Научная статья
УДК 519.85

МОДЕЛЬ И ПРОТОКОЛ ПЕРСПЕКТИВНОЙ СИСТЕМЫ ДИСТАНЦИОННОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ ДЛЯ РЕСПУБЛИКИ ИРАК НА ОСНОВЕ ГОМОМОРФНОГО ШИФРОВАНИЯ

✉Салман Васан Давуд.
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия
✉salman.vd@sut.ru

Аннотация. Описана существующая система голосования в Республике Ирак, которая использовалась на выборах 2021 г., отмечены присущие ей угрозы и недостатки. Проанализированы принципы построения современных систем дистанционного электронного голосования. Сформированы требования к безопасности системы дистанционного электронного голосования. Разработана модель и протокол перспективной системы дистанционного электронного голосования Ирака, основанной на гомоморфном шифровании с распределенным дешифрованием, которая учитывает особенности избирательной системы республики. Проанализированы наиболее вероятные угрозы информационной безопасности в этой системе и способы их предотвращения. Разработан демонстрационный макет модели дистанционного электронного голосования. Сделан вывод, что предлагаемый протокол отвечает требованиям безопасности системы голосования: обеспечивается тайна голосования и анонимность голосующего; аутентификация избирателя; уникальность и точность голосования; подтверждение голосования.

Ключевые слова: дистанционное электронное голосование, выборы в Ираке, криптосистема Эль-Гамаля, микс-сети, слепая подпись, гомоморфное шифрование с распределенным ключом

Для цитирования: Салман Васан Давуд. Модель и протокол перспективной системы дистанционного электронного голосования для Республики Ирак на основе гомоморфного шифрования // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2023. № 2. С. 91–111.

Scientific article

MODEL AND PROTOCOL OF A PROMISING SYSTEM OF REMOTE ELECTRONIC VOTING FOR THE REPUBLIC OF IRAQ BASED ON HOMOMORPHOUS ENCRYPTION

✉Salman Vasan Davud.
Saint-Petersburg state university of telecommunications them. prof. M.A. Bonch-Bruevich, Saint-Petersburg, Russia
✉salman.vd@sut.ru

Abstract. The existing voting system in the Republic of Iraq, which was used in the 2021 elections, is described, its inherent threats and shortcomings are noted. The principles of building modern systems of remote electronic voting are analyzed. The requirements for the security of the remote electronic voting system have been formed. A model and protocol for a promising system of remote electronic voting in Iraq based on homomorphic encryption with distributed decryption, which takes into account the features of the electoral system of the republic, has been developed. Analyzed the most likely threats to information security in this system and ways to prevent them. A demonstration layout of the remote electronic voting model has been developed. It is concluded

that the proposed protocol meets the security requirements of the voting system: the secrecy of the vote and the anonymity of the voter are ensured; voter authentication; uniqueness and accuracy of voting; vote confirmation.

Keywords: remote electronic voting, elections in Iraq, ElGamal cryptosystem, mix networks, blind signature, distributed key homomorphic encryption

For citation: Salman Vasan Davud. Model and protocol of a promising system of remote electronic voting for the Republic of Iraq based on homomorphous encryption // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2023. № 2. P. 91–111.

Введение

Голосование играет важную роль в построении демократической страны. Выборы позволяют населению свободно выразить свое волеизъявление к кандидатам. Конфиденциальность избирательного процесса имеет важное значение для самой демократии. Основными недостатками традиционных методов выборов являются фальсификация результатов голосования, проблемы с подсчетом голосов, длительный период подсчета голосов и высокая стоимость печати бюллетеней. Сегодня развивается множество новых технологических инноваций. Электронное голосование становится популярной тенденцией. Внедрение безопасных систем электронного голосования очень важно в каждой стране [1, 2]. Основные преимущества электронного голосования:

– содействие участию в выборах граждан, проживающих за рубежом;

– расширенный доступ к процессу голосования для избирателей с ограниченными возможностями или имеющих другие физические трудности для присутствия на избирательном участке и использования имеющихся там устройств;

– более быстрое предоставление результатов голосования намного быстрее; упрощение процедуры и более привлекательные решения для избирателя, что означает больше возможностей для расширения участия;

– сокращение бюджетных расходов на организацию и проведение голосования [3].

В настоящее время на выборах в Ираке используется традиционный бумажный бюллетень для голосования, который имеет много недостатков. В этой связи актуален переход на системы дистанционного электронного голосования, которые уже начинают применяться в некоторых странах.

Целью работы является разработка модели и протокола системы дистанционного электронного голосования в Республике Ирак с учетом особенностей избирательного процесса. Приведен анализ существующей системы голосования в Ираке. Описан анализ принципов построения современных систем дистанционного электронного голосования (ДЭГ). Представлено детальное описание предлагаемой модели и протокола перспективной иракской системы голосования. Дан анализ угроз в системе ДЭГ и способов их предотвращения. Приведены результаты разработанного демонстрационного макета предложенной модели ДЭГ.

Анализ существующей системы голосования в Ираке. Избирательная система Республики Ирак на парламентских выборах 2021 г.

Правовая основа выборов в Республике Ирак определена Законом о выборах № 9 от 2020 г. [4]. В соответствии с этим законом установлено 83 избирательных участка в 18 провинциях республики, каждый избирательный участок состоит из нескольких местных избирательных округов. Каждый избирательный округ обслуживает примерно 450 избирателей. В иракском парламенте согласно конституции 329 мест. 320 общественных мест распределяются между мухафазами (провинциями) в их избирательных округах и в соответствии с их административными границами (рис. 1). Остальные девять мест распределяются по конфессиям (христиане, езиды, сабейцы, шабаки и курды-Филен).

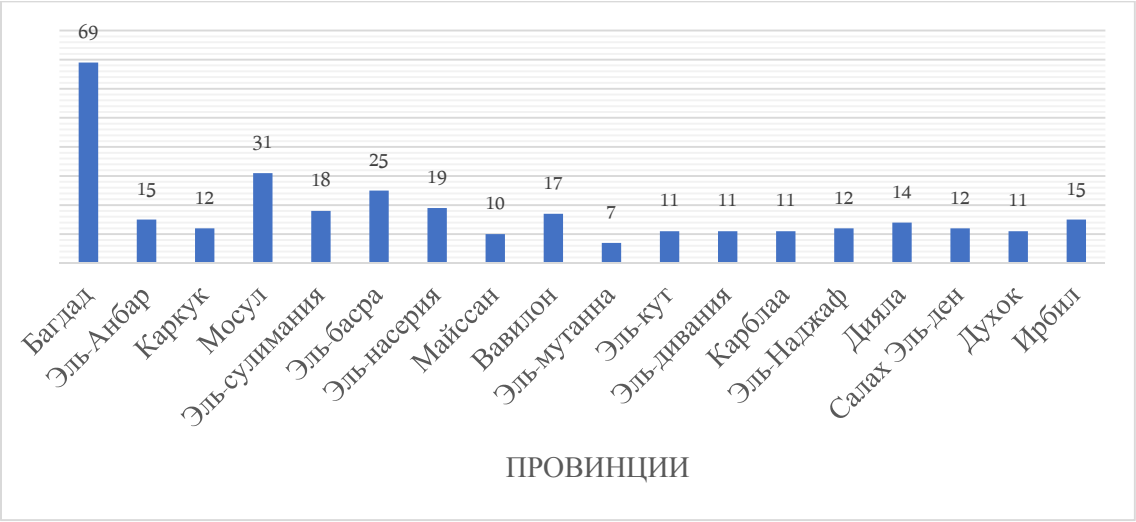

Рис. 1. **Распределения общих мест в парламенте**

Кандидаты избираются по открытому и единому списку, а каждому конкретному региону выделено определенное количество мест в соответствии с Законом о выборах. Не менее 25 % членов парламента должны составлять женщины.

Кандидаты в избирательном округе, независимо от того включены они в общий список или представлены самостоятельно, по итогам голосования расставляются в соответствии с количеством действительных голосов, полученных ими от самого высокого к самому низкому. Тот кандидат, который получил наибольшее количество голосов (мужчины или женщины), считается победителем. Если два или более кандидата имеют равное количество голосов, то для получения места используется лотерея в присутствии кандидатов с равными голосами или их уполномоченных.

Избиратель должен лично прийти на указанный избирательный округ по месту жительства. Согласно Закону о выборах, он может проголосовать только за одного кандидата, который участвует в его местном избирательном округе.

Легитимные избиратели, имеющие право голоса, должны иметь иракское гражданство, возраст не менее 18 лет, быть зарегистрированным в списке избирателей и иметь биометрическую карту избирателя.

Легитимные кандидаты должны иметь иракское гражданство, возраст не менее 30 лет, свидетельство об образовании (минимальная степень бакалавра) и не должны быть судимы. Кандидат может участвовать в выборах на конкретном избирательном участке, где он проживает [5].

В табл. 1 приведены факты о парламентских выборах 2021 г. в Ираке [6].

Таблица 1

Факты о парламентских выборах 2021 г. в Ираке

Факты	Количество	Комментарии
Иракское население	41 млн	2021 г.
Провинции	18	–
Избирательный участок	83	В каждом избирательном участке создается несколько местных избирательных округов, каждый местный избирательный округ обслуживает не более 450 избирателей

Факты	Количество	Комментарии
Зарегистрированные избиратели	22 116 368	На выборах 2021 г.
Зарегистрированные политические партии	108	3 225 кандидатов
Количество проголосовавших избирателей	9 629 601	Поданные голоса
Количество правильных голосов	8 854 025	Засчитаны голоса
Количество неверных голосов	775 576	Не засчитаны голоса
Общее количество проголосовавших	43,54 %	–

Требования к системе голосования

Основные требования к системе голосования в Ираке определены Законом от 5 ноября 2020 г. № 9 «Выборы иракского парламента» [4]:

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.

Процедуры выборов в Ираке

Рассмотрим технические и методологические методы, которые были использованы на выборах 2021 г. при избрании парламента. Опишем процедуру выборов более подробно по этапам. На рис. 2 показана общая блок-схема нынешней иракской системы голосования.

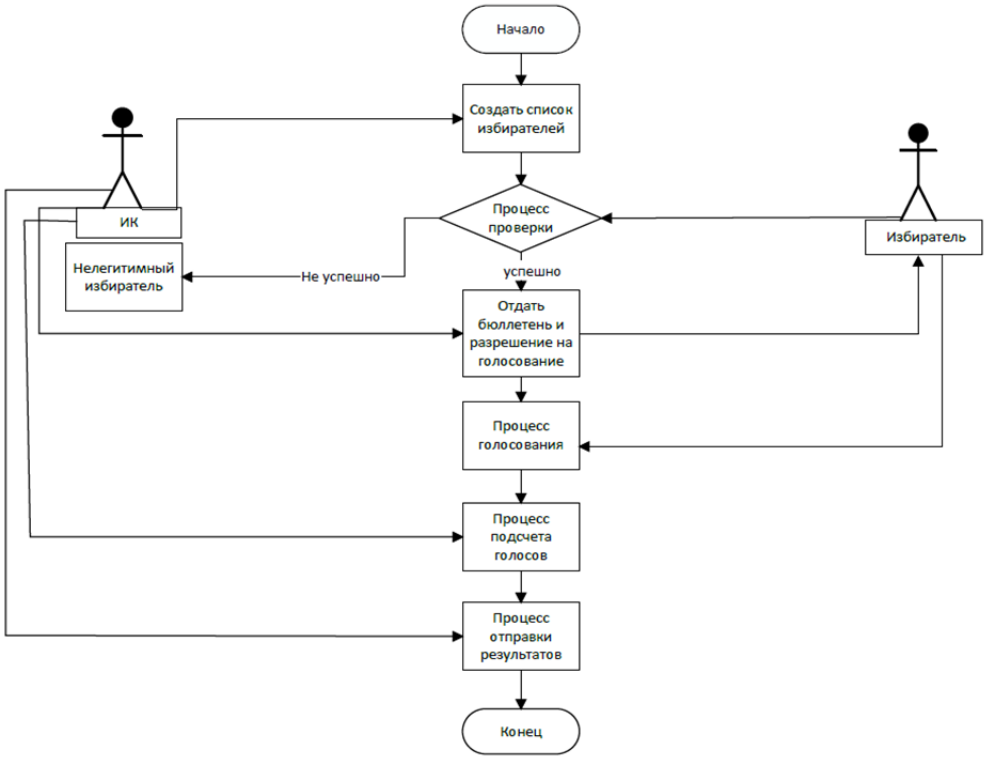

Рис. 2. **Алгоритм иракской системы голосования 2021 г. (ИК – избирательная комиссия)**

Этап регистрации и подготовка списков избирателей

В 2021 г. ИК использовала технологию биометрической регистрации и верификации. Избиратель должен был лично прийти на указанный избирательный участок по месту жительства и заполнить регистрационную форму. Сотрудник избирательного участка с помощью специальных устройств снимает десять отпечатков пальцев избирателя и делает его фотографию. После этого избиратель получает свою биометрическую карту, данные которой хранятся в базе данных регистрации избирателей на указанном избирательном участке. Каждый избирательный участок должен подготовить список избирателей за несколько дней до дня голосования.

Этап идентификации и аутентификации избирателя

ИК использует электронные устройства для проверки данных избирателей. Избиратель должен показать свою биометрическую карточку участковому сотруднику. После чего сотрудник помещает карточку избирателя на электронное устройство проверки. 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. Сотрудник проверяет имя избирателя в бумажном списке избирателей. При успешной проверке сотрудник выдает избирателю бумажные бюллетени.

Этап голосования

Выборы проходят в один день с 7:00 утра до 18:00 вечера. Перед голосованием руководитель избирательного участка вручает по 500 бюллетеней каждому руководителю избирательного округа. После успешного завершения процесса проверки данных, избиратель выбирает своего кандидата и помечает бюллетень специальной ручкой. На этой специальной ручке нанесен логотип избирательной комиссии. Далее, избиратель помещает бюллетень в электронное устройство для подсчета голосов (сканер). После этого избиратель должен обмакнуть палец правой руки в чернила для того, чтобы он не смог голосовать дважды.

Этап подсчета голосов и отправки результатов в Центральную избирательную комиссию

После завершения голосования начинается процесс подсчета голосов. ИК использует электронное устройство для подсчета голосов. Процесс подсчета голосов на избирательном участке проходит в два этапа:

1. Электронный подсчет и сортировка голосов на избирательном участке с использованием электронного устройства подсчета и сортировки (PCOS). Далее, осуществляется отправка результатов из всех избирательных участков в центральный офис ИК по каналам спутниковой связи с помощью устройства RTS.

2. Ручной подсчет и сортировка голосов в каждом округе избирательного участка. Для этого урна (ящик) для голосования вскрывается в присутствии представителей политических партий, наблюдателей или других лиц, заинтересованных в проверке процесса подсчета голосов. Сотрудник избирательного округа подсчитывает бумажные бюллетени, оказавшиеся внутри ящика. Общее количество бюллетеней внутри ящика и не использованных бюллетеней должно быть равно количеству бюллетеней, полученных руководителем избирательного округа до начала голосования. Затем проводится подсчет действительных и недействительных бюллетеней и подсчет голосов, поданных за каждого кандидата. Если обнаружится расхождение между количеством голосов, выданных электронным счетным устройством, и количеством голосов, полученных при ручном подсчете, то ручной подсчет бюллетеней повторяется еще раз. Если при повторном подсчете

будет расхождение между электронным и ручным подсчетом более чем на 5 %, то об этом будет объявлено партиям и наблюдателям, 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 (ЦИК). В ЦИК голоса сортируются, анализируются, и окончательные результаты голосования объявляются на веб-сайте ЦИК и по телевидению.

Рассмотренная система, безусловно, является шагом вперед по сравнению с предыдущей системой [5]. Однако она, несмотря на все свои достоинства, имеет ряд недостатков, не обеспечивающих защиту системы голосования от ряда угроз.

Анализ угроз и недостатков существующей системы голосования

1. Система использует бумажные бюллетени для голосования, это требует дополнительных существенных затрат на их изготовление.

2. Нарушение второго требования к системе голосования. Во время выборов 2021 г. было установлено, что сотрудники избирательных участков могут участвовать в фальсификации результатов выборов для конкретной партии, или партии назначают своих собственных сотрудников на избирательных участках, которые изменяют результаты голосования (https://al-ain.com/article/iraq-percentage-legislative-elections).

3. Нарушение третьего требования к системе голосования. Результаты, объявленные центрами, отличаются от предварительных результатов, полученных на избирательных участках при ручном подсчете голосов. Также имели место случаи использования голосов тех законных избирателей, которые не захотели (не смогли) принимать участие в голосовании.

4. Кража или уничтожение ящиков для голосования с целью изменения результата голосования за определенного кандидата.

Эти недостатки и угрозы традиционной системы голосования в основном обусловлены влиянием человеческого фактора и технологией обработки бумажных бюллетеней, которые во многом могут быть преодолены при переходе к системам ДЭГ. Рассмотрим возможности систем электронного голосования с точки зрения обеспечения безопасности голосования.

Анализ принципов построения современных систем ДЭГ

Будем считать, что система ДЭГ включает в себя следующие элементы: избиратель, ИК, наблюдатель, доска объявлений или блокчейн (БЧ), сервер или серверная платформа. Рассмотрим несколько вариантов систем ДЭГ, обращая внимание в первую очередь на удовлетворение ими требований безопасности избирательного процесса.

Требования к безопасности системы ДЭГ:

– тайна голосования. Результат голосования каждого избирателя должен оставаться втайне от других участников, включая избирательную комиссию;

– анонимность. Никто не может узнать, кто подал голос за того или иного кандидата;

– аутентификация избирателя. Голосовать могут только уполномоченные избиратели;

– уникальность. Избиратель может голосовать только один раз;

– точность. Система голосования должна вести корректный учет голосов;

– подтверждение голоса. Система голосования должна отправить электронное письмо избирателю, чтобы оповестить, что его голос был принят системой правильно.

Системы ДЭГ на основе микс-сетей

Микс-сети – метод создания анонимных каналов, предложенный Д. Чаумом [7]. Рассмотрим следующую систему голосования, основанную на микс-сетях [8–11]:

Этап инициации:

– схема Эль-Гамаля используется для генерации ключа, шифрования и дешифрования бюллетеня [12].

Этап голосования:

– избиратель выбирает своего кандидата;

– избиратель шифрует свой бюллетень $Enc(C_i)$ и отправляет его на сервер перемешивания, где *Enc ()* – функция шифрования;

– сервер перемешивания получает зашифрованный бюллетень $Enc(C_i)$;

– сервер выполняет маскировку, выбирает перестановку $\pi(1,2,..,k)$ и перемешивает в соответствии с этой перестановкой $Enc(C_i)$, отправляет ее в ИК.

Подсчет голосов и расшифровка:

– ИК расшифровывает зашифрованный бюллетень. Далее, подсчитываются и объявляются результаты выборов.

За счет шифрования обеспечивается тайна голосования. Преимущество этого метода заключается в том, что невозможно установить связь между данными избирателей и их бюллетенями до этапа расшифровки и подсчета голосов, что обеспечивает анонимность. Недостатки: медленно осуществляется подсчет голосов, и может иметь место нарушение анонимности, в случае небольшого числа избирателей на выборах. Сервер отвечает за сбор зашифрованных голосов, если он нечестный, то сервер может заменить результат голосования. Избиратель не может проверить принят ли его голос. Также в этой схеме существует возможность нарушения аутентификации избирателя, так в выборах может участвовать нелегитимный избиратель. Нарушения уникальности, связанные с тем, что избиратель может проголосовать дважды. Для предотвращения сговора между сервером и ИК используется не один сервер, а несколько серверов. В этом случае сервера передают бюллетени избирателей друг другу, а последний сервер передает бюллетени в ИК.

Системы ДЭГ на основе слепой подписи

Рассмотрим следующую систему голосования, основанную на слепой подписи [13, 14]:

Этап инициации:

– каждый избиратель генерирует свою пару ключей по схеме РША [15]: $d_{\text{и}}, n_{\text{и}}, e_{\text{и}}$ (закрытый/открытый ключ) и публикует открытый ключ на доске объявлений;

– избиратель, желающий принять участие в голосовании, генерирует свой идентификационный номер *I* (ИН);

– избиратель маскирует свой ИН:

$$I_m = m^{e_{\text{ик}}} \cdot I \; mod \; n_{\text{ик}}, \; (e_{\text{ик}}, n_{\text{ик}}) \; ,$$

где I – открытый ключ ИК; m – случайно сгенерированное целое число из диапазона $(1, 2, \dots, n_{\text{ик}} - 1)$, и отправляет в ИК маскированный ИН:

$$\mathrm{M_1} = \left(\mathrm{n}, \mathrm{E_{d_и}(n, I_m)}\right),$$

где $d_{\text{и}}$ – закрытый ключ избирателя; n – порядковый номер этого избирателя в списке легитимных избирателей.

Заметим, что по n нельзя определить избирателя.

– ИК подписывает маскированный ИН и отправляет обратно избирателю;

– избиратель демаскирует подписанный ИН: $\mathrm{I_s} = (\mathrm{I_{sm}})/\mathrm{m} \bmod \mathrm{n_{ик}} = \mathrm{I}^{\mathrm{d_{ик}}} \bmod \mathrm{n_{ик}}$;

Этап голосования:

– избиратель создает бюллетень с результатом своего голосования, зашифровывает его и отправляет в ИК по анонимному каналу. Далее, каждый из избирателей формирует следующее сообщение:

$$M_2 = (P, E_{d_v}(I, I_s, V),$$

где P – это любое число.

Подсчет голосов и расшифровка:

– избиратель отправляет по анонимному каналу ключ для расшифровки сообщения;

– ИК дешифрует сообщение и публикует результаты голосования.

Система обеспечивает тайну голосования, анонимность и аутентификацию избирателя. Анонимность за счет избирателя маскирует его ИН и отправляет его в ИК, которая подписывает «вслепую» замаскированный ИН, используя анонимный канал.

Недостатки: необходимо выполнить дополнительные процедуры, связанные с идентификационной подписью избирателя. Процесс подсчета голосов идет медленно. Существует возможность фальсификации результатов голосования [16]. Избиратель не может проверить принят ли его голос.

Системы ДЭГ на основе гомоморфного шифрования

Система голосования на основе системы шифрования с аддитивным гомоморфизмом может быть представлена следующим образом [17, 18]:

Этап инициации:

– сервер генерирует открытый и закрытый ключи криптосистемы; гомоморфного шифрования Эль-Гамаля [12]: закрытый ключ s, $1 \le s \le p-1$, s выбирается случайным, открытый ключ вычисляется как $h = g^s mod\, p$, где p – простое число; g – примитивный элемент поля Галуа GF(p); h передаётся в БЧ;

– БЧ передает открытый ключ h всем избирателям. Секретный ключ s хранится на сервере или может быть разделен на доли и находиться у хранителей ключа до окончания выборов.

Этап голосования:

– каждый избиратель выбирает кандидата (кандидатов) из списка кандидатов;

– шифрует свой голос с помощью открытого ключа в виде пары чисел: $C_i = Enc(M_i) = (x_i, y_i) = (g^r, h^r \cdot G^{m_i}) modp$ и отправляет его в БЧ, где $m_i \in \{0,1\}$ – выбор избирателя; r – случайное число, $1 \le r \le p-1$; G – примитивный элемент поля GF(p), (x_i, y_i) – две части криптограммы C_i;

Подсчет голосов:

– после завершения голосования в БЧ осуществляется агрегирование голосов всех избирателей: $T = C_1 * C_2 * \ldots * Cm$ и отправляет криптограмма T в ИК, где T – результаты агрегирования голосов;

– ИК расшифровывает T с помощью закрытого ключа: $R = Dec(T)$, сумма всех голосов вычисляется так: $\sum m_i = \log_G G^{\sum m_i} modp$, и объявляет результаты выборов.

Данная система обеспечивает тайну голосования, анонимность и точность. Анонимность при применении гомоморфных криптосистем обеспечивается за счет гомоморфной суммы при подсчете количества голосов.

Преимуществом гомоморфного шифрования является эффективный подсчет голосов (в отличие от схем слепой подписи и микс-сетей), поскольку голоса не нужно расшифровывать по отдельности; простота реализации; безопасность таких схем обеспечивается криптостойкостью используемых криптосистем [16]. Никто не может узнать результаты голосования до завершения голосования. Вместо того чтобы скрывать личность избирателей, эта схема скрывает содержимое самого бюллетеня. При подсчете голосов бюллетень необходимо расшифровать, чтобы выявить результаты выборов избирателей.

Этого можно избежать, зашифровав бюллетень с использованием гомоморфного шифрования, поскольку при умножении зашифрованных бюллетеней они дают результат, который является зашифрованным итогом выборов [19]. Нет необходимости в анонимном канале (в отличие от схем слепой подписи).

Ввиду преимуществ гомоморфной системы, автор будет использовать ее в модели для обеспечения безопасности избирательного процесса.

Важность применения гомоморфного шифрования заключается в том, что оно позволяет безопасно передавать, хранить и главное обрабатывать данные в зашифрованном виде без ущерба для конфиденциальности информации [20].

Предлагается модель перспективной системы ДЭГ Ирака на основе гомоморфного шифрования с распределенным дешифрованием [21].

Модель перспективной иракской системы голосования

На рис. 3. показана общая схема системы ДЭГ в Ираке.

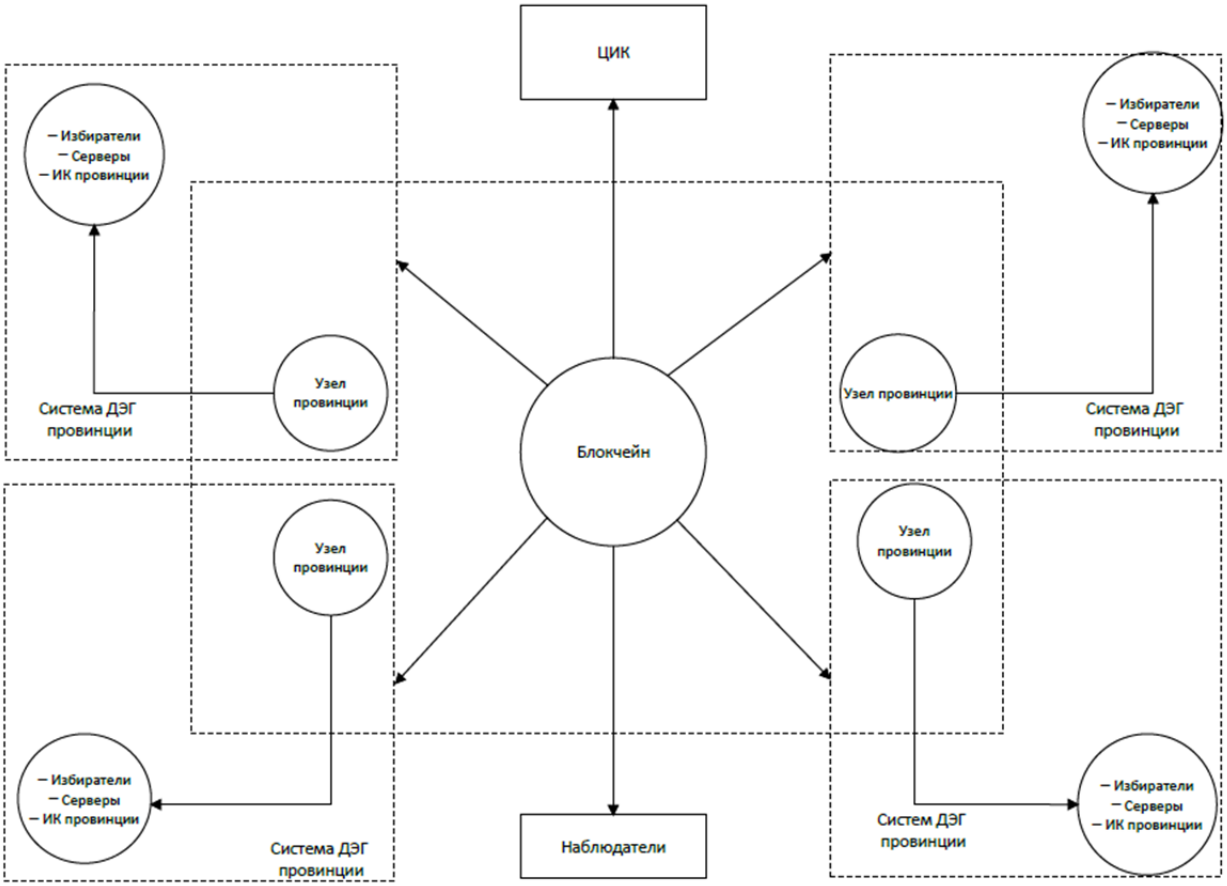

Рис. 3. **Общая перспективная схема ДЭГ для Республики Ирак**

Предлагается систему ДЭГ Республики Ирак строить в виде объединения подсистем ДЭГ провинций. Технологически такое объединение выполняется на основе БЧ, узлы которого размещаются в каждой провинции. На каждый узел замыкаются избирательные участки и округа провинций.

В табл. 2 представлены количество избирательных участков и округов в Республике Ирак на выборах 2021 г.

Таблица 2

Количество избирательных участков и округов в Республике Ирак [6]

Провинция	Кол-во избират. участков	Кол-во избират. округов	Провинция	Кол-во избират. участков	Кол-во избират. округов (примерно)
Багдад	17	1 000	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 БЧ. Для каждой провинции создается узел голосования, включающий в себя серверную платформу, состоящую из сервера регистрации, сервера аутентификации, узла БЧ в провинции, нескольких серверов голосования.

Рассмотрим функционирование системы ДЭГ на провинциальном уровне (рис. 4).

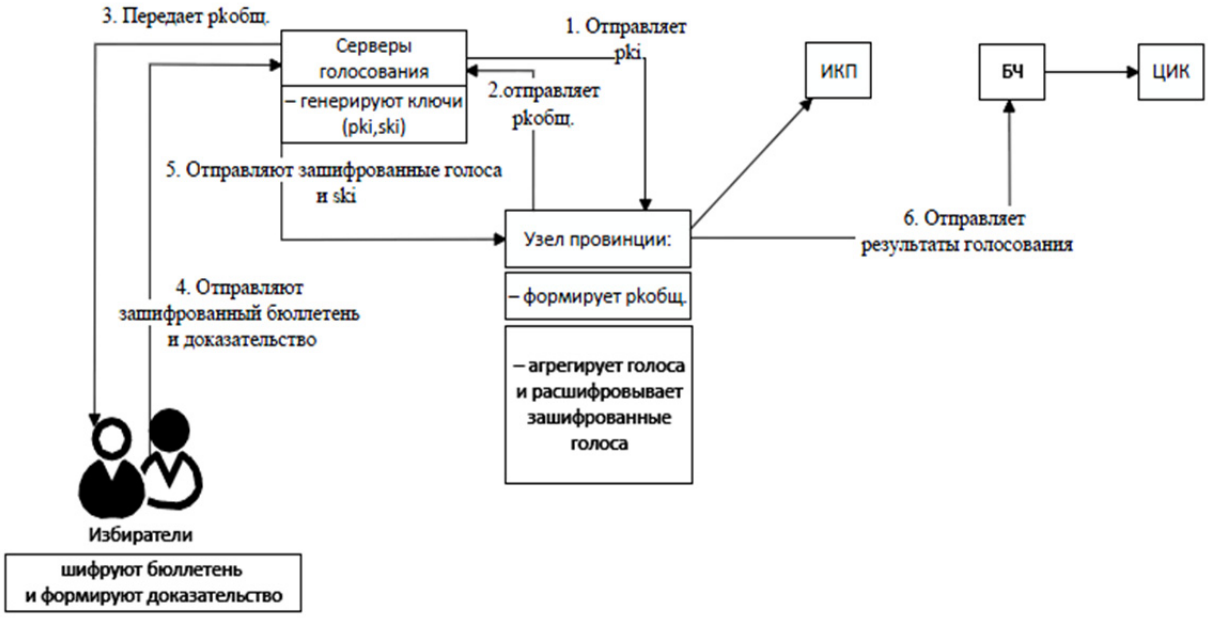

Рис. 4. **Модель системы ДЭГ для провинций Республики Ирак**

Участники системы ДЭГ в провинции

Пользователи ДЭГ:

– избиратель – гражданин Ирака, который имеет биометрическую карту и включен в списки избирателей ДЭГ, 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 (списков их 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 провинции – 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. Предполагается, что серверы принадлежат разным партиям, имеющим квоту в парламенте;

– 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 выборах в Ираке избиратель должен проголосовать только за одного кандидата;

– сервер регистрации – участник, ответственный 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 – участник, осуществляющий идентификацию и аутентификацию избирателей;

– БЧ (компонент «Распределенное хранилище данных») и узел провинции – участник, представляющий собой хранилище транзакций. В нашей системе будем использовать БЧ консорциума. Каждая провинция имеет свой собственный узел на консорциум БЧ, который содержит информацию о голосовании на избирательных участках и округах для данной провинции.

Эта модель отличается от других моделей голосования тем, что сеть БЧ-узлов распределена по провинциям, а структура модели соответствовала традиционной структуре, используемой на выборах в Ираке.

Протокол функционирования системы ДЭГ провинции

1. Этап регистрации идентификации и аутентификации избирателей.

ЦИК Ирака создает базу данных биометрической регистрации избирателей, содержащую все данные (например, отпечатки пальцев и полное имя избирателя, дату рождения и т.д.), чтобы эти данные можно было использовать на выборах. На каждых выборах ИК провинции обновляет биометрическую базу данных избирателей. До дня голосования избиратель должен заполнить электронную биометрическую регистрационную форму, предоставить отпечатки пальцев и фотографию. Перед днем выборов ИК провинции передает список избирателей на сервер идентификации и аутентификации по защищенному каналу. Для участия в ДЭК избиратель должен зайти на сайт электронной регистрации (сервер регистрация) (используя персональный компьютер, ноутбук, планшет или смартфон) и зарегистрировать свои данные (полное имя избирателя, провинция и т.д.). Сервер регистрации отправляет данные избирателей на сервер идентификации и аутентификации. В день выборов избиратель заходит на сайт выборов через свою учетную запись. Сервер идентификации и аутентификации сверяет данные избирателя, полученные от ИК, с данными избирателя, отправленными с сервера регистрации. Если проверка прошла успешно, то ему будет предоставлен доступ к серверу голосования.

2. Этап инициализации системы.

На этом этапе осуществляется генерирование ключей [12].

Предполагается, что в системе ДЭГ будет использована криптографическая схема с распределенным ключом дешифрования [21]. Для этого каждый сервер генерирует пару ключей: открытый – pk_i и закрытый – sk_i. Открытые ключи отправляются к узлу провинции, где формируется общий ключ голосования. Этот ключ отправляется узлом провинции на любой из серверов голосования, передает ключ шифрования избирателя. Секретные ключи хранятся на серверах. Заметим, что сервера принадлежат разным партиям, что исключает сговор между ними.

3. Этап голосования, подсчет голосов и объявление результатов выборов.

Каждый избиратель выбирает кандидата из списка кандидатов, шифрует свой голос с помощью программного обеспечения на устройстве избирателя и отправляет его на серверов голосования, а затем сервера голосования направляют его к узлу провинции. После завершения голосования на узле провинции осуществляется агрегирование голосов, на серверах выполняется частичная расшифровка, и результат отправляется на узел провинции. Полная расшифровка выполняется на узле провинции. Далее, узел провинции направляет результаты в БЧ. БЧ направляет в ЦИК, и ЦИК объявляет результаты выборов на сайте выборов.

Криптографические преобразования, используемые в системе ДЭГ, как основа выполнения требований безопасности в системе голосования

В рассматриваемой системе ДЭГ предлагается использовать гомоморфную криптографическую схему Эль-Гамаля [12] в поле GF(p) для генерации ключей, шифрования и дешифрования бюллетеней (аналогичным образом может быть рассмотрена схема Эль-Гамаля на эллиптической кривой). Обе схемы хорошо зарекомендовали себя при построении систем шифрования и электронной подписи [22–25].

Генерация ключей:

Шаг 1. Каждый сервер A_j генерирует случайное число $1 < sk_j < p - 1$, затем формируют открытый ключ: $pk_i = g^{sk_j} \, mod \; p$.

Сгенерированные открытые ключи pk_i передаются серверами ИК провинции к узлу провинции, закрытые ключи sk_j остаются на хранении на серверах до этапа расшифровки бюллетеней.

Шаг 2. Узел провинции формирует общий открытый ключ голосования:

$pk_{\text{общ.}} = \prod_i pk_i = g^{sk_1} * g^{sk_2} *\ldots..* g^{sk_j}(mod \; p) = g^{sk_1+sk_2+\ldots+sk_j} \, mod \; p.$

Общий открытый ключ узел провинции отправляет на серверы голосования, чтобы сервер голосования передал его избирателю. Для того чтобы уменьшить риск подделки или модификации переданного пользователю ключа, узел провинции подписывает общий открытый ключ своей цифровой подписью, а избиратели, имея сертификаты открытого ключа узла провинции, верифицируют подпись.

Шифрование:

Шаг 3. Избиратель V_i голосует, выбирая одно число из двух возможных: $b_i = (0,1)$, где b_i=1 – «за», b_i=0 – «против». И шифрует свой голос следующим образом:

$$(x_i, y_i) = \left(g^{\alpha_i}, pk_{\text{общ.}}{}^{\alpha_i} * G^{b_i}\right), \quad (1)$$

где α_i – случайное число, $1 \le \alpha_i \le p - 1$; G – фиксированный генератор G_q; (x_i, y_i) – первая и вторая части криптограммы (1) зашифрованного бюллетеня избирателя.

Шаг 4. Избиратель V_i формирует доказательство корректности заполнения бюллетеня B_i, используя, например, схему CGS [26]. Также мы разработали метод для проверки корректности заполнения бюллетеня в целом, который имеет низкую сложность на стороне БЧ [27].

Шаг 5. Зашифрованный бюллетень и доказательство корректности все избиратели направляют сначала на серверы голосования, затем серверы голосования направляют

их на узел провинции. После этого избиратель получает сообщение о том, что его голос принят и учтен.

Частичное расшифровывание:

Шаг 6. Каждый сервер проверяет доказательство и, в случае если доказательство успешно прошло проверку, переходит к выполнению частичной расшифровки, используя свой секретный ключ s_j.

Шаг 7. Сервер A_j выполняет частичную расшифровку бюллетеней каждого избирателя, вычисляя:

$$W_{1,j} = x_1^{s_j}, W_{2,j} = x_2^{s_j}, \ldots, W_{i,j} = x_i^{s_j},$$

где $W_{i,j}$ – частичная расшифровка бюллетеня; i – номер избирателя; j – номер сервера; sk_j – закрытый ключ сервера j. Затем каждый сервер вычисляет произведение частичных расшифровок: $X_j = \prod_i W_{i,j}$.

Заметим, что частичная расшифровка не дает серверу никакой информации о том, как проголосовал избиратель, чтобы никто не смог узнать результаты текущего голосования до завершения процедуры голосования.

Шаг 8. Произведение $X_j = \prod_i W_{i,j}$ каждый сервер отправляет на узел провинции.

Полное расшифрование и подсчет голосов избирателей:

Шаг 9. На узле провинции вычисляется произведение величин X_j от разных серверов $X = \prod_j X_j$, где j – номер сервера. Раскроем это произведение:

$$X = \left(W_{1,1} * W_{2,1} * \ldots * W_{n,1}\right) * \left(W_{1,2} * W_{2,2} * \ldots * W_{n,2}\right) * \ldots * \left(W_{1,k} * W_{2,k} * \ldots * W_{n,k}\right),$$

где k – количество серверов; n – количество избирателей.

Перегруппировав множители в данном выражении, получим:

$$X = \left(W_{1,1} * W_{1,2} * \ldots * W_{1,j}\right) * \left(W_{2,1} * W_{2,2} * \ldots * W_{2,j}\right) * \ldots * \left(W_{i,1} * W_{i,2} * \ldots * W_{i,j}\right) =$$
$$\left(g^{\alpha_1 s_1} * g^{\alpha_1 s_2} * \ldots * g^{\alpha_1 s_j}\right) * \left(g^{\alpha_2 s_1} * g^{\alpha_2 s_2} * \ldots * g^{\alpha_2 s_j}\right) * \ldots * \left(g^{\alpha_i s_1} * g^{\alpha_i s_2} * \ldots * g^{\alpha_i s_j}\right) mod\ p =$$
$$g^{\alpha_1(s_1+s_2+\ldots+s_j)} * g^{\alpha_2(s_1+s_2+\ldots+s_j)} * \ldots * g^{\alpha_i(s_1+s_2+\ldots+s_j)}\ mod\ p\ g^{(s_1+s_2+\ldots+s_j)} *$$
$$\left(g^{\alpha_1+\alpha_2+\ldots+\alpha_i}\right) mod\ p = g^{\sum s_j} * g^{\sum \alpha_i}\ mod\ p.$$

Шаг 10. Полное расшифровывание на узле провинции.

Сначала вычисляется $Y = \prod_i y_i$:

$$Y = y_1 * y_2 * \ldots * y_n = \left(pk_{\text{общ.}}{}^{\alpha_1} * G^{b_2}\right) * \left(pk_{\text{общ.}}{}^{\alpha_2} * G^{b_2}\right) * \ldots * \left(pk_{\text{общ.}}{}^{\alpha_n} * G^{b_n}\right) mod\ p =$$
$$pk_{\text{общ.}}{}^{\sum \alpha_i} * G^{\sum b_i}.$$

Далее, вычисляется:

$$\frac{Y}{X} = \frac{pk_{\text{общ.}}{}^{\sum \alpha_i * G^{\sum b_i}(mod\ p)}}{g^{\sum s_j * g^{\sum \alpha_i}(mod\ p)}} = \frac{g^{\sum s_j \sum \alpha_i * G^{\sum b_i}}}{g^{\sum s_j * g^{\sum \alpha_i}}} = G^{\sum b_i}\ mod\ p.$$

Шаг 11. Подсчет голосов (вычисление суммы голосов, поданных кандидатами):

$$\sum b_i = log_G\, G^{\sum b_i}\ mod\ p.$$

Логарифм вычисляется по заранее составленной таблице, в которой до начала выборов, в зависимости от числа участников и параметра G, посчитаны возможные результаты голосования (табл. 3).

Таблица 3

Общий вид таблицы возможных результатов голосования

$\sum b_i$	$G^{\Sigma b_i} mod\, p$
0	$G^0 mod\, p$
1	$G^1 mod\, p$
2	$G^2 mod\, p$
…..	
k	$G^k mod\, p$

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

Протокол отличается от других тем, что он обеспечивает комплексную защиту от атак на разных уровнях.

Анализ угроз в системе ДЭГ и способы их предотвращения

Для всех систем голосования существует достаточно много угроз, связанных с действиями нарушителя и неправомерными действиями участников протокола голосования [28]. В табл. 4 показано несколько наиболее опасных типов угроз, которые могут существовать в системе ДЭГ.

Таблица 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 за кандидатов до окончания голосования

Рассмотрим способы предотвращения этих угроз в предлагаемой системе ДЭГ.

Предотвращение нарушения тайны голосования обеспечивается за счет шифрования бюллетеня по схеме Эль-Гамаля, которая при выборе соответствующих параметров является вычислительно стойкой. В данной системе голосования применено разделение секретного ключа 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 k серверов является честным. Автор предполагает, что сговор k серверов маловероятен. Единый ключ расшифрования никогда не формируется и нигде не хранится. ИК участвует в расшифровании бюллетеня на втором

этапе без использования секретного ключа и не может повлиять на результат расшифрования. Также сервера предоставляют доказательства корректности частичного расшифрования. За счет разделения ключей расшифрования никто не может узнать результаты текущего голосования до закрытия процедуры голосования.

Анонимность голосования достигается за счет использования гомоморфного свойства криптосистемы Эль-Гамаля. В этом случае осуществляется расшифрование агрегированных голосов. После расшифрования известна сумма голосов, поданных за кандидата, по сумме голосов никто не может узнать, как проголосовал отдельный избиратель. Более того, предложенная схема имеет повышенную защищенность от атаки нарушения анонимности отдельных избирателей после окончания выборов. 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. ИК даже после окончания выборов не имеет секретного ключа, поэтому не может расшифровать бюллетень.

Предотвращение 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) ИК округа, провинции, ЦИК также невозможен, поскольку все голоса помещены в транзакцию БЧ, которая содержит доказательство корректности процедуры расшифрования.

Предотвращение 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 сервера голосования. Посторонние лица, в том числе ИК, не смогут сформировать подпись избирателя, поскольку никто не знает секретного ключа подписи избирателя и, следовательно, не сможет проголосовать за избирателя.

Предотвращение неправильного заполнения 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, в работах [11, 26, 29–31].

Предотвращение 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.

Предотвращение 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 ИК осуществляет полное расшифрование. Досрочное расшифрование невозможно, если хотя бы один из серверов выдержит регламент голосования и не начнет расшифрование раньше окончания выборов.

Приведем также доказательства выполнения основные требований к системе голосования в Ираке, определенных законом от 5 ноября 2020 г. № 9 «Выборы иракского парламента» [4].

Технически система отвечает следующим требованиям:

Свобода выбора избирателями своего кандидата. Данное требование выполняется при использовании ДЭГ, так как избиратель, имея доступ в интернет и компьютер (смартфон), может свободно выбирать своего кандидата, и никто не может сказать ему, за кого он должен голосовать или увидеть за кого он проголосовал.

Обеспечение прав избирателя и кандидата на участие в выборах. Любой желающий (легитимные кандидаты) может принять участие в выборах, выполнив требования, может подать заявку на участие в выборах и может проголосовать с помощью любого устройства (например, персонального компьютера, ноутбука, планшета и смартфона) в любое время и в любом месте без давления со стороны какой-либо партии или организации.

Требования к безопасности системы также выполнены: аутентификация избирателя осуществляется путем подтверждения учетной записи избирателя, и его имя включается в список избирателей; уникальность выполняетсятся за счет того, что избиратель не может зайти на сайт выбора более одного раза со своей учетной записью; подтверждение голоса выполнится за счет того, что после того, как избиратель отправляет свой зашифрованный бюллетень в систему, он получает сообщение о том, что его голос принят и учтён.

Разработка демонстрационного макета модели ДЭГ

С целью демонстрации работоспособности предложенной модели ДЭГ и элементов протокола, был разработан программный комплекс, состоящий из нескольких программ и интерфейсов для участников избирательного процесса.

Согласно предложенной модели, каждый сервер генерирует открытый и закрытый ключи. Закрытый ключ хранится на сервере. Из открытых ключей серверов формируется общий открытый ключ, который передается участникам голосования. Этим открытым ключом все участники голосования шифруют свои голоса и передают криптограммы на сервера. Сервера выполняют частичную расшифровку и отправляют частичные расшифровки своих голосов в избирательную комиссию. В ИК выполняется полная расшифровка. Результатом является число, равное сумме всех голосов.

Для упрощения демонстрации работы модели ДЭГ существует возможность симулировать наличие нескольких серверов голосования через единый интерфейс сервера. Интерфейс сервера голосования представлен на рис. 5.

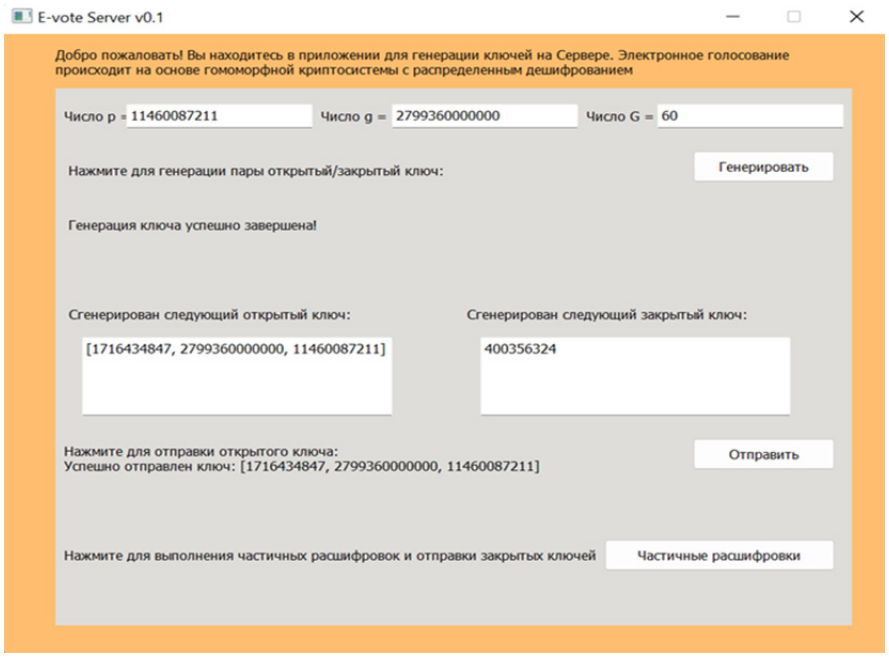

Рис. 5. **Интерфейс сервера голосования (генерация и отправка ключа)**

Для голосования избирателю необходимо нажать кнопку «За» или кнопку «Против», а затем отправить голос (рис. 6). При нажатии кнопки «Отправить», голос шифруется и записывается в файл.

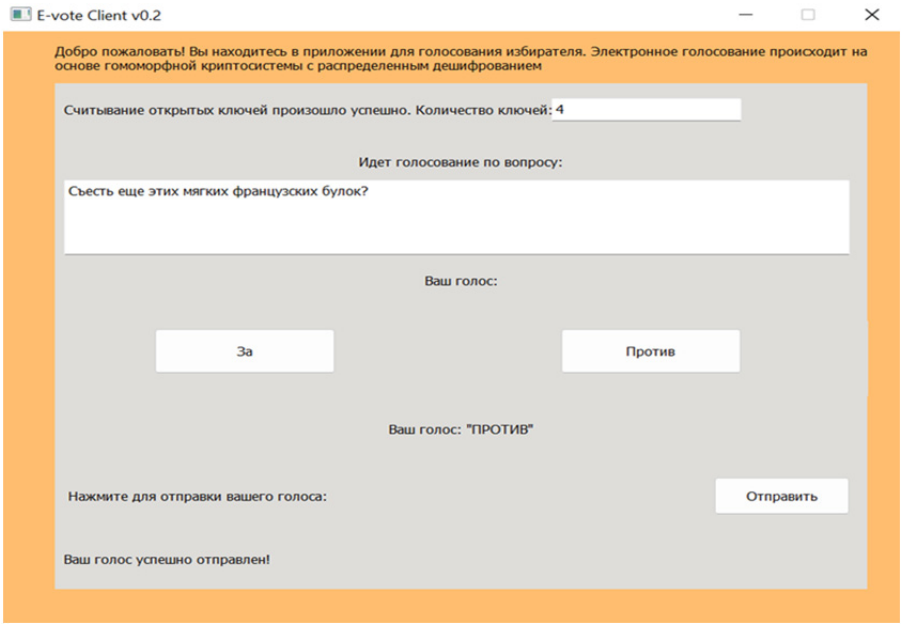

Рис. 6. **Интерфейс избирателя, отправка голоса**

После выполнения частичной расшифровки и отправки закрытых ключей можно воспользоваться интерфейсом ИК (рис. 7). Сверху отображается количество избирателей, принявших участие в ДЭГ, и количество пар ключей. Кнопка «Расшифровать» выводит полную информацию об итогах голосования, включая рассчитанные частичные расшифровки X и Y, и расшифрует результаты голосования по каждому кандидату.

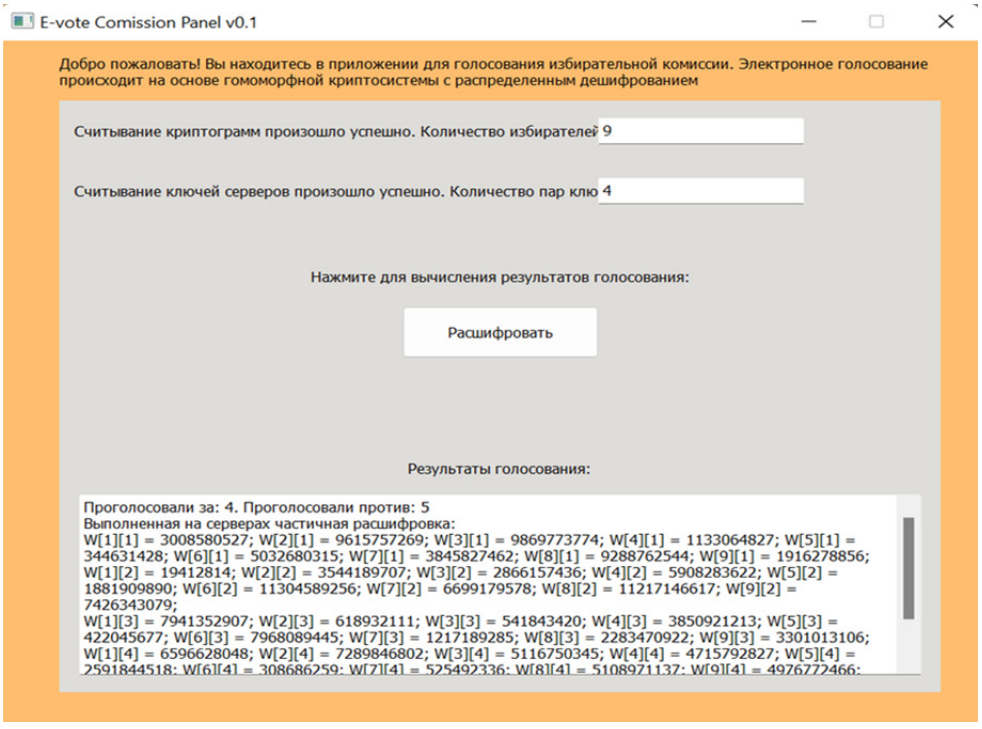

Рис. 7. **Интерфейс ИК**

Все приложения были разработаны на языке программирования Python 3.10 с использованием библиотеки PyQt5 для создания графического интерфейса приложений [21].

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 операционной системы: 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. А секретный ключ 72 байта. Зашифрованный голос занимает 8.192 байт дискового пространства. Заметим, что в данном макете БЧ не был использован.

Заключение

В работе проведен анализ существующей системы голосования в Республике Ирак. Анализ выявил в ней достаточно много недостатков, которые делают систему небезопасной. Чтобы устранить эти недостатки необходимо перейти на систему ДЭГ. Проанализированы принципы построения современных систем ДЭГ микс-сетей, слепой подписи и гомоморфного шифрования. Результаты анализа показывают, что гомоморфное шифрование обладает рядом преимуществ, поэтому эта схема взята за основу в предлагаемой модели системы ДЭГ для обеспечения безопасности избирательного процесса. В предлагаемой модели шифрование бюллетеней каждым избирателем сочетается с распределенным дешифрованием на нескольких серверах без восстановления единого ключа дешифрования, что существенно повышает безопасность данной системы голосования. Предлагаемая система ДЭГ Республики Ирак построена в виде комбинации подсистем ДЭГ провинций. Технологически такое объединение осуществляется на основе БЧ, узлы которого расположены в каждой провинции. Дано подробное описание криптографических преобразований, используемых в системе ДЭГ, которые обеспечивают требования безопасности в системе голосования. Проанализированы несколько наиболее описанных типов угроз, которые могут существовать в системе ДЭГ, и представлены доказательства их предотвращения в этой системе. Для тестирования качества работы предложенной модели ДЭГ разработан программный комплекс (макет), состоящий из нескольких программ и интерфейсов для участников избирательного процесса.

Список источников

1. Singh A., Ramakanth Kumar P., Cholli N.G. Empowering E-governance with E-voting // Indones. J. Electr. Eng. Comput. Sci. 2018. Vol. 12. № 3. P. 1081–1086.

2. Schneider A., Meter C., Hagemeister P. Survey on remote electronic voting // arXiv. 2017. P. 10.

3. Hussien H., Aboelnaga H. Design of a secured e-voting system // International Conference on Computer Applications Technology, ICCAT 2013. 2013. P. 5.

4. Official gazzete of iraq. Iraqi Council of Representatives elections law // Al-Waqai Al-iraqiyya. 2020. P. 37.

5. Chalabi M.H. E-voting framework for elections in iraq. 2014. P.135.

6. Official gazzete of iraq. Independent High Electoral Commission law // Al-Waqai Al-iraqiyya. baghdad. 2019. P. 6.

7. Chaum D.L. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms // Commun. ACM. 1981. Vol. 24. № 2. P. 84–90.

8. Mateu V., Miret J.M., Sebé F. A hybrid approach to vector-based homomorphic tallying remote voting // Int. J. Inf. Secur. Springer Berlin Heidelberg, 2016. P. 211–221.

9. Furukawa J., Mori K., Sako K. An implementation of a mix-net based network voting scheme and its use in a private organization // Lect. Notes Comput. Sci. (including Subser. Lect.

Notes Artif. Intell. Lect. Notes Bioinformatics). 2010. Vol. 6000 LNCS. P. 141–154.

10. Park C., Itoh K., Kurosawa K. Efficient anonymous channel and all/nothing election scheme // Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 1994. Vol. 765 LNCS. P. 248–259.

11. Peng K. An efficient shuffling based eVoting scheme // J. Syst. Softw. Elsevier Inc., 2011. Vol. 84. № 6. P. 906–922.

12. Elgamal T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Trans. Inf. Theory. 1985. Vol. 31. № 4. P. 469–472.

13. Fujioka A., Okamoto T., Ohta K. A practical secret voting scheme for large scale elections // Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 1993. Vol. 718 LNCS. P. 245–251.

14. Secure E-voting with blind signature / S. Ibrahim [et al.] // 4th Natl. Conf. Telecommun. Technol. NCTT 2003 – Proc. 2003. P. 193–197.

15. Rivest R.L., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public- Key Cryptosystems // Commun. ACM. 1978. Vol. 21. № 2. P. 120–126.

16. Криптографические методы обеспечения конфиденциальности электронных выборов / Е.Н. Сергиенко [и др.] // Проблемы информатики в образовании, управлении, экономике и технике: сб. статей XVII Междунар. науч.-техн. конф. Пенза: ПДЗ. 2017. P. 51–56.

17. Provotum: A Blockchain-based and End-to-end Verifiable Remote Electronic Voting System / C. Killer [et al.] // Proc. – Conf. Local Comput. Networks, LCN. 2020. Vol. 2020-Novem. P. 172–183.

18. Practical Multi-Candidate Election System / O. Baudron [et al.] // Proc. Twent. Annu. ACM Symp. Princ. Distrib. Comput. 2001.

19. Zissis D. Technologies and Methodologies for Designing Secure Electronic Voting Information Systems. 2011. P. 257.

20. Салман В.Д. Анализ гомоморфных криптосистем Бенало и Пэйе для построения системы электронного голосования // Труды учебных заведений связи. 2021. Vol. 7. № 2. P. 8.

21. Яковлев В.А., Салман В.Д., Шевцов Д.С. Исследование системы электронного голосования на основе гомоморфного шифрования с распределенным дешифрованием // Защищенные системы связи. 2022. Vol. 2. P. 10.

22. Kefa Rabah. Elliptic Curve ElGamal Encryption and Signature Schemes // Inf. Technol. J. 2005. Vol. 4. № 3. P. 299–306.

23. Caelli W.J., Dawson E.P., Rea S.A. PKI, elliptic curve cryptography, and digital signatures // Comput. Secur. 1999. Vol. 18. № 1. P. 47–66.

24. Ordonez A.J., Gerardo B.D., Medina R.P. Digital signature with multiple signatories based on modified ElGamal Cryptosystem // Proc. 2018 5th Int. Conf. Bus. Ind. Res. Smart Technol. Next Gener. Information, Eng. Bus. Soc. Sci. ICBIR 2018. IEEE, 2018. P. 89–94.

25. Czeslaw K. A new approach to the elgamal encryption scheme // Int. J. Appl. Math. Comput. Sci. 2004. Vol. 14. № 2. P. 265–267.

26. Cramer R., Gennaro R., Schoenmakers B. A secure and optimally efficient multi-authority election scheme // Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 1997. Vol. 1233. P. 103–118.

27. Салман В.Д., Яковлев В.А. Методы защиты от угрозы неправильного заполнения избирательного бюллетеня в системе дистанционного электронного голосования // АПИНО. 2023. Vol. 1. P. 5.

28. An Experience in Testing the Security of Real-World Electronic Voting Systems / D. Balzarotti [et al.]. 2010. Vol. 36. № 4. P. 453–473.

29. Multi-authority secret-ballot elections with linear work / R. Cramer [et al.] // Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 1996. Vol. 1070. P. 72–83.

30. Peng K., Dawson E., Bao F. Modification and optimisation of a shuffling scheme: Stronger security, formal analysis and higher efficiency // Int. J. Inf. Secur. 2011. Vol. 10. № 1. P. 33–47.

31. Яковлев В.А., Салман В.Д. Методы защиты от угрозы неправильного заполнения избирательного бюллетеня в системе дистанционного электронного голосования // Труды учебных заведений связи. 2023. Vol. 9. № 1. P. 21–36.

References

1. Singh A., Ramakanth Kumar P., Cholli N.G. Empowering E-governance with E-voting // Indones. J. Electr. Eng. Comput. Sci. 2018. Vol. 12. № 3. P. 1081–1086.

2. Schneider A., Meter C., Hagemeister P. Survey on remote electronic voting // arXiv. 2017. P. 10.

3. Hussien H., Aboelnaga H. Design of a secured e-voting system // International Conference on Computer Applications Technology, ICCAT 2013. 2013. P. 5.

4. Official gazzete of iraq. Iraqi Council of Representatives elections law // Al-Waqai Al-iraqiyya. 2020. P. 37.

5. Chalabi M.H. E-voting framework for elections in iraq. 2014. P.135.

6. Official gazzete of iraq. Independent High Electoral Commission law // Al-Waqai Al-iraqiyya. baghdad, 2019. P. 6.

7. Chaum D.L. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms // Commun. ACM. 1981. Vol. 24. № 2. P. 84–90.

8. Mateu V., Miret J.M., Sebé F. A hybrid approach to vector-based homomorphic tallying remote voting // Int. J. Inf. Secur. Springer Berlin Heidelberg, 2016. P. 211–221.

9. Furukawa J., Mori K., Sako K. An implementation of a mix-net based network voting scheme and its use in a private organization // Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 2010. Vol. 6000 LNCS. P. 141–154.

10. Park C., Itoh K., Kurosawa K. Efficient anonymous channel and all/nothing election scheme // Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 1994. Vol. 765 LNCS. P. 248–259.

11. Peng K. An efficient shuffling based eVoting scheme // J. Syst. Softw. Elsevier Inc., 2011. Vol. 84. № 6. P. 906–922.

12. Elgamal T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Trans. Inf. Theory. 1985. Vol. 31. № 4. P. 469–472.

13. Fujioka A., Okamoto T., Ohta K. A practical secret voting scheme for large scale elections // Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 1993. Vol. 718 LNCS. P. 245–251.

14. Secure E-voting with blind signature / S. Ibrahim [et al.] // 4th Natl. Conf. Telecommun. Technol. NCTT 2003 – Proc. 2003. P. 193–197.

15. Rivest R.L., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public- Key Cryptosystems // Commun. ACM. 1978. Vol. 21. № 2. P. 120–126.

16. Kriptograficheskie metody obespecheniya konfidencial'nosti elektronnyh vyborov / E.N. Sergienko [i dr.] // Problemy informatiki v obrazovanii, upravlenii, ekonomike i tekhnike: sb. statej XVII Mezhdunar. nauch.-tekhn. konf. Penza: PDZ. 2017. P. 51–56.

17. Provotum: A Blockchain-based and End-to-end Verifiable Remote Electronic Voting System / C. Killer [et al.] // Proc. – Conf. Local Comput. Networks, LCN. 2020. Vol. 2020-Novem. P. 172–183.

18. Practical Multi-Candidate Election System / O. Baudron [et al.] // Proc. Twent. Annu. ACM Symp. Princ. Distrib. Comput. 2001.

19. Zissis D. Technologies and Methodologies for Designing Secure Electronic Voting Information Systems. 2011. P. 257.

20. Salman V.D. Analiz gomomorfnyh kriptosistem Benalo i Peje dlya postroeniya sistemy elektronnogo golosovaniya // Trudy uchebnyh zavedenij svyazi. 2021. Vol. 7. № 2. P. 8.

21. Yakovlev V.A., Salman V.D., Shevcov D.S. Issledovanie sistemy elektronnogo golosovaniya na osnove gomomorfnogo shifrovaniya s raspredelennym deshifrovaniem // Zashchishchennye sistemy svyazi. 2022. Vol. 2. P. 10.

22. Kefa Rabah. Elliptic Curve ElGamal Encryption and Signature Schemes // Inf. Technol. J. 2005. Vol. 4. № 3. P. 299–306.

23. Caelli W.J., Dawson E.P., Rea S.A. PKI, elliptic curve cryptography, and digital signatures // Comput. Secur. 1999. Vol. 18. № 1. P. 47–66.

24. Ordonez A.J., Gerardo B.D., Medina R.P. Digital signature with multiple signatories based on modified ElGamal Cryptosystem // Proc. 2018 5th Int. Conf. Bus. Ind. Res. Smart Technol. Next Gener. Information, Eng. Bus. Soc. Sci. ICBIR 2018. IEEE, 2018. P. 89–94.

25. Czeslaw K. A new approach to the elgamal encryption scheme // Int. J. Appl. Math. Comput. Sci. 2004. Vol. 14. № 2. P. 265–267.

26. Cramer R., Gennaro R., Schoenmakers B. A secure and optimally efficient multi-authority election scheme // Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 1997. Vol. 1233. P. 103–118.

27. Salman V.D., Yakovlev V.A. Metody zashchity ot ugrozy nepravil'nogo zapolneniya izbiratel'nogo byulletenya v sisteme distancionnogo elektronnogo golosovaniya // APINO. 2023. Vol. 1. P. 5.

28. An Experience in Testing the Security of Real-World Electronic Voting Systems / D. Balzarotti [et al.]. 2010. Vol. 36. № 4. P. 453–473.

29. Multi-authority secret-ballot elections with linear work / R. Cramer [et al.] // Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 1996. Vol. 1070. P. 72–83.

30. Peng K., Dawson E., Bao F. Modification and optimisation of a shuffling scheme: Stronger security, formal analysis and higher efficiency // Int. J. Inf. Secur. 2011. Vol. 10. № 1. P. 33–47.

31. Yakovlev V.A., Salman V.D. Metody zashchity ot ugrozy nepravil'nogo zapolneniya izbiratel'nogo byulletenya v sisteme distancionnogo elektronnogo golosovaniya // Trudy uchebnyh zavedenij svyazi. 2023. Vol. 9. № 1. P. 21–36.

Информация о статье:
Статья поступила в редакцию: 18.05.2023; одобрена после рецензирования: 28.05.2023; принята к публикации: 29.05.2023
Information about the article:
The article was submitted to the editorial office: 18.05.2023; approved after review: 28.05.2023; accepted for publication: 29.05.2023

Сведения об авторах:
Салман Васан Давуд, аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича (193232, Санкт-Петербург, пр. Большевиков, д. 22/1), e-mail:salman.vd@sut.ru

Information about authors:
Salman Vasan Davud, graduate student Saint-Petersburg state university of telecommunications them. prof. M.A. Bonch-Bruevich (193232, Saint-Petersburg, pr. Bolshevikov, 22/1), e-mail: salman.vd@sut.ru