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

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2023

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» на кафедре защищенных систем связи.

Научный руководитель: доктор технических наук, профессор
Яковлев Виктор Алексеевич

Официальные оппоненты: **Александрова Елена Борисовна**,
доктор технических наук, доцент,
Санкт-Петербургский политехнический университет Петра Великого, Высшая школа кибербезопасности, профессор

Левина Алла Борисовна,
кандидат физико-математических наук, доцент,
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), кафедра информационной безопасности, доцент кафедры

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Петербургский государственный университет путей сообщения Императора Александра I», г. Санкт-Петербург

Защита состоится 06 марта 2024 года в 16.00 на заседании объединенного диссертационного совета 99.2.038.03, созданного на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова», Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» по адресу: Санкт-Петербург, пр. Большевиков, д. 22, корп. 1, ауд. 554/1.

С диссертацией можно ознакомиться в библиотеке СПбГУТ по адресу Санкт-Петербург, пр. Большевиков, д. 22, корп. 1 и на сайте www.sut.ru.

Автореферат разослан 29 декабря 2023 года.

Ученый секретарь
диссертационного совета 99.2.038.03,
канд. техн. наук, доцент А.Г. Владыко

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. В современном мире стремительно развиваются информационно-коммуникационные технологии, оказывающие влияние на общество и такие его сферы как образование, здравоохранение, банковское дело, медиа, транспорт, производство, торговля и другие. Научно-технический прогресс затронул также такую важную сферу человеческой деятельности, как различные виды голосования, посредством которых граждане осуществляют свое волеизъявление. Уже много 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, молодых избирателей и создания других удобств голосующим.

Дистанционное электронное голосование (ДЭГ) – переход к системе онлайн-голосования, базирующейся на интернет-платформе с использованием криптографических методов. Однако использование открытой среды (Интернета) для функционирования системы ДЭГ создает много рисков надежности системы ДЭГ и безопасности ее функционирования, поэтому в системе ДЭГ должны выполняться требования обеспечения тайны голосования, анонимности голосующего, аутентификации избирателя, уникальности и точности голосования.

Анализ практических систем ДЭГ в разных странах: «Комплекс ДЭГ» и «Крипто Вече» – Россия, «Apollo», «Bronco». «Helios» – США, «Provotum» – Швейцария и др. показал, что эти системы реализованы с учетом конкретных условий их использования: количество избирателей; актуальные угрозы; технические возможности реализации и пр. Некоторые системы представляют коммерческий продукт без полного и открытого описания принципа работы, 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.

Вопросы построения выборной системы регулируются законодательно индивидуально в каждой стране. 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. При построении системы голосования должны учитываться угрозы безопасности информации, характерные для данного региона или группы стран. Такие угрозы в основном связаны с технологией обработки бумажных бюллетеней и

влиянием субъективного (человеческого) фактора, в частности, возможными 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 современных и безопасных систем дистанционного электронного голосования для арабских государств, является актуальной научно-практической задачей. 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. Основоположниками исследований 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 и присущих им недостатков;

– анализ угроз безопасности информации в системе ДЭГ, способов их предотвращения и блокирования;

– 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 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 построена на основе распределенной сети узлов блокчейн-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. На узле голосования провинции есть несколько смарт-контрактов, в которых хранятся зашифрованные голоса избирателей избирательного участка.

- 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 субъективным (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.

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.

Методология и методы исследования. Использовались методы анализа криптографических схем гомоморфного шифрования в числовом поле и на эллиптической кривой; методы доказательства с нулевым разглашением секрета; методы доказательства корректности заполнения бюллетеня, технология блокчейн-консорциума. Моделирование функционирования предложенного протокола ДЭГ выполнено на основе комплекса приложений, разработанного на языке программирования Python 3.10 с использованием библиотеки PyQt5,

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.

Апробация результатов. 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-

теоретической 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, 2021–2023).

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 Минобрнауки России, 1 статья в рецензируемых изданиях, входящих в международные базы данных SCOPUS, 8 статей в журналах и сборниках конференций, включенных в РИНЦ.

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 с научным руководителем, д.т.н., профессором В.А. Яковлевым. С научным руководителем проводились обсуждение и контроль полученных результатов. Результаты теоретических и экспериментальных исследований получены автором самостоятельно.

Структура и объем диссертации. Диссертации состоит из введения, четырех глав, заключения, списка литературы и 4 приложения. Общий объем работы 177 страниц, из них основного текста 131 страница. Работа содержит 21 рисунок и 40 таблиц. Список литературы включает 114 источников.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении определены актуальность темы диссертации, цель и задачи диссертационной работы, сформулированы положения, выносимые на защиту, научная новизна результатов их теоретическая и практическая значимость, приведены сведения об опубликованных работах, выступлениях на конференциях и семинарах.

В первой главе диссертации проанализированы характеристики существующей системы голосования в Республике Ирак, примененной на выборах 2021 года, отмечены присущие ей недостатки и угрозы информационной безопасности. Недостатки и угрозы традиционной системы голосования в основном обусловлены влиянием субъективного (человеческого) фактора и технологией обработки бумажных бюллетеней.

Рассмотрены особенности избирательных систем в арабских странах с парламентской правовой системой. Показано, что организация и проведение выборов в них совпадает с общемировой практикой, однако всем им присущи свои специфические особенности, связанные с культурными и цивилизационными особенностями, Многие угрозы и недостатки существующей избирательной системы могут быть преодолены при переходе к системам дистанционного электронного голосования (ДЭГ).

Проведен анализ опыта внедрения и применения систем дистанционного электронного голосования в разных странах. Сделан вывод, что создание такой системы для республики Ирак и других арабских стран является актуальной научной задачей. Сформулированы функциональные требования и требования безопасности информации, которые должны быть выполнены при создании перспективной системы ДЭГ в арабских государствах.

Во второй главе проанализированы принципы построения современных систем дистанционного электронного голосования на основе микс-сетей, слепой подписи, гомоморфного шифрования и использования блокчейн технологий. Результаты анализа показывают, что системы ДЭГ на основе гомоморфного шифрования обладают рядом преимуществ и поэтому эта криптосхема в сочетании с блокчейн взята за основу в предлагаемой модели системы ДЭГ для обеспечения безопасности избирательного процесса.

Предложена модель системы дистанционного электронного голосования (ДЭГ) для республики Ирак (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, что гарантирует полноту подсчета голосов, сокращает время подсчета голосов и снижает нагрузку на блокчейн-сеть (рисунок 1). В предлагаемой модели усилена функция защиты от угроз нарушения анонимности избирателя за счет атак со стороны административного ресурса. С этой целью использован принцип

распределенного дешифрования, исключающий использования в системе ДЭГ единого ключа расшифрования бюллетеней.

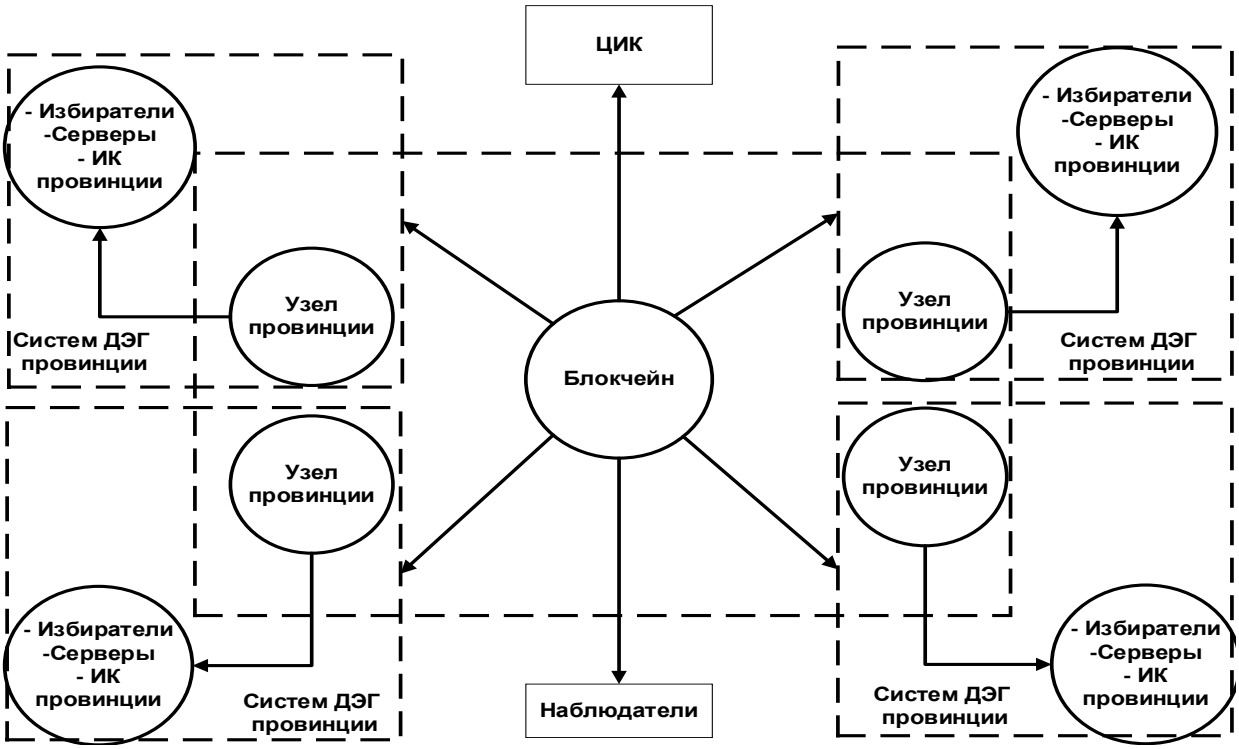

Рисунок 1 – Общая перспективная схема ДЭГ для Республике Ирак

При разработке модели ДЭГ были учтены следующие особенности избирательного процесса в арабских государствах, которые имели место на предыдущих выборах:

1. Сильное влияние субъективного (человеческого) фактора, которое выражается:

– в нарушении членами избирательных комиссий инструкций по порядку подготовки и проведения голосования;

– влиянии (в том числе путем подкупа) на действия членов избирательных комиссий заинтересованных лиц и организаций;

– влиянии на выбор избирателей религиозного (исламского) фактора и мнения старейшин;

– особенностях менталитета избирателей, осознающих свою идентичность, как часть 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.

Системы ДЭГ на провинциальном уровне представлена на рисунке 2.

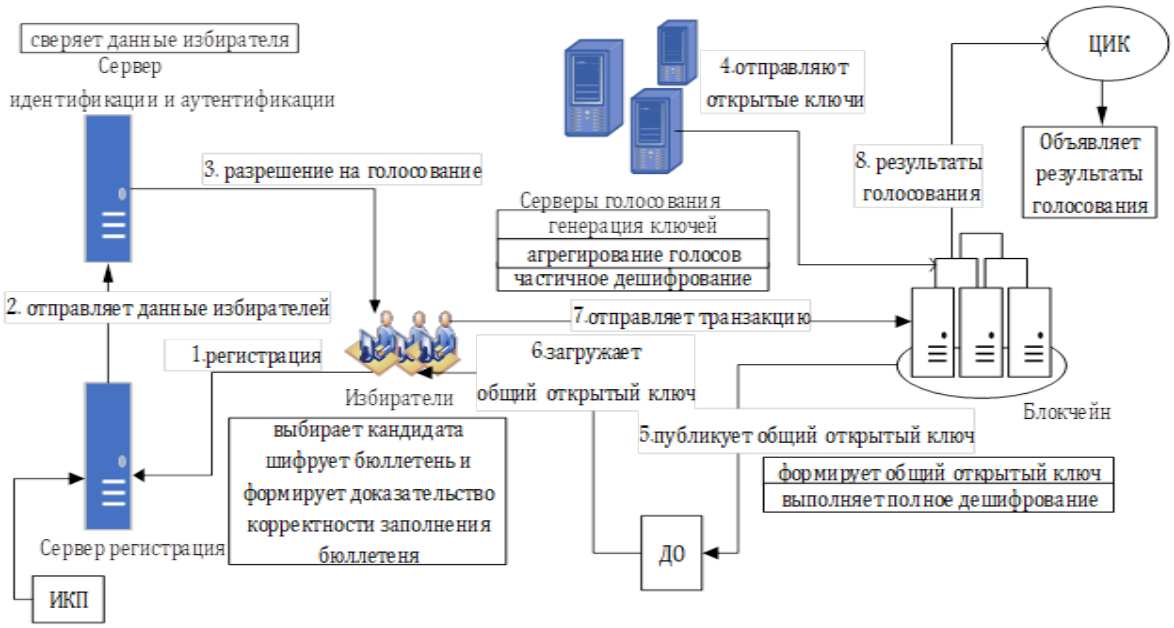

Рисунок 2 – Структура системы ДЭГ провинции

Система ДЭГ провинции включает:

- Избирателей. Избиратель – гражданин Ирака, который имеет биометрическую карту и включен в списки избирателей ДЭГ. Он должен зарегистрироваться на сайте электронной регистрации до дня голосования.
- Избирательную комиссию 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. ИКП подготавливает список избирателей и организует процесс ДЭГ.
- Наблюдателей – участники, осуществляющие наблюдение за процессом голосования и аудит результатов голосования.
- Серверы голосования партий (Серверы голосования) – выделенные или специализированные компьютеры для генерации пар ключей (открытый и закрытый ключ). 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 ИКП, 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.
- Сервер регистрации – отвечает за регистрацию избирателей в электронной форме. Избиратели до дня голосования должны зарегистрироваться онлайн на веб-сайте электронной регистрации посредством создания учетной записи.
- Сервер идентификации и аутентификации – осуществляет идентификацию и аутентификацию избирателей.
- Узел блокчейн провинции – участник, представляющий собой хранилище транзакций. В нашей системе применяется блокчейн-консорциум. Каждая провинция имеет свой собственный узел на блокчейн-консорциуме, содержащий информацию о голосовании на избирательных участках и округах для данной провинции.
- Доска объявлений (ДО) – в нее помещается общий открытый ключ.

Предлагаемая модель основана на гомоморфном шифровании с распределенным дешифрованием, и отличается от существующих систем тем, что предполагает наличие нескольких серверов, каждый из которых генерирует закрытый ключ и открытый ключ. Из открытых ключей в БЧ формируется общий открытый ключ, который передается всем голосующим. Расшифровка осуществляется частично каждым сервером, поэтому общий ключ расшифровки не формируется, что защищает от возможной атаки со стороны системной администрации. Предполагается, что серверы голосования независимы от ИК и ИКП, например, принадлежат партиям, участвующим в выборах.

В предложенной модели выполняются следующие требования безопасности информации:

- Тайна голосования. Обеспечивается за счет шифрования бюллетеня по криптосхеме Эль-Гамаля 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 после расшифрования становится известной сумма голосов, поданных за кандидата, но никто не может узнать, как проголосовал отдельный избиратель. Кроме того, обеспечивается повышенная анонимность избирателя при атаках со стороны административного ресурса. Это достигается за счет того, что в предлагаемой системе нет процедуры восстановления ключа расшифрования из распределенных до начала голосования его долей. Поэтому даже после окончания выборов администрация системы не может

воспользоваться этим ключом для расшифрования бюллетеня конкретного избирателя.

- Аутентификация избирателя. Осуществляется путем подтверждения учетной записи избирателя, имя которого заранее включено в список избирателей.
- 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.

В таблице 1 приведены количественные параметры предлагаемой модели ДЭГ.

Таблица 1. 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, остальные для основных партий.

В системе ДЭГ предлагается использовать блокчейн–консорциум с использованием смарт-контрактов, а именно Hyperledger Fabric (HF)) и алгоритм консенсуса – доказательство власти (Proof-of-Authority (PoA)), Скорость обработки транзакций – от 1000–2000 транзакций/с.

Проведен анализ стойкости блокчейн и криптоалгоритмов в условиях применения нарушителем квантового компьютера, который представляет угрозу традиционным криптосистемам с открытым ключом, а, следовательно, и информационным системам, например, ДЭГ, где используются асимметричные криптоалгоритмы. Показано, что имеющийся в настоящее время задел в построении квантово-устойчивых криптоалгоритмов и планируемая в ближайшей перспективе международная стандартизация этих криптоалгоритмов, дают уверенность в том, что эта проблема будет преодолена и применение квантово-устойчивых криптоалгоритмов в системах ДЭГ обеспечат необходимый уровень информационной безопасности.

В третьей главе разработан протокол функционирования перспективной системы ДЭГ в соответствии с выбранной моделью.

Проведен анализ криптосхем Бенало, Пэйе, Эль-Гамаля для построения протокола голосования. Результаты эксперимента по оценке времени генерации ключа, шифрования и дешифрования бюллетеня показали преимущество схемы Эль-Гамаля, поэтому эта схема использована в разрабатываемом протоколе функционирования системы ДЭГ.

Предлагаемый протокол голосования включает в себя несколько этапов: *Этап инициализации системы*. На этом этапе осуществляется генерирование серверами ключей. Открытые ключи отправляются в БЧ, где формируется общий ключ голосования *h*. БЧ помещает этот ключ на доску объявлений (ДО), где избиратели его получают. Секретные ключи хранятся на северах. Заметим, что сервера принадлежат разным партиям, что делает маловероятным сговор всех партий сразу;

Этап регистрация избирателей. 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.);

Этап идентификации и аутентификации избирателей. Перед днем выборов ИКП передает список избирателей на сервер идентификации и аутентификации по защищенному каналу. Сервер сверяет данные избирателя, полученные от ИКП, с данными избирателя, отправленными с сервера регистрации;

Этап голосования. Каждый избиратель с помощью программного обеспечения на своем устройстве выбирает кандидата (кандидатов) из списка кандидатов, шифрует свой голос (создает криптограмму по схеме Эль –Гамаля из двух частей: *Ai, Bi* и доказательство корректности выполнения операции шифрования) и отправляют бюллетени и доказательства корректности их заполнения в БЧ;

Этап расшифровки бюллетеней. БЧ проверяет доказательства и передает первые части криптограмм *Ai* на серверы голосования. Они делают предварительную расшифровку своими секретными ключами, агрегируют расшифровки от всех избирателей и отправляют их в БЧ. В БЧ хранятся вторые части криптограмм *Bi*. 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.

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

Математическая модель протокола голосования обосновывается следующими соотношениями.

Генерация ключей:

Каждый сервер голосования партии (сервер голосования) E_t генерирует секретный ключ s_t (случайное число) $1 < s_t < p - 1$, затем формируют открытый ключ:

$$h_t = g^{s_t} mod\ p, \quad (1)$$

где p – простое число, g – примитивный элемент поля Галуа GF(p), t = 1, 2, …, T, T – количество серверов. Сгенерированные открытые ключи h_t передаются в БЧ, закрытые ключи s_t остаются на хранении на серверах до этапа расшифровки бюллетеней.

БЧ формирует общий открытый ключ голосования:

$$h_{общ.} = g^{s_1} \cdot g^{s_2} \cdot \ldots \cdot g^{s_T} (mod\ p) = g^{s_1+s_2+\ldots+s_T} mod\ p\,. \quad (2)$$

БЧ помешает общий открытый ключ ($h_{общ.}$) 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.

Шифрование

Избиратель V_i, голосуя за j-го кандидата, выбирает одно число из двух возможных значений: $v_{ij} = (0,1)$, где v_{ij} = 1 – «за», v_{ij} = 0 – «против» j-го кандидата, где $i = 1,2,\ldots,n$, n – количество избирателей, $j = 1,2,\ldots,k$. k – количество кандидатов и шифрует свой голос следующим образом:

$$(A_i, B_i) = \left(g^{r_i}, h_{общ.}{}^{r_i} . G^{v_{ij}}\right), \quad (3)$$

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 зашифрованного бюллетеня избирателя.

Избиратель V_i формирует доказательство корректности заполнения бюллетеня. Зашифрованный бюллетень и доказательство корректности избиратель отправляет в БЧ. БЧ проверяет корректность заполнения ИзБ. После проверки избиратель получает сообщение о том, что его голос принят и учтен.

Частичное расшифровывание:

После окончания времени голосования серверы голосования получают от блокчейна первые части криптограммы избирателей и делают предварительную расшифровку своими секретными ключами s_j.

Например, сервер E_t выполняя частичную расшифровку бюллетеней каждого избирателя по кандидату j, вычисляет:

$$W(j)_{1t} = A_1^{s_t},\ W(j)_{2t} = A_2^{s_t}, \ldots, W(j)_{nt} = A_n^{s_t}, \quad (4)$$

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

$$X(j)_t = \prod_i W(j)_{it}. \quad (5)$$

Произведение $X(t)_t = \prod_i W(j)_{it}$ каждый сервер отправляет в БЧ.

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 голосования до завершения процедуры голосования.

Полное расшифрование и подсчет голосов избирателей

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):

$$X(j) = (W_{11} \cdot W_{21} \cdot \ldots \cdot W_{n1}) \cdot (W_{12} \cdot W_{22} \cdot \ldots \cdot W_{n2}) \cdot \ldots \cdot (W_{1T} \cdot W_{2T} \cdot \ldots \cdot W_{nT}) \quad (6)$$

Перегруппировав множители в данном выражении, получим:

$$X = (W_{11} \cdot W_{12} \cdot \ldots \cdot W_{1T}) \cdot (W_{21} \cdot W_{22} \cdot \ldots \cdot W_{2T}) \cdot \ldots \cdot (W_{n1} \cdot W_{n2} \cdot \ldots \cdot W_{nT}) = g^{\sum s_t} \cdot g^{\sum r_i} \bmod p \quad (7)$$

Далее в БЧ вычисляется произведение вторых частей криптограмм всех избирателей $Y(j) = \prod_i B_i$:

$$Y(j) = B_1 \cdot B_2 \cdot \ldots \cdot B_n = \left(h_{общ.}{}^{r_1} \cdot G^{v_{1j}}\right) \cdot \left(h_{общ.}{}^{r_2} \cdot G^{v_{2j}}\right) \cdot \ldots \cdot \left(h_{общ.}{}^{r_n} \cdot G^{v_{nj}}\right) \bmod p = h_{общ.}{}^{\sum r_i} \cdot G^{\sum v_i} (\bmod p) \quad (8)$$

и находится:

$$\frac{Y(j)}{X(j)} = \frac{h_{общ.}^{\sum_{i=1}^{n} r_i} \cdot G^{\sum_{i=1}^{n} v_i} (mod\ p)}{g^{\sum_{i=1}^{n} s_t} \cdot g^{\sum_{i=1}^{n} r_i} (mod\ p)} = \frac{g^{\sum_{i=1}^{n} s_t \sum_{i=1}^{n} r_i} \cdot G^{\sum v_i}}{g^{\sum_{i=1}^{n} s_t} \cdot g^{\sum_{i=1}^{n} r_i}} = G^{\sum_{i=1}^{n} v_i}\ mod\ p. \quad (9)$$

Подсчет голосов (вычисление суммы голосов), поданных за j-го кандидата) осуществляется путем логарифмирования результата (9):

$$\sum_{i=1}^{n} v_{ij} = log_G\, G^{\sum_{i=1}^{n} v_{ij}}\ mod\ p. \quad (10)$$

Логарифм вычисляется по заранее составленной таблице, в которой до начала выборов, в зависимости от числа участников и параметра G, посчитаны возможные результаты голосования.

Проанализированы наиболее опасные угрозы, которые могут существовать в предлагаемой системе ДЭГ и представлены доказательства возможности их предотвращения или блокирования. Отметим, что основные угрозы связаны с влиянием субъективного фактора.

С целью демонстрации работоспособности, предложенной модели ДЭГ и отдельных этапов протокола, был разработан программный комплекс, состоящий из нескольких программ и интерфейсов для участников избирательного процесса. В комплексе есть возможность симулировать наличие нескольких серверов голосования через единый интерфейс. Графические интерфейсы разработаны на языке программирования *Python 3.10* с использованием библиотеки PyQt5. По результатам моделирования предложенный протокол подтвердил свою работоспособность.

В четвертой главе исследованы два вида атак на систему ДЭГ со стороны избирателя. Первый вид атаки заключается в том, что избиратель случайно или преднамеренно указывает некорректное число, соответствующее его выбору ЗА или ПРОТИВ по конкретному кандидату (например, использует числа 2 или (–1), поданные за какого-то кандидата, а по правилам должны использоваться только числа 1 или 0).

Второй вид атаки заключается в нарушении избирателем, правила голосования по количеству поданных голосов ЗА в одном бюллетене. То есть необходима проверка заполнения ИзБ по общему числу голосов *m*, поданных ЗА. Это число должно быть в интервале: $m_{min} \leq m \leq m_{max}$, где $m_{\min}$, $m_{\max}$ – минимальное и максимальное число кандидатов соответственно, за которых может проголосовать избиратель согласно правилу голосования, установленному ИК. Этот способ проверки бюллетеня назван в работе проверкой бюллетеня в целом.

Нетривиальность обоих видов проверок заключается в том, что она должна проводиться по бюллетеню в зашифрованной форме.

В существующих методах проверки корректности заполнения ИзБ, избиратель (доказывающий) формирует доказательство того, что он заполнил свой бюллетень, исходя из значения (0,1), и отправляет их проверяющему. Проведены исследования двух методов проверки корректности заполнения бюллетеня по отдельному кандидату с использованием методов доказательства с нулевым разглашением секрета: на основе равенства логарифмов и на основе правильности перемешивания голосов в бюллетене. Оценена сложность реализации этих методов, сделаны выводы о целесообразности их использования в системах ДЭГ.

Отмечено, что в известном методе проверки корректности заполнения ИзБ по всем кандидатам (в целом), избиратель указывает общее количество поданных голосов «ЗА» (m') в открытом виде, что, на наш взгляд, является слабостью этого метода, так как позволяет посторонним лицам проводить оценку интенсивности хода голосования. В этой связи предложен метод обнаружения некорректного заполнения бюллетеня в целом, устраняющий этот недостаток.

Метод основывается на криптосистеме Эль-Гамаля и позволяет контролирующему органу (блокчейну) убедиться в том, что избиратель корректно выбрал количество кандидатов из диапазона возможных значений без раскрытия количества поданных голосов.

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, выполняя вычисления:

– 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: $U_{D_i} = y_i^{r_i} g^{v_i}$.

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

– генерирует $e \in Z_p$, вычисляет $X' = h^e$, $x = e + \sum_{i=1}^{k} r_i \cdot f$.

– посылает в БЧ доказательство: $(U'_{\sum}, X', x)$.

БЧ выполняет проверку доказательства:

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

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: $h^x =^? X' \cdot V$.

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

Выполнение сравнения свидетельствует о том, что 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: $V = (\prod_{i=1}^{k} B_i / U_\Sigma \cdot g^{-v_{k+1}})^f = (h^{\Sigma r_i} \cdot g^{\sum_{i=1}^{k} v_i} g^{-\sum_{i=1}^{k+1} v_i} \cdot g^{v_{k+1}})^f$.

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

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

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

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.

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 известными методами 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

В диссертационной работе были получены следующие основные результаты:

1. Проанализированы особенности избирательного процесса на парламентских выборах в республике Ирак и арабских государствах. Рассмотрены основные преимущества внедрения дистанционного электронного голосования (ДЭГ) на выборах и возникающие при этом угрозы избирательному процессу.

2. Проанализированы принципы построения современных систем ДЭГ на основе микс-сетей, слепой подписи, гомоморфного шифрования и технологии блокчейн. Результаты анализа показали, что гомоморфное шифрование обладает рядом преимуществ и поэтому эта схема взята за основу для дальнейшего исследования.

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, что гарантирует полноту подсчета голосов, сокращает время подсчета голосов и снижает нагрузку на блокчейн-сеть.

4. Разработан протокол функционирования перспективной системы дистанционного электронного голосования на основе гомоморфного шифрования с распределенным дешифрованием, обеспечивающий защищенность от атаки, нацеленной на нарушение анонимности избирателя со стороны административного ресурса системы, за счет использования разделенного дешифрования, при котором никто из участников системы не имеет доступа к ключу дешифрования. Дано математическое описание преобразований предложенного протокола голосования. Функционирование протокола апробировано на разработанном макете системы ДЭГ, что подтверждает его реализуемость.

5. Разработан метод проверки корректности заполнения бюллетеня избирателем, обеспечивающий скрытность волеизъявления избирателя по отдельным кандидатам и по всем кандидатам в целом, позволяющий контролирующему органу (блокчейну) убедиться в том, что избиратель корректно 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.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

Научные статьи, опубликованные в рецензируемых научных изданиях

1. 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. DOI:10.31854/1813-324X-2021-7-2-102-109.

2. Салман В.Д. Методы защиты от угрозы неправильного заполнения избирательного бюллетеня в системе дистанционного электронного голосования / В.Д. Салман, В.А. Яковлев // Труды учебных заведений связи. 2023. Т. 9. № 1. С. 21–27. DOI:10.31854/1813-324X-2023-9-1-21-27.

3. 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 Государственной противопожарной службы МЧС России». 2023. №. 2. С. 91-101.

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

Научные статьи, опубликованные в изданиях, индексируемых в международных база данных

5. Salman W. Analysis of the traditional voting system and transition to the online voting system in the republic of Iraq / Salman W., Yakovlev V., Alani S. //2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, – 2021. – С. 1-5. DOI: 10.1109/HORA52670.2021.9461387.

Научные статьи, опубликованные в других изданиях и материалах научных конференций

6. Салман В.Д. Требования к системам электронного голосования / В.Д. Салман // Национальная безопасность России: актуальные аспекты. 2020. С. 14–17.

7. Салман В.Д. Анализ системы голосования в республике Ирак и пути перехода к системе электронного голосования / В.Д. Салман // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). X Юбилейная международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. С. 400–404.

8. Салман В.Д. Подход к улучшению существующей иракской системы голосования с использованием дистанционного голосования / В.Д. Салман // Теория и практика обеспечения информационной безопасности. Москва. 2021. С. 11–19.

9. Салман В.Д. Способ обеспечения анонимности электронного голосования от атаки отслеживания голосов отдельных избирателей / В.Д. Салман, В.А. Яковлев, Д.А. Орлов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2022. С. 723–726.

10. Салман В.Д. Исследование системы электронного голосования на основе гомоморфного шифрования с распределенным дешифрованием / В.Д. Салман, В.А. Яковлев, Д.С. Шевцов // Научный журнал «защищенные системы связи». 2022. № 2. С. 86–92.

11. Салман В.Д. Оценка сложности метода проверки корректности заполнения избирателем бюллетеня в системе дистанционного электронного голосования / В.Д. Салман // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023) XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. Т. 1. С. 880–885.

12. Салман В.Д. Метод проверки корректности заполнения избирательного бюллетеня в системе дистанционного электронного голосования / В.Д. Салман, В.А. Яковлев // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023) XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. Т. 1. С. 885–890.

13. Салман В.Д. Гомоморфная криптосистема для подсчета голосов / В.Д. Салман // Новые импульсы развития: вопросы научных исследований. Саратов. 2020. № 1–1. С. 94–100.

Подписано в печать 22.12.2023. Формат 60×84 1/16.
1,0 а.л. Тираж 100 экз.

Отпечатано в СПбГУТ, 193232, Санкт-Петербург, пр. Большевиков, д. 22, корп. 1