Gritzalis, S. Kokolakis, K. Vassiliou // Security in the Information Society. IFIP Advances in Information

and Communication Technology. – Vol. 86. – 2002. – pp. 507-519. DOI:10.1007/978-0-387-35586-3_40.

11. Zissis D. Technologies and methodologies for designing secure electronic voting information systems. MS. Thesis / Dimitrios Zissis. – Греция. – 2011. – 257 p.
12. Hussien H. Design of a secured e-voting system / H. Hussien, H. Aboelnaga // International Conference on Computer Applications Technology (ICCAT). – 2013. – pp. 1-5.
13. Schneider A. Survey on remote electronic voting / A. Schneider, C. Meter, P. Hagemeister // arXiv preprint arXiv:1702.02798. – 2017. – pp. 1-10.
14. Butterfield K. Analysis and implementation of internet based remote voting / K. Butterfield, X. Zou // Proceedings of the 11th International Conference on Mobile Ad Hoc and Sensor Systems. – 2014. – pp. 714-719. DOI:10.1109/MASS.2014.134.
15. Алексеев Р. А. Проблемы и перспективы применения электронного голосования и технологии избирательного блокчейна в России и за рубежом / Р. А. Алексеев, А. В. Абрамов / / Гражданин. Выборы. Власть. – 2020. – №. 1. – С. 9-21.
16. Федоров В. И. Дистанционное электронное голосование и явка избирателей: опыт Эстонии и Москвы / В. И. Федоров // Избирательное законодательство и практика. – 2019. – Т. 4. – С. 37.
17. Норберт К. Электронное голосование и демократия в Европе / К. Норберт // Политическая наука. – 2007. – №. 4. – С. 123-144.
18. Минтусов И. Е., Гуляев Д. С. Дистанционное электронное голосование в странах англосаксонской системы: США, Австралия, Великобритания. Почему голосование ДЭГ не прижилось? / И. Е. Минтусов, Д. С. Гуляев // Гражданин. Выборы. Власть. – 2022. – №. 1 (23). – С. 122.
19. Ерохина О. В. Технологии электронного голосования в России / О. В. Ерохина // Вестник университета. – 2019. – №. 11. – С. 5-11.

20. Eflova M. Y. Experience of remote E-voting in political elections in Russia/ M. Y. Eflova, A. I. Dudochnikov, I. I. Shamsutdinova // res militaries. – 2022. – Vol. 12. – №. 2. – pp. 2468-2477.
21. Требования к системе дистанционного электронного голосования (интернет-голосования), разрабатываемой ЦИК России. [Электронный ресурс] // https://st.golosinfo.org.
22. Gritzalis D. A. Principles and requirements for a secure e-voting system / D. A. Gritzalis // Computers & Security. – 2002. – Vol. 21. – №. 6. – pp. 539-556.
23. Volkamer M. Requirements and evaluation procedures for e-voting / M. Volkamer, M. McGaley // The second international conference on availability, reliability and security (ARES'07). – 2007. – pp. 895-902.
24. Alamleh H. Analysis of the design requirements for remote internet-based E-voting systems / H. Alamleh, A. A. S. AlQahtani // IEEE World AI IoT Congress (AIIoT). 2021. – pp. 0386-0390. DOI: 10.1109/AIIoT52608.2021.9454194.
25. Schmidt, A. Developing a legal framework for remote electronic voting / A. Schmidt, D. Heinson, L. Langer, Z. Opitz-Talidou, Ph. Richter, M. Volkamer, J. Buchmann // E-voting and identity: Second international conference, VOTE-ID. – Springer. – 2009. – pp. 92-105. DOI.org/10.1007/978-3-642-04135-8_6.
26. Puiggali, J. Remote voting schemes: A comparative analysis / J. Puiggali, R. Morales // E-voting and identity: First International conference, VOTE-ID. – 2007. – pp. 16-28. DOI.org/10.1007/978-3-540-77493-8_2.
27. Коржик В.И., Яковлев В.А. Основы криптографии: учебное пособие / В.И. Коржик, В.А. Яковлев // Санкт Петербург.: ИЦ Интермедия. – 2016. – 296 с.
28. Mateu V., Sebé F., Valls M. Constructing credential-based E-voting systems from offline E-coin protocols / V. Mateu, F. Sebé, M. Valls // Journal of Network and Computer Applications. – 2014. – Vol. 42. – pp. 39–44. DOI:10.1016/j.jnca.2014.03.009.

29. Aziz A. A., Qunoo H. N., Samra A. A. Using homomorphic cryptographic solutions on e-voting systems / A. A. Aziz, H. N. Qunoo, A. A. Samra // International Journal of Computer Network and Information Security. – 2018. –Vol. 12. –№. 1. – pp. 44 59.
30. Moayed M. J., Ghani A. A. A., Mahmod R. A survey on cryptography algorithms in security of voting system approaches / M. J. Moayed, A. A. A. Ghani, R. Mahmod // International conference on computational sciences and its Applications. – 2008. – pp. 190-200.
31. Alam K. M. R., Tamura S. Electronic voting -scopes and limitations / K. M. R. Alam, S. Tamura // International conference on informatics, electronics & vision (ICIEV). – 2012. – pp. 525-529.
32. H. Li, A. R. Kankanala and X. Zou. A taxonomy and comparison of remote voting schemes / H. Li, A. R. Kankanala, X. Zou // 23rd International Conference on Computer Communication and Networks (ICCCN). – China. – 2014. – pp. 1-8. DOI: 10.1109/ICCCN.2014.6911807.
33. Furukawa J., Mori K., Sako K. An implementation of a Mix-Net based network voting scheme and its use in a private organization / J. Furukawa, K. Mori, K. Sako // Towards trustworthy elections: New directions in electronic voting. – Springer. – Berlin. – 2010. – pp. 141-154. DOI:10.1007/978-3-642-12980-3_8.
34. Park C., Itoh K., Kurosawa K. Efficient anonymous channel and all/nothing election scheme / C. Park, K. Itoh, K. Kurosawa // Advances in cryptology—EUROCRYPT'93: Workshop on the theory and application of cryptographic techniques. – Springer. – 1994. – pp. 248-259.
35. Chaum D.L. Untraceable electronic mail, return addresses, and digital pseudonyms / D.L. Chaum // Communications of the ACM. – 1981. – Vol. 24. – №. 2. – pp. 84-90.
36. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms / T. ElGamal // IEEE transactions on information theory. – 1985. – Vol. 31. – №. 4. – pp. 469-472.

37. Czeslaw K. A new approach to the elgamal encryption scheme / K. Czeslaw // International journal of applied mathematics and computer Science. – 2004. – Vol. 14. – №. 2. – pp. 265-267.
38. Chaum D. Blind Signature System / D. Chaum // Advances in cryptology: Proceedings of crypto 83. – Boston. – Springer. – 1983. Vol.2. – pp. 199-203.
39. Rivest R.L., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public- Key Cryptosystems / R.L. Rivest, A. Shamir, L. Adleman // Communications of the ACM. – 1978. – Vol. 21. – №. 2. – pp. 120-126.
40. Ordonez A.J., Gerardo B.D., Medina R.P. Digital signature with multiple signatories based on modified ElGamal cryptosystem / A.J. Ordonez, B.D. Gerardo, R.P. Medina // 5th International Conference on Business and Industrial Research (ICBIR). – 2018. – pp. 89-94.
41. Fujioka A., Okamoto T., Ohta K. A practical secret voting scheme for large scale elections / A. Fujioka, T. Okamoto, K. Ohta // Advances in Cryptology—AUSCRYPT'92: Workshop on the theory and application of cryptographic techniques Gold Coast, Queensland, Australia. – Springer. – Berlin. – 1993. – pp. 244-251. DOI:10.1007/3-540-57220-1_66.
42. Ibrahim S., Kamat M., Salleh M., Aziz S.R.A. Secure E-voting with blind signature / S. Ibrahim, M. Kamat, M. Salleh, S.R.A. Aziz // 4th National Conference of Telecommunication Technology. – 2003. – pp. 193-197. DOI:10.1109/NCTT.2003.1188334.
43. Jabbar I., Alsaad N.S. Design and implementation of secure remote E-voting system using homomorphic encryption / I. Jabbar, N.S. Alsaad // International Journal of Network Security. – 2017. – Vol. 19. – №. 5. – pp. 694-703.
44. Huszti A. A homomorphic encryption-based secure electronic voting scheme /A. Huszti // Publicationes mathematicae. – 2011. – Vol. 79. – №. 4. – pp. 479-496.

45. Fontaine C. A Survey of homomorphic encryption for nonspecialists / C. Fontaine, F. Galand // EURASIP Journal on information security. – 2007. – Vol. 2007. – pp. 1-10.
46. Bhumika P., Dharmendra B. Homomorphic Encryption: Privacy preserving amicable E-voting system / P. Bhumika, B. Dharmendra // International journal of computer sciences and engineering. – 2019. – Vol. 7. – pp. 46–50. DOI:10.26438/ijcse/v7i12.4650.
47. Suwandi R., Nasution S. M., Azmi F. Secure E-voting system by utilizing homomorphic properties of the encryption algorithm / R. Suwandi, S. M. Nasution, F. Azmi // Telkomnika (Telecommunication Computing Electronics and Control). – 2018. – Vol. 16. – №. 2. – pp. 862-867. DOI:10.12928/telkomnika.v16i2.8420.
48. Салман В.Д. Анализ гомоморфных криптосистем Бенало и Пэйе для построения системы электронного голосования / В.Д. Салман // Труды учебных заведений связи. – 2021. – Т. 7. – №. 2. – С. 102-109.
49. Segundo M.T, Luis J. Ch., Javier G.O., Luis E. M. A Homomorphic encryption approach in a voting system in a distributed architecture / M.T. Segundo, J. Ch. Luis, G.O. Javier, E. M. Luis // IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS). – 2020. – pp. 206-210.
50. Tannishk Sh. E-Voting using Homomorphic Encryption Scheme / Sh. Tannishk // International Journal of Computer Applications. – 2016. – Vol. 5. – pp. 14-16.
51. Трубей А.И. Гомоморфное шифрование: безопасность облачных вычислений и другие приложения (обзор) / А.И. Трубей // Информатика. – 2016. – №. 1. – С. 90-101.
52. Okediran O. O. A comparative study of generic cryptographic models for secure electronic voting / O. O. Okediran, E. O. Omidiora, S. O. Olabiyisi, R. A. Ganiyu // British journals of science. – 2011. – Vol. 1. – №. 2. – pp. 135-142.

53. Сергиенко Е.Н. Криптографические методы обеспечения конфиденциальности электронных выборов / Е. Н. Сергиенко, А. С. Чурилов, С. В. Черников // Проблемы информатики в образовании, управлении, экономике и технике. – 2017. – С. 51-56.
54. Kannan B. A Homomorphic crypto system for electronic election schemes/ B. Kannan, M. Jayanthi // Circuits and Systems. – 2016. – Vol. 7. – №. 10. – pp. 3193-3203. DOI: 10.4236/cs.2016.710272.
55. Morris L. Analysis of partially and fully homomorphic encryption/ L. Morris // Rochester Institute of Technology. – 2013. – Vol. 10. – pp. 1-5.
56. Benaloh J.C. Verifiable Secret-Ballot Elections: MS. Thesis / Josh Daniel Cohen Benaloh. – Yale University. – 1996. – 134 p.
57. Paillier P. Public-key cryptosystems based on composite degree residuosity classes/ P. Paillier // International conference on the theory and applications of cryptographic techniques. – Berlin. – 1999. – pp. 123–139.
58. Baudron O. Practical Multi-Candidate Election System / O. Baudron, P. Fouque, D. Pointcheval, J. Stern, G. Poupard // Proceedings of the twentieth annual ACM symposium on Principles of distributed computing. – 2001. – pp. 274–283. DOI:10.1145/383962.384044.
59. Ryan P.Y.A. Pret a Voter with Paillier encryption / P.Y.A. Ryan // Mathematical and Computer Modelling. – 2008. – Vol. 48. – pp 1646-1662.
60. Ayed A. B. A conceptual secure blockchain-based electronic voting system / A. B. Ayed // International journal of network security & its applications. – 2017. – Vol. 9. – №. 3. – pp. 01-09. DOI: 10.5121/ijnsa.2017.9301.
61. Спиркина А. В. Научные аспекты структурно-параметрического моделирования блокчейн-систем / А. В. Спиркина Труды учебных заведений связи. – 2021. – Т. 7. – №. 1. – С. 122-131.
62. Dagher, G. BroncoVote: Secure Voting System Using Ethereum's Blockchain / G.G. Dagher, PB. Marella, M. Milojkovic, J. Mohler // Proceedings of the 4th International Conference on Information Systems Security and Privacy. – 2018. – pp. 96-107. DOI: 10.5220/0006609700960107.

63. Khan K. M. Secure digital voting system based on blockchain technology / K. M. Khan, J. Arshad, M. M. Khan // International journal of electronic government research (IJEGR). – 2018. – Vol. 14. – №. 1. – pp. 53-62. DOI: 10.4018/IJEGR.2018010103.
64. Hsiao, J.H. Decentralized E-voting systems based on the blockchain technology/ J.H. Hsiao, R. Tso, C.M. Chen, M. Wu // In advances in computer science and ubiquitous computing: CSA-CUTE 17. –2018. – pp. 305-309. DOI:10.1007/978-981-10-7605-3_50.
65. Prasetyadi G. C. Blockchain-based electronic voting system with special ballot and block structures that complies with Indonesian principle of voting / G. C. Prasetyadi, A. B. Mutiara, R. Refianti // International journal of advanced computer science and applications. – 2020. – Vol. 11. – №. 1. – pp. 164-170.
66. Hjálmarsson F. Blockchain-Based E-Voting System / F. Hjálmarsson, G.K. Hreiðarsson, M. Hamdaqa, G. Hjálmtýsson // IEEE 11th International conference on cloud computing (CLOUD). – USA. – 2018. – pp. 983-986, DOI: 10.1109/CLOUD.2018.00151.
67. Yu B. Platform-Independent Secure Blockchain-Based Voting System // B. Yu, K. L. Joseph, A. Sakzad, S. Nepal, R. Steinfeld, P. Rimba, H. A. Man // Information Security: 21st International conference, ISC. – UK. – Springer International Publishing. – 2018. – pp. 369-386. DOI:10.1007/978-3-319-99136-8_20.
68. Mingxiao D. A review on consensus algorithm of blockchain/ D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, C. Qijun // IEEE international conference on systems, man, and cybernetics (SMC). – 2017. – pp. 2567-2572. DOI: 10.1109/SMC.2017.8123011.
69. Taş, R. A Systematic review of challenges and opportunities of blockchain for E-voting/ R. Taş, Ö.Ö. Tanrıöver // Symmetry. – 2020. – Vol. 12. – №. 8. – pp. 1328. DOI:10.3390/sym12081328.

70. Dib O. Consortium blockchains: Overview, applications and challenges / O. Dib, K. L. Brousmiche, A. Durand, E. Thea, E. B. Hamida // International journal of advanced Telecommuting. – 2018. – Vol. 11. – №. 1. – pp. 51-64.
71. Kshetri N. Blockchain-enabled e-voting / N. Kshetri, J. Voas // IEEE Software. – 2018. – Vol. 35. – №. 4. – pp. 95-99.
72. Storublevtcev N. Cryptography in blockchain / N. Storublevtcev // Computational science and its applications – ICCSA: 19th International conference. – Saint Petersburg. – Russia. – 2019. – Springer International Publishing. – pp. 495-508.
73. Sun X. et al. A simple voting protocol on quantum blockchain / X. Sun, Wang Q., Kulicki P., Sopek M. // International journal of theoretical physics. – 2019. – Vol. 58. – pp. 275-281.
74. Kiktenko E. O. et al. Quantum-secured blockchain / E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.I. Lvovsky, A.K. Fedorov // Quantum science and technology. – 2018. – Vol. 3. – №. 3. – pp. 1-9.
75. Sun X. et al. Towards quantum-secured permissioned blockchain: Signature, consensus, and logic / X. Sun, Wang Q., Kulicki P., Sopek M. // Entropy. – 2019. – Vol. 21. – №. 9. – pp. 1-15.
76. Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring / P. Shor // Proceedings 35th annual symposium on foundations of computer science. – 1994. – pp. 124-134.
77. Высоцкая В. В., Чижов И. В. Проект методических рекомендаций для стандартизации постквантовой электронной подписи на основе кодов, исправляющих ошибки / В. В. Высоцкая, И. В. Чижов. Рабочие материалы.
78. Петренко А. Квантово–устойчивый блокчейн. – СПБ.: Питер. –2023. – 320 с.:ил. ISBN 9785-4461-2357-5.

79. Cachin C. Architecture of the hyperledger blockchain fabric / C. Cachin // Workshop on distributed cryptocurrencies and consensus ledgers. – 2016. – Vol. 310. – №. 4. – pp. 1-4.
80. Mohan, V. Apollo. A secure, anonymized voting system using the Paillier cryptosystem / V. Mohan, R. Sridhar, L. Sun, K. Zhu // Project Report. – 2016. – pp. 1-12
81. Adida B. Helios: Web-based open-audit voting / B. Adida // USENIX security symposium. – 2008. – Vol. 17. – pp. 335-348.
82. Alonso L.P. E-Voting system evaluation based on the council of Europe recommendations: Helios voting / L.P. Alonso, M. GASCÓ, D.Y.M. del BLANCO, J.Á.H. Alonso, J. Barrat, H.A. Moreton // IEEE Transactions on emerging topics in computing. – 2018. – Vol. 9. – №. 1. – pp. 161-173. DOI:10.1109/TETC.2018.2881891.
83. Estehghari S., Desmedt Y. Exploiting the client vulnerabilities in internet E-voting systems: Hacking Helios 2.0 as an example / S. Estehghari, Y. Desmedt // Electronic voting technology workshop trustworthy elections (EVT/WOTE 10). – 2010. – pp.1-13.
84. Blum M. Non-interactive zero-knowledge and its applications / M. Blum, P. Feldman, S. Micali // Providing sound foundations for cryptography: On the work of Shafi Goldwasser and Silvio Micali. – 2019. – pp. 329-349. DOI:10.1145/62212.62222.
85. Huqing W. Research on Zero-Knowledge Proof Protocol / W. Huqing, S. Zhixin // International journal of computer science issues (IJCSI). – 2013. – Vol. 10. – №. 1. – pp 194-200.
86. Михайлович К. А. Блокчейн технологии в бухгалтерском учёте и аудите: дис.магис. 38.04.01 / Кукин Александр Михайлович. – 2023. – 112с.
87. Killer C. Provotum: A Blockchain-based and End-to-end verifiable remote electronic voting system / C. Killer, B. Rodrigues, E. J. Scheid, M. Franco, M. Eck, N. Zaugg, B. Stiller // IEEE 45th Conference on local computer networks (LCN). – 2020. – pp. 172-183. DOI:10.1109/LCN48667.2020.9314815.

88. Cramer R. A Secure and optimally efficient multi-authority election scheme / R. Cramer, R. Gennaro, B. Schoenmakers // European transactions on telecommunications. – 1997. – Vol. 8. – №. 5. – pp. 481-490. DOI:10.1007/3-540-69053-0_9.
89. Chaum D., Pedersen T.P. Wallet databases with observers / D. Chaum, T.P. Pedersen // Annual international cryptology conference. – Berlin. – Springer – 1992. – pp. 89-105.
90. Fouque P. A., Poupard G., Stern J. Sharing decryption in the context of voting or lotteries / P. A. Fouque, G. Poupard, J. Stern // Financial cryptography. – Springer. – Berlin. – 2001. – pp. 90-104.
91. Белоусов С. А. Вопросы использования электронного голосования при проведении заседаний диссертационных советов / С. А. Белоусов, В. Е. Николаев / /Правовая политика и правовая жизнь. – 2021. – №. 4. – С. 127-138.
92. Криптовече. [Электронный ресурс] // Режим доступа: https://s3.dtln.ru/unti-prod-people/file/presentation/project/b1kcn3vsvd.pdf.
93. Программно-техничческий комплекс, обеспечивающий электронное голосование избирателей (участников референума) вне зависиммомти от места их нахождения. [Электронный ресурс] // Описание ПТК ДЭГ. Режим доступа: https://evoting.digitaldem.ru/wpcontent/uploads/sites/2/2021/07/ptkdeg_general_description_2021-07-15.pdf.
94. Shamir A. How to share a secret / A. Shamir // Communications of the ACM. – 1979. – Vol. 22. – №. 11. – pp. 612-613.
95. Boruah D. Implementation of ElGamal elliptic curve cryptography over prime field using C / D. Boruah, M. Saikia // International conference on information communication and embedded systems. – 2014. – pp. 1-7. DOI:10.1109/ICICES.2014.7033751.

96. Caelli W. J. PKI, elliptic curve cryptography, and digital signatures / W. J. Caelli, E. P. Dawson, S. A. Rea // Computers & Security. – 1999. – Vol. 18. – №. 1. – pp. 47-66. DOI:10.1016/S0167-4048(99)80008-X.
97. Kapoor V. Elliptic curve cryptography / V. Kapoor, V.S. Abraham, R. Singh // Ubiquity. – 2008. – pp. 1-8. DOI:10.1145/1378355. 1378356.
98. Cramer R. Proofs of partial knowledge and simplified design of witness hiding protocols / R. Cramer, I. Damgård, B. Schoenmakers // Annual International Cryptology Conference. – Berlin. – Springer. – 1994. – pp. 174-187.
99. Истомин Е. П. Некоторые аспекты применения блокчейн-технологий в современной экономике / Е. П. Истомин, С. А. Кирсанов, Д. В. Леонтьев // Информационные технологии и системы: управление, экономика, транспорт, право. – 2020. – №. 1. – С. 88-102.
100. Яковлев В.А. Исследование системы электронного голосования на основе гомоморфного шифрования с распределенным дешифрованием / Яковлев В.А., Салман В.Д., Шевцов Д.С. // Защищенные системы связи. – 2022. – Т. 2. – С. 10.
101. Koblitz, N. Algebraic aspects of cryptography/ N. Koblitz, A. J. Menezes, Y. H. Wu, R. J. Zuccherato // Springer. – 1998. – Vol. 198. – pp. 1-17. DOI:10.1007/978-3-662-03642-6.
102. Galbraith S. D. Mathematics of public key cryptography/ S. D. Galbraith // – Cambridge University Press. – 2012. – 564 p.
103. Silverman J.H. An Introduction to mathematical cryptography / J.H. Silverman, J. Pipher, J. Hoffstein // Springer. – New York. – 2008. – Vol. 1. – 149 p. DOI: 10.1007/978-0-387-77993-5.
104. Yan S. Y. Computational number theory and modern cryptography/ S. Y. Yan. – John Wiley & Sons. – 2013. – 417 p.
105. Damgård, I. The Theory and implementation of an electronic voting system / I. Damgård, J. Groth, G. Salomonsen // Secure electronic voting. – 2003. – pp. 77-99. DOI:10.1007/978-1-4615-0239-5_6.

106. Cramer R. Multi-authority secret-ballot elections with linear work / R. Cramer, M. Franklin, B. Schoenmakers, M. Yung // International conference on the theory and applications of cryptographic techniques. – Berlin. – 1996. – pp. 72-83. DOI:10.1007/3-540-68339-9_7.

107. Hao F. Anonymous voting by two-round public discussion/ F. Hao, P.Y.A. Ryan, P. Zieliński // IET Information security. – 2010. – Vol. 4. – №. 2. – pp. 62-67. DOI:10.1049/iet-ifs.2008.0127.

108. Mateu V. A hybrid approach to vector-based homomorphic tallying remote voting / V. Mateu, J.M. Miret, F. Sebé // International journal of information security. – 2016. – Vol. 15. – pp. 211-221. DOI:10.1007/s10207-015-0279-8.

109. Peng K. An efficient shuffling based E-voting scheme/ K. Peng // Journal of systems and software. – 2011. – Vol. 84. – №. 6. – pp. 906-922. DOI:10.1016/j.jss.2011.01.001.

110. Seol S. An Efficient open vote network for multiple candidates / S. Seol, H. Kim, J.H. Park // IEEE Access. – 2022. – Vol. 10. – pp. 124291-124304. DOI:10.1109/ACCESS.2022.3224798.

111. Yang X. A secure verifiable ranked choice online voting system based on homomorphic encryption / X. Yang, X. Yi, S. Nepal, A. Kelarev, F. Han // IEEE Access. – 2018. – Vol. 6. – pp. 20506-20519. DOI:10.1109/ACCESS.2018.2817518.

112. Яковлев В.А. Методы защиты от угрозы неправильного заполнения избирательного бюллетеня в системе дистанционного электронного голосования / В.А. Яковлев, В.Д. Салман // Труды учебных заведений связи. – 2023. – Т. 9. – №. 2. – С. 128-142.

113. Салман В.Д. Способ защиты от атаки некорректного заполнения избирательного бюллетеня в системе дистанционного электронного голосования / Яковлев В.А., Салман В.Д. // Труды учебных заведений связи. – 2023. – Т. 9. – № 4. – С. 95–111. DOI:10.31854/1813-324X-2023-9-4-95-111.

114. Peng K. Modification and optimization of a shuffling scheme: Stronger security, formal analysis and higher efficiency/ K. Peng, E. Dawson, F. Bao // International journal of information security. – 2011. – Vol. 10. – pp. 33-47. DOI:10.1007/s10207-010-0117-y.

ПРИЛОЖЕНИЕ 1. АКТ О ВНЕДРЕНИИ РЕЗУЛЬТАТОВ ДИССЕРТАЦИОННОЙ РАБОТЫ

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Санкт-Петербург

УТВЕРЖДАЮ
Первый проректор-проректор по учебной работе
к.т.н. _____ А. В. Абилов
«23» 09 2023 г.

Акт

об использовании результатов диссертационной работы
Салман Васан Давуд Салман

«Разработка и исследование модели и протокола защищенной системы дистанционного электронного голосования для арабских государств с парламентской правовой системой (на опыте и примере республики Ирак)»

Настоящий Акт составлен в том, что результаты диссертационной работы Салман Васан Давуд Салман, а именно:

- Модель системы дистанционного электронного голосования (ДЭГ) для арабских государств с парламентской правовой системой, в том числе для Республики Ирак, основанная на распределенной сети блокчейн-узлов (БЧ);
- Протокол функционирования перспективной системы ДЭГ на основе гомоморфного шифрования с распределенным дешифрованием, учитывающий специфические угрозы в ДЭГ арабских государств и обеспечивающий повышенную защищенность от угроз, связанных с человеческим фактором;
- Метод проверки корректности заполнения бюллетеня избирателем, обеспечивающий скрытность волеизъявления избирателя по отдельным кандидатам и по всем кандидатам в целом;

используются кафедрой защищенные системы связи федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» в учебном процессе на старших курсах обучения бакалавров по направлению подготовки 10.03.01 «Информационная безопасность» по дисциплине «Криптографические протоколы» (рабочая программа дисциплины, регистрационный № 23.05/216-Д) при чтении курсов лекций, проведении практических занятий и лабораторных работ.

Председатель комиссии:

Заведующий кафедрой ЗСС, к.т.н., доцент — Красов Андрей Владимирович

Члены комиссии:
к.т.н., доцент — Ушаков Игорь Александрович

к.т.н., доцент — Кушнир Дмитрий Викторович

جمهورية العراق
مفوضية العليا المستقلة للانتخابات
الإدارة الانتخابية

بسم الله الرحمن الرحيم

he Independent High Electoral Commission
كۆمیسیۆنی بالای سەربەخۆی هەڵبژاردنەکان

العدد: ٦٥٥٣/٦/٥٣
التاريخ: ٢٠٢٣/١١/٣٠

الى / وزارة التعليم العالي والبحث العلمي / دائرة البعثات والعلاقات الانتخابية
قسم شؤون الدارسين / شعبة أوروبا الشرقية

م / الاستفادة من البحث

السلام عليكم ورحمة الله وبركاته ...

كتابكم بالعدد (ص ب /٢٤/ ٣٩٠٨١) في ٢٠٢٣/١١/١٤ المتضمن بيان رأي مفوضيتنا عن مدى الاستفادة من موضوع بحث طالبة الزمالة الدراسية السيدة (**وسن داود سلمان**) الموسوم (**تطوير النظام الانتخابي الحالي من ورقي الى الكتروني باستخدام التقنيات الحديثة والتشفير**) .

نؤيد لكم ان البحث أعلاه يدخل ضمن عمل مفوضيتنا باستخدام التطور التكنولوجي في الانتخابات وتحويلها من العمل الانتخابي الورقي الى الالكتروني في التسجيل والاقتراع واعتماده في المشاريع المستقبلية في عمل مفوضيتنا .

مع التقدير

مهند فاضل عباس
معاون رئيس الإدارة الانتخابية
للشؤون الفنية
٢٠٢٣/١١/٣٠

صورة عنه الى:
- مكتب السيد رئيس الادارة الانتخابية / للتفضل بالاطلاع ... مع التقدير .
- الامانة العامة لمجلس المفوضين / مكتب السيد الامين العام / للتفضل بالاطلاع ... مع التقدير .
- مكتب السيد معاون رئيس الادارة الانتخابية للشؤون الفنية / للتفضل بالاطلاع ... مع التقدير .
- مكتب السيد معاون رئيس الادارة الانتخابية للشؤون الادارية والمالية / للتفضل بالاطلاع ... مع التقدير .
- الدائرة الادارية والمالية / للتفضل بالاطلاع ... مع التقدير .
- دائرة العمليات وتكنولوجيا المعلومات / شعبة الإجراءات والتدريب / كتابكم بالعدد (د/٦٢٦) في ٢٠٢٣/١١/٢٧/ للتفضل بالاطلاع ... مع التقدير .
- قسم التدقيق والرقابة الداخلية / للتفضل بالاطلاع ... مع التقدير .

٩٩٦٨
١١/٣٠
الحسابات الرسمية للمفوضية

حنان ٢٠٢٣/١١/٢٩

Перевод с арабского языка на русский язык

Республика Ирак
Независимая Высшая избирательная комиссия
Избирательная администрация

№ АД\6\6553
Дата: 30\11\2023

Министерство высшего образования и научных исследований \
отдел миссий и культурных связей \
отдел по делам студентов \ отдел Восточноевропейский

АКТ
об использовании результатов диссертационной работы

На Ваш номер (сп\ 24\ 39081) от 14\11\2023 сообщаем мнение нашей комиссии о значимости диссертационной работы Салман Васан Давуд Салман на тему «Разработка и исследование модели и протокола защищенной системы дистанционного электронного голосования для арабских государств с парламентской правовой системой (на опыте и примере Республики Ирак».

Мы подтверждаем, что диссертационная работа является составной частью тематики работ, проводимых нашей комиссией по применению современных выборных технологий при переходе от традиционного избирательного процесса к системе дистанционного голосования и особенно в части процедур регистрации и голосования избирателей. Также целесообразно внедрение результатов работы в будущие проекты в рамках деятельности нашей комиссии.

С признательностью

Подпись:

Муханнад Фадель Аббас

Помощник начальника избирательного отдела по технике

30\11\2023 Печать: Независимая Высшая избирательная комиссия

Подпись:

29\11

Копии акта для:

- Офис президента избирательного отдела \ к ознакомлению \с признательностью.
- Офис генерального секретариата совета \ генерального секретаря\ к ознакомлению \с признательностью.
- Офис помощника начальника избирательного отдел по техническим делам \ к ознакомлению \с признательностью.
- Офис помощника начальника избирательного отдел по финансам и управлению\ ознакомлению \ с признательностью.
- Финансовый и административный отделы \ к ознакомлению \ с признательностью.
- Отдел операций и информационных технологий \ Отдел процедур и обучения\ на Ваш номер (626\д) в 27\11\2023\ к ознакомлению \ с признательностью.
- Отдел аудита и внутреннего контроля \к ознакомлению \ с признательностью.

9928
30\11
QR-код: Официальные веб-сайты

Печать - Ханан 29\11\2023

----------Конец перевода документа----------

ПРИЛОЖЕНИЕ 2. Обзор блокчейн

Одним из принципов построения современных систем ДЭГ является использование блокчейн (БЧ), суть которого заключается в распределенном хранении информации на электронных носителях без возможности ее изменения [60, 61]. Проведем краткий обзор блокчейн-технологий [60 – 69, 71-72, 86, 99].

Блокчейн — это распределенная база данных, способная хранить и обрабатывать данные в равной степени на множестве компьютеров. Принцип работы БЧ основан на создании блоков информации и последующем их цепочном связывании с помощью криптографических методов [62 - 69].

Существует много различных криптографических алгоритмов, используемых на разных блокчейн-платформах, но большинство из них относятся к одной из основных категорий: алгоритмы хеширования (SHA-256) и асимметричные алгоритмы шифрования и цифровая подпись [69].

Например, блокчейн Ethereum использует следующие криптографические алгоритмы [71]:

- ECDSA (Elliptic Curve Digital Signature Algorithm);
- Эллиптическая кривая secp256k1 с генератором G;
- NIST SP 800-56 Concatenation Key Derivation Function;
- Код аутентификации сообщения на основе хеша (HMAC) с использованием хэш-функции SHA-256;
- Функция шифрования AES-128 в режиме CTR.

Каждый блок в цепочке содержит необходимую информацию в виде транзакций, которые добавляются в блок. Когда блок заполнен, он связывается с предыдущим блоком в цепочке путем применения криптографических хэш-функций, что обеспечивает целостность и неизменность всех предыдущих блоков в цепочке. Данная процедура делает невозможным внесение изменений в имеющиеся данные, что, в свою очередь, делает блокчейн надежным и безопасным способом хранения и передачи информации [61]. БЧ был

разработан как технология для работы с криптовалютами. Например, блокчейн Биткоин позволяет совершать транзакции без участия посредников - банков. Однако, блочейн может быть использован в различных областях информационных технологий, таких как голосование, управление данными в медицинской сфере, регистрация прав на недвижимость, и многих других [60, 61]. Одной из ключевых особенностей блокчейна является его децентрализованность, что подразумевает отсутствие центрального управляющего органа. Все узлы сети имеют равные права и одинаковый доступ к информации, что делает блокчейн прозрачным и надежным [66]. БЧ включает в себя такие понятия: узел, блок, транзакция.

Узел — это устройство в блокчейн-сети, позволяющее ему функционировать [61- 66]. Данные о транзакциях записываются распределенной сетью специальных компьютеров со всего мира, называемых узлами.

Блок – представляет собой некий контейнер, который объединяет транзакции для включения в публичный реестр. Каждый блок в блокчейне имеет уникальный хеш, который служит его идентификатором и связан с предыдущим в цепочке. Блок состоит из заголовка, содержащего метаданные, а также тело из списка транзакций. Структура и размер блока зависят от реализации. Максимальное количество транзакций, которое может содержать блок, зависит от размера блока и размера каждой транзакции [61 - 66]. На рисунке 1 представлена структура стандартного блока.

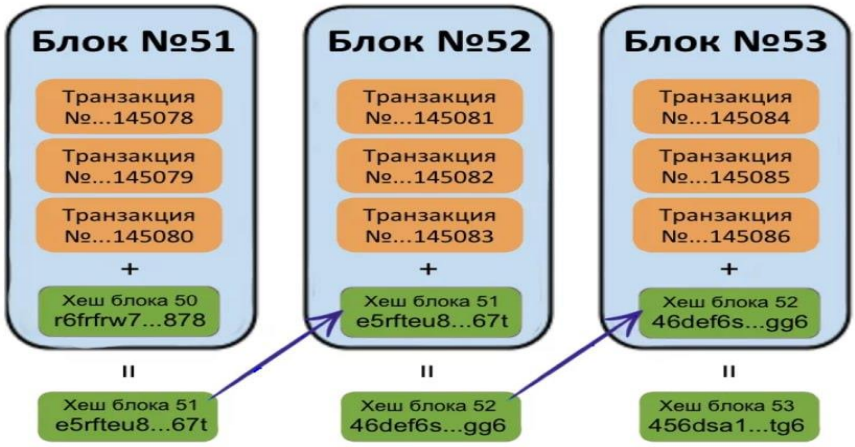

Рис. 1. Структура блока

Транзакция — это запись в распределенном реестре (блокчейне), которая содержит информацию о перемещении, например, криптовалютных единиц (биткоинов) между участниками сети. Транзакции в блокчейн-сети осуществляются между криптовалютными кошельками, каждый из которых имеет свою собственную цифровую подпись. В блокчейне каждая транзакция представлена в виде уникального хэша, который служит ее идентификатором [72]. Она содержит следующие элементы [61- 66]:

- Входы: ссылки на выходы предыдущих транзакций, которые используются для определения суммы денежных средств, которые должен отправить отправитель.
- Выходы: указание того, куда и сколько криптовалютных единиц должен отправить отправитель.
- Подписи: специальные данные, которые используются для подтверждения транзакции и защиты от мошенничества.

Когда транзакция создается и отправляется, она распределяется по всей сети блокчейна, где она подтверждается и записывается в блок. Запись транзакции в блок является неотменяемой операцией и означает, что перемещение криптовалютных единиц было окончательно завершено.

БЧ работает следующим образом [60 - 69]:

- Каждый блок содержит информацию о выполненных транзакциях, временную метку и уникальный код (хеш).
- Каждый блок связан с предыдущим блоком с помощью уникального кода предыдущего блока, что образует цепочку блоков.
- БЧ состоит из множества копий, хранящихся на компьютерах участников сети. Это означает, что БЧ не имеет центрального узла контроля, и данные защищены от взлома или изменений.
- Узлы могут добавлять новые блоки к цепочке только в том случае, если они выполняют сложные математические вычисления, которые называются «майнингом». Эта процедура обеспечивает безопасность и надежность блокчейна.

Алгоритм консенсуса

Среди основных принципов построения блокчейна, наиважнейшим является алгоритм консенсуса, определяющей порядок размещения нового блока в существующей цепи блоков. Алгоритмы консенсуса — это наборы протоколов, которые обеспечивают способ, с помощью которого узлы могут координировать свои действия в распределенной и децентрализованной среде. Выбор конкретного алгоритма зависит от ряда факторов, включая размер группы участников, доступность ресурсов, уровень безопасности, ограничения по времени и другие [68].

Не все типы блокчейн создаются одинаково, и многие из них сильно различаются в зависимости от типа используемого ими алгоритма консенсуса [71].

Существует несколько основных типов консенсусных алгоритмов [61, 63, 68]:

- «Доказательство работы» (Proof-of-work - PoW) – это механизм, позволяющий сетевым узлам конкурировать, чтобы их блок был следующим, добавленным в цепочку, путем вычислительного решения сложной задачи. В

PoW майнераы хешируют данные, которые они хотят добавить, пока не получат подходящее решение криптографической головоломки. Распространенный метод решения задачи заключается в нахождении хэша заголовока блока меньше целевого значения. В каждой попытке майнер должен вычислить хэш для всего заголовка блока [61, 68];

- «Доказательство доли» (Proof-of-stake - PoS) – В этом алгоритме узел, который имеет право добавлять блоки в цепочку блоков, – участник имеющий больший баланс, например, количество токенов. Токен — это форма представления актива или ценности в блокчейне. Это может быть виртуальная валюта, акции и другие ценные бумаги, произведения искусства, объекты недвижимости и другие активы. Токенами можно торговать, их можно покупать и продавать, точно так же, как монетами. Узел не получает вознаграждения за создание самого блока. Вознаграждение выплачивается за транзакцию. Недостатком данного механизма является мотивация в концентрации средств, что может приводить к небольшой централизации сети. Однако алгоритм предусматривает увеличение шанса на право создания блока, исходя не только из количества токенов, но и времени пребывания в системе без создания блока [61, 68].

- «Делегированное доказательство доли» (Delegated Proof-of-Stake DPoS) – это разновидность алгоритма PoS. Владельцы с наибольшим балансом выбирают своих представителей, каждый из которых получает право подписывать блоки в блокчейн сети [61, 68];

- «Арендное доказательство доли» (Leased Proof-of-Stake - LPoS) – является модификацией алгоритма PoS, где любой пользователь имеет возможность передавать свой баланс в аренду другим узлам, за дополнительную прибыль [61, 68];

- «Доказательство способности» (Proof-of-Capacity/ Proof-of-Space PoC) – алгоритм, где каждый валидатор (участник блокчейна, который проверяет транзакцию) обрабатывает достаточно большой объем данных, которые записывается в подсистему узла, при этом вычислительные ресурсы

ограничены временем. Эта концепция подобна PoW за исключением того, что она потребляет дисковое хранилище вместо вычислительных возможностей [61, 68];

- «Доказательство важности» (Proof-of-Importance - PoI) – значимость пользователя определяется количеством средств, имеющихся у него на балансе и количеством проведенных транзакций [61, 68];

- «Доказательство деятельности» (Proof-of-Activity - PoA) — это комбинация двух других алгоритмов консенсуса в блокчейне: proof-of-work (PoW) и proof-of-stake (PoS). Это попытка объединить лучшие аспекты как PoW, так и PoS-систем; процесс майнинга начинается как система PoW, но после успешного майнинга нового блока система переключается на подобие PoS-системы [61, 68];

- «Доказательство власти» (Proof-of-Authority - PoAuth) – Алгоритм консенсуса PoA использует ценность удостоверений участников, что означает, что участники блоков используют не монеты, а свою собственную репутацию. (Монеты используются в качестве валюты для транзакций и имеют свою собственную независимую блокчейн-сеть, например, Биткоин), таким образом, PoA-блокчейны защищены проверяющими узлами, которые произвольно выбраны в качестве надежных объектов [61, 68];

- «Практическая византийская отказоустойчивость» (Practical Byzantine Fault Tolerance - PBFT) – практическаяа система византийской отказоустойчивости может функционировать при условии, что максимальное количество вредоносных узлов не должно превышать или равняться одной трети всех узлов в системе [61].

Рассмотрим далее основные особенности технологии блокчейн [60, 61, 65]:

1- Децентрализация. Данный термин означает передачу контроля и принятия решений от централизованного субъекта (отдельного лица, организации или их группы) к распределенной сети [60 - 64].

2- Неизменность. Означает, что данные не могут быть изменены. Ни один участник не может вмешаться в транзакцию после ее внесения в реестр [60 – 61, 66].

3- Консенсус. Система БЧ устанавливает набор правил, с помощью которых участники одобряют транзакции. Новые транзакции можно регистрировать только с согласия большинства участников сети [61, 67, 68].

Существуют различные типы блокчейн-технологий [60, 61, 69, 70]:

- **Общедоступные (публичные) блокчейн-сети**. Любой пользователь может присоединиться к общедоступной блокчейн-сети (например, Bitcoin). К недостаткам такой сети можно отнести высокие требования к вычислительной мощности [66, 67, 69].
- **Частные блокчейн-сети**. Такая сеть принадлежит одной организации, которая отвечает за управление участниками, внедрение согласованного протокола и ведение общего реестра. В зависимости от сценария использования, такой подход может значительно повысить надежность информации, передаваемой между участниками [60 - 61, 69].
- **Блокчейн-консорциум**. За администрирование блокчейна могут отвечать несколько предварительно выбранных организаций. Эти организации устанавливают права доступа для выполнения транзакций или доступа к данным. Блокчейн-консорциум - идеальное решение для компаний, когда все участники имеют разрешения и несут коллективную ответственность за блокчейн [70].

Следует отметить, что в последнее время в разных странах технология блокчейн начала использоваться в избирательных процессах для повышения безопасности системы голосования.

ПРИЛОЖЕНИЕ 3. Примеры построения криптосистем Бенало и Пэйе и их применения в системе голосования

В данном приложении приведены примеры построения криптосхем Пэйе [57, 59] и Бенало [56] и систем голосования на основе использования их гомоморфных свойств [48].

В рассмотренных ниже примерах все числа генерировались с использованием датчика системных чисел в программе Mathcad. В реальных системах предполагается, что будет использован физический датчик чисел.

Пример схемы Пэйе

Генерация ключей:

1. Выберем два простых числа p=7, q=5 и проверяем условие $\gcd\big(pq,(p-1)(q-1)\big)=1,$
2. Вычисляем $n=pq=35, n^2=1225$ и $\lambda=\mathrm{lcm}(6,4)=12.$
3. Выбираем случайное целое число y, такое что $y\in Z_{n^2}^*, y=3;$
4. Находим $x=\left(L\left(y^{\lambda}\ mod\ n^2\right)\right)^{-1}\ mod\ n=29.$

Таким образом, найдены: (3,35) - открытый ключ, (12,29) - закрытый ключ.

Шифрование сообщения:

Пусть $m\in Z_n, m=8$:

1. Выбираем произвольное $u\in Z_n^*, u=9,$

Тогда $c=3^8\times 9^{35}\ mod\ 1225=939.$

Расшифровывание шифротекста $c\in Z_{n^2}^*$:

Вычисляем $m=L(939^{12}\ mod\ 1225)\times 29\ mod\ 35=8.$

Таким образом, восстановленный открытый текст m=8.

Пример построения схемы Бенало

Генерация ключей:

1. Выберем размер блока сообщения $r<100$ и два больших различных простых числа $p=397, q=191.$

2. Выберем $r = 99,$ таким образом, что:

   $(397-1) mod\ 99 = 0, \gcd(99, \left(\frac{397-1}{99}\right) = 1, \gcd(99,191-1) = 1.$

3. 3.Вычисляем $n = 397 \times 191 = 75827, \varphi(n) = 75240.$
4. Выбираем случайное целое число $y = 13213, y \in Z_n$ и проверяем условие $y^{\varphi/r} \neq 1 mod\ n.$
5. Находим $x = y^{\varphi/r} mod\ n = 13213^{75240/99} mod\ 75827 = 24640.$

Таким образом, найдены: $(13213,75827)$ - открытый ключ, $(75240,24640)$ - закрытый ключ.

Шифрование сообщения. Пусть $m \in Z_r, m = 78$:

Выбираем произвольное $u \in Z_n^*, u = 66183,$

Тогда $c = 13213^{78} 66183^{99}\ mod\ 75827 = 47158.$

Расшифровывание криптограммы $c \in Z_n^*$:

1. Вычисляем $a = 47158^{75240/99}\ mod\ 75827 = 47178,$
2. Строим таблицу значений $x^m = a\ mod\ n$ для m=0,1,2…77,78,…,98.

   И проверяем выполнение сравнения $x^m = a\ mod\ n$?

$m = 0,\ 24640^0\ mod\ 75827 = 1 \neq a$

$m = 1,\ 24640^1\ mod\ 75827 = 24640 \neq a$

$m = 2, 24640^2\ mod\ 75827 = 58638 \neq a$

$m = 78, 24640^{78}\ mod\ 75827 = 47178 = a$

Таким образом, восстановлен открытый текст m=78.

Примеры построения систем электронного голосования на криптосхемах Пэйе и Бенало

Гомоморфная система голосования на основе схемы Пэйе

Обозначим: N_v - количество избирателей, N_c - количество кандидатов, b-основание системы счисления, которое должно выбираться из условия, $b > N_v,$ то есть должно быть больше, чем число избирателей.

Рассмотрим следующий пример:

Предположим, что избираются 2 члена студенческого совета из пяти кандидатов. Выбор одного кандидата или оставление бюллетеня пустым также возможны. Пусть N_v=9, N_c=5, b=10, $b > N_v$. Результаты выбора избирателей представлены в таблице 1.

Таблица 1. Результаты выбора избирателей

Кандидаты / Избиратели	C_1 10^0	C_2 10^1	C_3 10^2	C_4 10^3	C_5 10^4	Шифрование сообщения
V1		•				$m=10^1=10$
V2			•		•	$m=10^2+10^4=10100$
V3						$m=0$
V4				•		$m=10^3=1000$
V5	•			•		$m=10^0+10^3=1001$
V6		•		•		$m=10^1+10^3=1010$
V7			•	•		$m=10^2+10^3=1100$
V8		•		•		$m=10^1+10^3=1010$
V9	•					$m=10^0=1$
Итого	2	3	2	5	1	

Каждому кандидату C_i присваивается идентификатор – число b^i, где i номер кандидата в списке. В данном случае выбрана десятичная система счисления b=10.

Согласно правилу выборов (голосовать можно не более чем за двух кандидатов), максимальное сообщение о голосовании, которое может быть зашифровано избирателем $m_{max} = 10^3 + 10^4 = 11000.$

А максимально возможная сумма голосов всех избирателей

$T_{max} = N_v \times m_{max} = 9 \times 11000 = 99000.$

Поэтому выберем модуль $n > T_{max}; n > 99000.$

Генерирование ключей (Избирательная комиссия):

Используя шаги, описанные в криптосистеме Пэйе для генерации ключей, получим ключи: открытый ключ (6497955158,126869), закрытый ключ (31536,53022).

Шифрование сообщения каждым избирателем:

Пусть сообщение $m \in Z_n$:

1. Выбирается (программой) произвольное $u \in Z_n^*$;
2. Создается криптограмма первым избирателем

$$c_i = 6497955158^{m_i} \times u_i^{126869} \ mod\ 16095743161.$$

Криптограмму каждый избиратель посылает на сервер. Криптограммы от всех избирателей сведены в таблице 2.

Таблица 2. Криптограммы от всех избирателей

Избиратель	Сообщение избираеля	Случайное число u_i	Криптограмма c_i
V1	$m=10^1=10$	35145	13039287935
V2	$m=10^2+10^4=10100$	74384	848742150
V3	$m=0$	96584	7185465039
V4	$m=10^3=1000$	10966	80933260
V5	$m=10^0+10^3=1001$	17953	722036441
V6	$m=10^1+10^3=1010$	7292	350667930
V7	$m=10^2+10^3=1100$	24819	4980449314
V8	$m=10^1+10^3=1010$	4955	7412822644
V9	$m=10^0=1$	118037	3033281324
Общая сумма голосов	15232		

Обработка криптограмм на сервере.

Сервер вычисляет произведение криптограмм c_i и отправляет результат в избирательную комиссию.

$$T = \prod_{i=1}^{N_v} c_i \ mod\ n^2 = (13039287935 * 848742150 * 7185465039 * 80933260 * 722036441 * 350667930 * 4980449314 * 7412822644 * 3033281324) mod\ 16095743161 = 2747997353.$$

Избирательная комиссия, используя закрытый ключ, проводит расшифрование криптограммы произведения

$$T_{m\ общ.} = L\left(c^{\lambda}\ mod\ n^2\right) \times x\ mod\ n = \left(\frac{(2747997353^{81586}\ mod\ 16095743161)-1}{126869}\right) \times 53022\ mod\ 126869 = 15232$$

Далее расшифрованное сообщение записывается, как сумма разрядов в десятичной системе счисления

$$15232 = 1 \times 10^4 + 5 \times 10^3 + 2 \times 10^2 + 3 \times 10^1 + 2 \times 10^0.$$

Наибольшие значения имеют коэффициенты при степенях 10^3 и 10^1. Это означает, что победителями выборов являются кандидаты C_2 и C_4.

Гомоморфная система голосования на основе схемы Бенало

Условия голосования такие же, как при рассмотрении схемы Пэйе N_v =9, N_c=5. Выберем основание системы счисления b=10, $b > N_v$

Избирательная комиссия генерирует ключи:

Используя шаги, описанные в криптосистеме Бенало для генерации ключей, получим ключи: открытый ключ (62369,20205597437), закрытый ключ (20205310716,6922019540). Открытый ключ передается всем избирателям.

Шифрование сообщения избирателем:

Пусть сообщение $m \in Z_r$:

1. Выбирается (программой) произвольное $u \in Z_n^*$,
2. Создается криптограмма первым избирателем

$c = 15^{m_i} \times u_i^{62369} \; mod \; 20205597437.$

Криптограммы других избирателей показаны в таблице 3:

Таблица 3. Криптограммы других избирателей

Избирателя	Шифрование сообщения	u_i	c_i
V1	$m=10^1=10$	35145	183946066
V2	$m=10^2+10^4=10100$	74384	10050175893
V3	$m=0$	96584	16340434784
V4	$m=10^3=1000$	10966	8189135103
V5	$m=10^0+10^3=1001$	17953	4202784310
V6	$m=10^1+10^3=1010$	7292	14220855747
V7	$m=10^2+10^3=1100$	24819	7937933779
V8	$m=10^1+10^3=1010$	4955	15466873618
V9	$m=10^0=1$	118037	1049803439
Сумма голосов, поданных избирателями *T*общ.	15232		

Обработка криптограмм на сервере.

$T = \prod_{i=1}^{N_v} c_i \; mod \; n = (183946066 * 10050175893 * 1634043784 * 8189135103 * 4202784310 * 14220855747 * 7937933779 * 15466873618 * 1049803439) \; mod \; 20205597437 = 4249761249.$

Расшифровывание криптограммы $c \in Z_n^*$:

1. Вычисляем $a_i = 4249761249^{323964} \ mod \ 20205597437 = 2281530556$,
2. Строим таблицу значений $x^m \ mod \ n$

   для m=0,1,2,3,4…..,15232,15777,16123,20000,24565,30567. И проверяем выполнение сравнения $x^m \ mod \ n$?

Таблица 4. Значение функции x^m для m=1,…..,15232

m	$x^m \ mod \ n$
0	$6922019540^0 \ mod \ 20205597437 = 1 \neq a$
1	$6922019540^1 \ mod \ 20205597437 = 6922019540 \neq a$
2	$6922019540^2 \ mod \ 20205597437 = 12864689861 \neq a$
3	$6922019540^3 \ mod \ 20205597437 = 17168902137 \neq a$
.....	……
15232	$6922019540^{15232} \ mod \ 20205597437 = 2281530556 = a$

Из таблицы следует, что восстановленный открытый текст m=15232. Из анализа этого числа $15232 = 1 \times 10^4 + 5 \times 10^3 + 2 \times 10^2 + 3 \times 10^1 + 2 \times 10^0$ следует, что кандидаты C_2 и C_4 являются победителями. Наибольшие значения имеют коэффициенты при степенях 10^3 и 10^1.

ПРИЛОЖЕНИЕ 4. Примеры формирования и проверки доказательства корректности заполнения бюллетеня по каждому кандидату на основе криптосхемы Эль -Гамаля на эллиптической кривой

Рассмотрим примеры формирования и проверки доказательства корректности заполнения ИзБ для варианта, когда выбирается один кандидат $D1$ из 4 кандидатов.

Пусть на этапе инициализации системы ДЭГ выбраны параметры криптосхемы Эль-Гамаля на эллиптической кривой: p=59, q=17, (a=3,b=9). Выбор кривой и параметров шифрования носят иллюстрационный характер. Эллиптическая кривая является несингулярной и имеет следующие точки:

{(0, 3), (0, 56), (3, 24), (3, 35), (4, 12), (4, 47), (6, 19), (6, 40), (7, 14), (7, 45), (9, 23), (9, 36), (10, 6), (10, 53), (11, 4), (11, 55), (12, 11), (12, 48), (13, 11), (13, 48), (14, 9), (14, 50), (15, 19), (15, 40), (17, 28), (17, 31), (19, 9), (19, 50), (20, 24), (20, 35), (25, 29), (25, 30), (26, 9), (26, 50), (29, 0), (34, 11), (34, 48), (36, 24), (36, 35), (38, 19), (38, 40), (42, 1), (42, 58), (46, 29), (46, 30), (47, 29), (47, 30), (49, 10), (49, 49), (50, 16), (50, 43), (51, 2), (51, 57), (54, 20), (54, 39), (55, 13), (55, 46), (58, 8), (58, 51) и точка $\mathcal{O}$)}.

Используя схему ЭГ и выбрав базовую точку $P = (19,9)$, генерируются ключи: закрытый – $d = 4$ и открытый – $Q = 4(19,9) \bmod 59 = (6,19)$.

Параметры p, E, m, P, F, Q публикуются в БЧ. (Порядок выполнения операций сложения и умножения точек эллиптической кривой на целое число можно найти в [27]).

В дальнейшем будем предполагать, что для вычисления хэш-функции используется некоторый алгоритм, вырабатывающий по заданному аргументу число, которое мы в числовых примерах указываем произвольно.

А) Проверка корректности заполнения бюллетеня методом доказательства с нулевым разглашением секрета на основе равенства логарифмов

Рассмотрим два «полярных» случая.

Случай 1. Избиратель правильно заполнил свой бюллетень, как показано в таблице 1.

Таблица 1. Правильное заполнение бюллетеня

Кандидаты	D_1	D_2	D_3	D_4
Выбор избирателя V_1	1	0	0	0

Алгоритм голосования, формирование доказательства корректности заполнения ИзБ и их проверки описаны в п.4.1и отображены в таблицах 2 и 3.

Таблица 2. Формирование доказательства корректности заполнения бюллетеня

Избиратель	
Проголосовал «за» за первого кандидата, как показано на таблице 1:	$v_1 = 1$.
Осуществляет шифрование бюллетеня по каждому кандидату (вычисляет): $(A_1, B_1) = (r_1P, M + r_1Q) \bmod p$;	Выбирает случайным образом $r_1 = 2$; $C_1 = \big(2(19,9) + 1(52,2) + 2(6,19)\big) \bmod 59$ = ((49, 10), (6, 40));
Вычисляет доказательство корректности голосования):(A_1, B_1): $a_1 = (t_1P - u_1A) \bmod p$; $b_1 = (t_1Q - u_1(B - v_i\mathrm{P}) \bmod p$; $a_2 = wP \bmod p$; $b_2 = wQ \bmod p$.	Вычисляет доказательство для криптограммы $(A_1, B_1) = ((49,10),(6,40))$; Если $v_1 = 1$, Случайным образом выбирает числа: $t_1 = 2$, w = 2, $u_1 = 5$; Вычисляет: $a_1 = \big(2(19,9) - 5(49,10)\big) \bmod 59 = (34,48)$; $b_1 = (2(6,19) - 5\big((6,40) - 1(19,9)\big)$ $\bmod 59 = (54,39)$; $a_2 = 2(19,9) \bmod 59 = (49,10)$; $b_2 = 2(6,19) \bmod 59 = (34,11)$.
Вычисляет хэш-функцию $c = H(A, B, a_1, b_1, a_2, b_2) \bmod q$:	$c = 3$.
Вычисляет доказательство: $u_2 = c - u_1 \bmod q$; $t_2 = w - r_1u_2 \bmod q$.	Вычисляет: $u_2 = 3 - 5 \bmod 17 = 15$; $t_2 = 2 - 2 \times 15 \bmod 17 = 6$.
Отправляет в БЧ зашифрованный бюллетень и доказательство.	Зашифрованный бюллетень: $(A_1 = (49,10), B_1 = (6,40))$; доказательство: $\begin{pmatrix} a_1 = (34,48), b_1 = (54,39), a_2 = (49,10), \\ b_2 = (34,11), u_1 = 5, u_2 = 15, t_1 = 2, \\ t_2 = 6 \end{pmatrix}$

Таким же образом шифруются голоса для остальных кандидатов:$C_2 = ((6,19),(19,9)), C_3 = ((51,2),(51,2)),$

$C_4 = ((34,48),(49,49))$.

где криптограммы C_2, C_3, C_4 является зашифрованными значениями точки $\mathcal{O}$.

В таблице 3, показана проверка в БЧ, что избиратель правильно заполнил свой бюллетень.

Таблица 3. Алгоритм проверки корректности голосования за кандидата

БЧ	
Вычисляет хэш-функцию c = $H(A, B, a_1, b_1, a_2, b_2)$;	$c = 3$.
Проверяет сравнения: $c \bmod q =^{?} u_1 + u_2 \bmod q$; $t_1 P \bmod p =^{?} a_1 + u_1 A \bmod p$; $t_1 Q \bmod p =^{?} b_1 + u_1 (B - v_i P) \bmod p$.	-Находит: $(u_1 + u_2) \bmod q = (5 + 15) \bmod 17 = 3$. сравнение выполняется: $3 = 3$; -Находит $t_1 P \bmod p = (49, 10)$ и $a_1 + u_1 A_1 \bmod p = (49, 10)$ и проверяет, что сравнение выполняется: $t_1 P \bmod p =^{?} a_1 + u_1 A_1 \bmod p$; $(49, 10) = (49, 10)$; -Вычисляет: $t_1 Q \bmod p = (34, 11)$ и $b_1 + u_1 (B_1 - v_i P) \bmod p = (34, 11)$; Сравнение выполняется: $(34, 11) = (34, 11)$.

Таким образом, все сравнения выполнены, следовательно, корректность заполнения бюллетеня для *D*1 доказана.

Аналогично, проверяются доказательства корректности голосования за других кандидатов.

Случай 2. **Избиратель неправильно заполнил свой бюллетень:**

Пусть, избиратель поставил число 2 за кандидата *D*1, как показано в таблице 4.

Таблица 4. Формирование неправильного заполнения бюллетеня

Кандидаты	D_1	D_2	D_3	D_4
Выбор избирателя V_1	2	0	0	0

Все шаги алгоритма аналогичны предыдущему примеру:

Таблица 5. Формирование доказательства корректности заполнения бюллетеня

Избиратель	
Проголосовал за первого кандидата, как показано на таблице 4:	$v_1 = 2$.
Осуществляет шифрование бюллетеня по каждому кандидату (вычисляет): $(A_1, B_1) = (r_1 P, M + r_1 Q) \bmod p$;	Находит: $(A_1, B_1) = (r_1 P, M + r_1 Q) \bmod p = ((54, 39), (54, 39))$.

Формирует доказательство корректности голосования (вычисляет):(A_1, B_1): $a_1 = (t_1P - u_1A) \bmod p$; $b_1 = (t_1Q - u_1(B - v_i\mathrm{P}) \bmod p$; $a_2 = wP \bmod p$; $b_2 = wQ \bmod p$.	Вычисляет доказательство для криптограммы $(A_1, B_1) = ((54, 39), (54, 39))$; Вычисляет: $a_1 = (6, 40), b_1 = (11, 4), a_2 = (49, 10), b_2$ =(34, 11),$c = 5, u_2 = 3, t_2 = 13$.
Вычисляет хэш-функцию $c = H(A, B, a_1, b_1, a_2, b_2) \bmod q$:	$c = 5$.
Вычисляет доказательство: $u_2 = c - u_1 \bmod q$; $t_2 = w - r_1u_2 \bmod q$.	Вычисляет: $u_2 = 3, t_2 = 13$.
Отправляет в БЧ зашифрованный бюллетень и доказательство.	Зашифрованный бюллетень: $(A_1 = (54, 39), B_1 = (54, 39))$; Доказательство: $\begin{pmatrix} a_1 = (6, 40), b_1 = (11, 4), a_2 = (49, 10), \\ b_2 = (34, 11), u_1 = 2, u_2 = 3, t_1 = 3, t_2 = 13 \end{pmatrix}$.

В таблице 6 приведен алгоритм проверки доказательства корректности заполнения бюллетеня на стороне БЧ.

Таблица 6. Алгоритм проверки корректности голосования за кандидата

БЧ	
Вычисляет хэш-функцию с = $H(A, B, a_1, b_1, a_2, b_2)$;	$c = 5$.
Проверяет сравнения: $c \bmod q =^{?} u_1 + u_2 \bmod q$; $t_1P \bmod p =^{?} a_1 + u_1A \bmod p$; $t_1Q \bmod p =^{?} b_1 + u_1(B - v_iP) \bmod p$.	-Находит: $(u_1 + u_2) \bmod q = (2 + 3) \bmod 17 = 5$. Сравнение выполняется: $5 = 5$; -Находит $t_1P \bmod p$ = (49, 10) и $a_1 + u_1A_1 \bmod p = (49, 10)$ $t_1P \bmod p =^{?} a_1 + u_1A_1 \bmod p$; Сравнение выполняется: $(49, 10) = (49, 10)$; -Вычисляет: $t_1\mathrm{Q} \bmod p = (34, 11)$ и $b_1 + u_1(B_1 - v_iP) \bmod p = (49, 10)$; Видим, что сравнение не выполняется: $(34, 11) \neq (49, 10)$.

Видно, что не все сравнения выполнены, следовательно, корректность заполнения бюллетеня для *D*1 не доказана.

Б) Проверка корректности заполнения бюллетеня методом доказательства с нулевым разглашением секрета на основе перемешивания криптограмм бюллетеня

На рисунке 1 представлены принципы схемы перемешивания голосов избирателей.

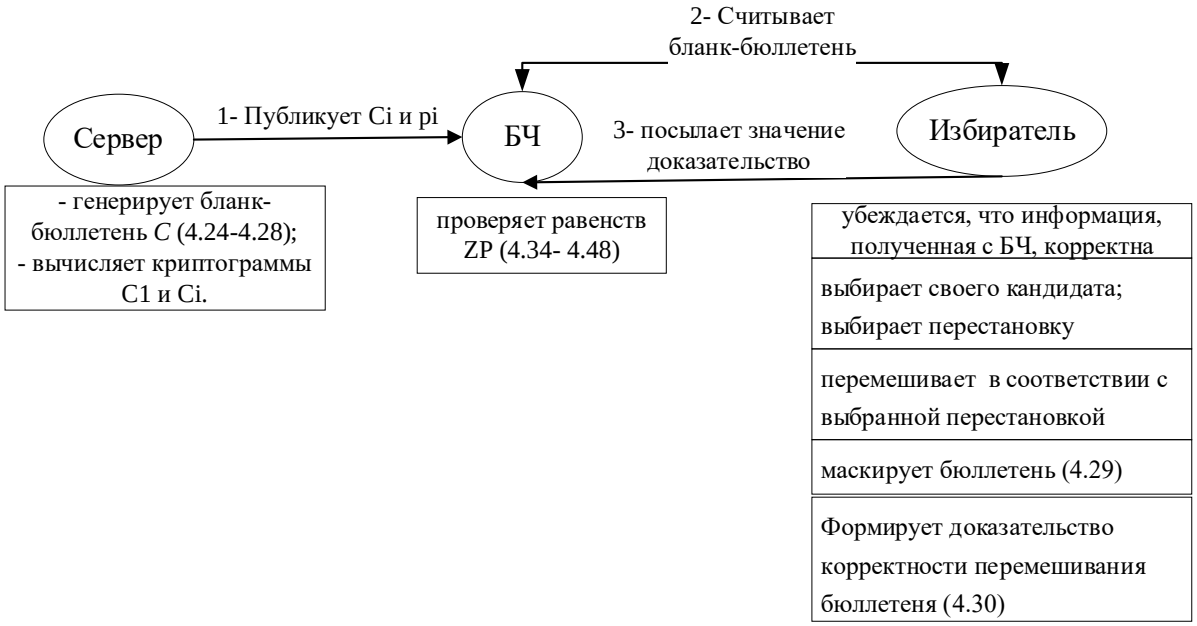

Рис.1. Схема перемешивания голос избирателя

***Случай 1*: Избиратель правильно перемешал голоса в бюллетене [112].**

Приступает к голосованию:

– Выбирает своего кандидата – *D*4.

– Выбирает перестановку: $\pi(1) = 4,\ \pi(2) = 2,\ \pi(3) = 3, \pi(4) = 1$. Для этого перемешивает координаты C в соответствии с выбранной перестановкой и осуществляет маскировку бюллетеня, для этого:

– Генерирует случайным образом набор целых чисел r_i= {4, 2, 1, 3};

– Вычисляет $C_i' = C_{\pi(i)} + (r_i P, r_i Q) = (A_{\pi(i)} + r_i P,$

$B_{\pi(i)} + r_i Q) = ((\rho_1 + r_i)P,\ F_i + (\rho_1 + r_i)Q) \bmod p$, получает:

$\{C_i'\}$ = {((11, 4), (11, 55)), ((54, 39), (54, 20)), ((6, 19), (19, 9)), ((34, 48), (19, 9))}.

Далее формирует доказательство корректности перемешивания бюллетеня. Для этого избиратель получает от БЧ случайным образом выбранные БЧ числа s_i и s_i', где $i = 1,..,4$.

Пусть $(s_1 = 2,\ s_2 = 3, s_3 = 1, s_4 = 4, s'_1 = 1, s'_2 = 3, s'_3 = 2, s'_4 = 4$. Далее избиратель вычисляет числа $t_i = s_{\pi(i)},\ t'_i = s'_{\pi(i)},\quad i = 1,2,\dots,k.$ Тогда $t_1 = 4, t_2 = 1, t_3 = 3, t_4 = 2. t'_1 = 4, t'_2 = 2, t'_3 = 3, t'_4 = 1.$ А потом выбирает $r'_i = \{1,3,4,2\}$ и вычисляет:

$C''_i = (t_i A'_i + r'_i P, t_i B'_i + r'_i Q), \{C''_i\} = \{((6,40),(19,50))$

$((11,55),(11,4)),((19,9),(6,19)),((19,9),(51,57))\}.$

и отправляет C'_i, C''_i, t_i и t'_i в БЧ.

Далее проверим выполнение сравнения. Для первой части криптограммы C'_1, необходимо доказать, что $A''_1 = A'_1 t_1 + r'_1 P.$ В нашем примере мы получили:

$C'_1 = (r_1 + r'_1)P, F + (r_1 + r'_1)Q = ((11,4),(11,5)); C''_1 = (t_1 A'_1 + r'_1 P, t_1 B'_1 + r'_1 Q) = ((6,40),(19,50)).$

Избиратель формирует доказательство для этой криптограммы следующим образом:

1) Выбирает случайные числа $z_1 = 2, u_1 = 1,$

вычисляет $L_1 = z_1 P \bmod p = (49,10), J_1 = u_1 A'_1 \bmod p = (54,20)$

и находит хеш-функцию: $h_1 = H\big((6,40),(19,9),(19,50)\big) \bmod 17 = 16;$

2) Вычисляет: $\theta_1 = z_1 + r'_1 h_1 \bmod q = 2 + 1 * 16 \bmod 17 = 1;$

$\alpha_1 = u_1 + t_1 h_1 \bmod q = 1 + 4 * 16 \bmod 17 = 14; T_1 = \theta_1 P + \alpha_1 A'_1 \bmod p = 1(19,9) + 14(11,4) \bmod 59$

$= (6,40);$

3) Пересылает в БЧ ($T_1 = (6,40),\ L_1 = (49,10), J_1 = (54,20)$).

БЧ вычисляет хеш-функцию

$h' = H\big(A''_1 = (6,40),\ P = (19,9), L_1 + J_1 = (19,50)\big) \bmod 17 = 16$ и h'_i, а также проверяет сравнение $L_1 + J_1 + h' \cdot A''_1 = ? T_1; (6,40) = T_1.$

Таким образом доказано, что сравнение выполняется для первой части криптограммы C_1.

Аналогично проверяем доказательство для A_2, A_3, A_4.

Избиратель выполняет следующие действия:

– Генерирует случайное число $w = 3$;

– Вычисляет $T = wP \bmod p = (54,39)$;

– Вычисляет: $r_\sum = \sum_{i=1}^{k} r_i t_i + r_i' = 3,\ U = r_\sum P \bmod p = (54,39)$;

– Вычисляет хеш-функцию

$h = H(P = (19,9),\ T = (54,39), U = (54,39), A_1'' = (6,40), A_2'' = (11,55), A_3'' = (19,9), A_4'' = (19,9)) \bmod 17 = 10$

– Вычисляет $z = w - r_\sum \cdot h \bmod q = 6$;

– Посылает в БЧ $(T = (54,39), z = 6)$.

Далее БЧ вычисляет: $U' = \sum_{i=1}^{k} A_i'' - \sum_{i=1}^{k} s_i A_i = \left(\sum_{i=1}^{k} t_i r_i + r_i'\right)P =$

$= r_\sum P = (54,39)$;

– хеш-функцию $h' = 10$;

– $T' = zP + h'U' = (54,39)$;

– Проверяет $T =^{?} T'; (54,39) = (54,39)$, т. е. Для первой части криптограмм C_i'' доказано.

Случай 2. **Избиратель неправильно перемешал голоса в бюллетене.**

Все шаги выполняются, как в предыдущем примере, до момента перемешивания. Избиратель выполняет перестановку π.

$\{C_i\}$= {((19, 9), (6, 19)), ((19, 9), (6, 19)), ((54, 39), (54, 20)), ((6, 19), (19, 9))}. Далее осуществляет маскировку бюллетеня, генерирует случайным образом набор целых чисел r_i = {4, 2, 1, 3}, вычисляет C_i':

$C_i' = C_{\pi(i)} + (r_i P, r_i Q) = (A_{\pi(i)} + r_i P, B_{\pi(i)} + r_i Q) = \left((\rho_i + r_i)P, F_i + (\rho_i + r_i)Q\right) \bmod p,$

для $i = 2,..,k$, получает: $\{C_i'\}$ = {((11, 4), (54, 20)), ((54, 39), (11, 4)), ((6, 19), (19, 9)), ((34, 48), (19, 9))}.

Следующий шаг – формирование доказательства корректности перемешивания бюллетеня. Для этого избиратель получает от БЧ случайным

образом выбранные числа s_i и s_i', где $i = 1,.., n$: пусть $(s_1 = 2, s_2 = 3, s_3 = 1, s_4 = 4, s_1' = 1, s_2' = 3, s_3' = 2, s_4' = 4)$, вычисляет числа t_i, t_i', как в предыдущем примере, выбирает r_i' = {1, 2, 3, 4} и вычисляет $C_i'' = (t_i A_i' + r_i' P, t_i B_i' + r_i' Q), \{C_i''\}$ = {((6, 40), (19, 50)), ((11, 55),(11, 4)), ((19, 9),(6, 19)), ((19, 9),(51, 57))}, после чего отправляет C_i', C_i'', t_i и t_i' в БЧ.

Далее проверим доказательства для первых частей криптограммы C_1', для этого покажем, что $A_1'' = A_1' t_1 + r_1' P$.

Ранее было получено: $C_1' = (r_1 + r_1')P,\ F + (r_1 + r_1')Q = ((11,4),(54,20))$и $C_1'' = (t_1 A_1' + r_1' P, t_1 B_1' + r_1' Q) = ((6,40),(19,50))$.

Избиратель формирует доказательство для каждой криптограммы:

– Выбирает случайные числа $z_1 = 2, u_1 = 1$, вычисляет $L_1 = z_1 P \bmod p = (49,10),\ J_1 = u_1 A_1' \bmod p = (54,20)$и хеш-функцию $h_1 = H\big(A_1'' = (6,40),\ P == (19,9),\ L_1 + J_1 = (19,50)\big) \bmod 17 = 16$;

– Вычисляет:$\theta_1 = z_1 + r_1' h_1 \bmod q = 2 + 1 * 16 \bmod 17 = 1$;

$\alpha_1 = u_1 + t_1 h_1 \bmod q = 1 + 4 * 16 \bmod 17 = 14$;

$T_1 = \theta_1 P + \alpha_1 A_1' \bmod p = 1(19,9) + 14(11,4) \bmod 59 = (6,40)$;

– Пересылает в БЧ ($T_1 = (6,40), P = (19,9), L_1 + + J_1 = (19,50)$).

БЧ вычисляет хеш-функцию:

$h' = H\big(A_1' = (6,40), P = (19,9), L_1 + J_1 = (19,50)\big) \bmod 17 = 16$,

и проверяет сравнение $L_1 + J_1 + h' \cdot A_1'' = ? T_1;\ (6,40) = T_1$. Сравнение выполняется, т. е. для первой части криптограммы C_1 доказано.

Аналогично проверяем доказательство для A_2, A_3, A_4.

Избиратель генерирует случайное число $w = 3$. После чего вычисляет:

– $T = wP \bmod p = (54,39)$;

– $r_\Sigma = \sum_{i=1}^{k} r_i t_i + r_i' = 3, U = r_\Sigma P \bmod p = (54,39)$;

– хеш-функцию:

$h = H(P = (19,9),\ T = (54,39),\ U = (54,39),\ A_1'' = (6,40),\ A_2'' = (11,55),\ A_3'' = (19,9),\ A_4'' = (19,9)) \bmod 17 = 10$

– $z = w - r_{\sum} \cdot h \bmod q = 6.$

Далее посылает в БЧ $(T = (54,39), z = 6)$.

БЧ вычисляет:

– $U' = \sum_{i=1}^{k} A_i'' - \sum_{i=1}^{k} s_i A_i = (51,57)$,

– хеш-функцию $h' = 10$;

– $T' = zP + h'U' = (6,40)$.

– Проверяет $T \stackrel{?}{=} T';\ (54,39) \neq (6,40)$ – не выполнено; следовательно, сравнение для первой части криптограммы C_1'' не доказано.

C) Проверка корректности заполнения бюллетеня методом доказательства с нулевым разглашением секрета на основе равенства логарифмов для всех кандидатов по предлагаемому методу на основе криптосхемы Эль - Гамаля на в поле GF(p).

Пусть на этапе инициализации системы ДЭГ выбраны параметры криптосхемы Эль-Гамаля $p = 11, g = 6, s = 3, h = 7$. Пусть в голосовании участвуют четыре кандидата: D1, D2, D3, D4. Избиратель голосует за кандидата D1 и против остальных кандидатов, т. е. $m = 1$.

***Случай 1*. Избиратель правильно заполнил свой бюллетень.**

Алгоритм голосования, формирование доказательства корректности заполнения ИзБ и их проверки описаны в п.4.3.

Перед процедурой голосования БЧ генерирует величину $A_{k+1} = g^{r_{k+1}}$, $r_{k+1} \in Z_p$, и число $f \in Z_p$ и посылает $(g^{r_{k+1}}, f)$ избирателю.

БЧ случайным образом выбирает числа $r_5 = 7$ и $f = 3$, вычисляет $A_5 = g^{r_5} \bmod p = 8$ и посылает $(A_5 = 8, f = 3)$ избирателю.

Таблица 7. Формирование доказательства корректности заполнения бюллетеня

Избиратель	$v_1 = 1.$
Генерирует числа, используя первые части криптограмм yi: $y_i = \frac{\prod_{j<i} A_j}{\prod_{j>i} A_j}$. Далее, вычисляет вторые части криптограмм B_i:	$r_1 = 10, A_1 = 1; r_2 = 9, A_2 = 2; r_3 = 8, A_3 = 4$ и $r_4 = 6, A_4 = 5.$ $y_1 = 6; y_2 = 9; y_3 = 1; y_4 = 2; y_5 = 3$ $B_1 = 6; B_2 = 8; B_3 = 9; B_4 = 4.$
Вычисляет: $U_{D_i} = y_i^{r_i} g^{v_i}$	$U_{D1} = 3; U_{D2} = 4; U_{D3} = 1; U_{D4} = 10.$
Находит произведение $U'_{\Sigma} = \prod_{i=1}^{k} U_{Di} = \prod_{i=1}^{k} y_i^{r_i} g^{v_i}$	$\prod_{i=1}^{k} U_{Di} = 10$
Вычисляет: $X' = h^s$, $x = e + \sum_{i=1}^{k} r_i \cdot f.$	e=3, вычисляет: $X' = 2$ и $x = 99$

Избиратель посылает U'_{Σ}, X'и x в БЧ и начнется процесс проверки заполнения бюллетеня как показано в таблице 8.

Таблица 8. Алгоритм проверки корректности голосования для всех кандидатов

БЧ	
Первая проверка: вычисляет: $y_{k+1}^{r+1} = A_1 A_2 \dots A_k.$ находит: $U_{Dk+1} = y_{k+1}^{r_{k+1}} \cdot g^{v_{k+1}}$ вычисляет: $U_{\Sigma} = U'_{\Sigma} U_{Dk+1} = g^{\sum_{i=1}^{k} v_i + v_{k+1}}.$	$y_5 = 1$ $U_{D5} = 7$ $U_{\Sigma} = 1$
проверяет неравенство: $m_{min} \le \sum_{i=1}^{n} v_i \le m_{max}.$	$1 \le 1 \le 1.$
Вторая проверка: проверяет сравнение: $h^x =^? X' \cdot V.$	2=2. Сравнения выполнены.

***Случай 2*. Избиратель неправильно заполнил свой бюллетень:**

Пусть, избиратель проголосовал за двух кандидатов и нарушил правила голосования, т.е. $m = 2$, тогда $m > m_{max}$, значит он нарушил правила голосования, потому что в нашем пример $m_{max} = 1$.

Таблица 9. Формирование доказательства корректности заполнения бюллетеня

Избиратель	$v_1 = 2.$

Генерирует числа, используя первые части криптограмм yi: $y_i = \frac{\prod_{j<i} A_j}{\prod_{j>i} A_j}$. Далее, вычисляет вторые части криптограмм B_i:	$r_1 = 5, A_1 = 10; r_2 = 4, A_2 = 9; r_3 = 6, A_3 = 5$ и $r_4 = 9, A_4 = 2$. $y_1 = 4; y_2 = 8; y_3 = 2; y_4 = 3; y_5 = 5$. Далее, вычисляет вторые части криптограмм B_i, то $B_1 = 5; B_2 = 3; B_3 = 2; B_4 = 8$.
Вычисляет: $U_{D_i} = y_i^{r_i} g^{v_i}$	$U_{D1} = 6; U_{D2} = 4; U_{D3} = 10; U_{D4} = 4$.
Находит произведение $U'_{\sum} = \prod_{i=1}^{k} U_{Di} = \prod_{i=1}^{k} y_i^{r_i} g^{v_i}$	$U'_{\sum} = 3$
Вычисляет: $X' = h^s$, $x = e + \sum_{i=1}^{k} r_i \cdot f$.	Выбирает случайном образом число *e=4*, вычисляет: $X' = 3$ и $x = 100$.

Избиратель посылает $U'_{\sum}$, X'и x в БЧ и начнется процесс проверки заполнения бюллетеня как показано в таблице 10.

Таблица 10. Алгоритм проверки корректности голосования для всех кандидатов

БЧ	
Первая проверка: вычисляет: $y_{k+1}^{r+1} = A_1 A_2 \dots A_k$. находит: $U_{Dk+1} = y_{k+1}^{r_{k+1}} \cdot g^{v_{k+1}}$ вычисляет: $U_{\sum} = U'_{\sum} U_{Dk+1} = g^{\sum_{i=1}^{k} v_i + v_{k+1}}$.	$y_5 = 8$ $U_{D5} = 7$ $U_{\sum} = 9$
проверяет неравенство: $m_{min} \le \sum_{i=1}^{n} v_i \le m_{max}$.	$1 \le 2 \le 1$
Вторая проверка: проверяет сравнение: $h^x =^? X' \cdot V$.	$1 \neq 9$ Сравнения не выполнены. Значит, избиратель нарушил правила голосования.