Научная статья
УДК 004.056(075.8)
DOI:10.31854/1813-324X-2023-9-4-114-121

Способ защиты от атаки некорректного заполнения избирательного бюллетеня в системе дистанционного электронного голосования

Виктор Алексеевич Яковлев, yakovlev.va@sut.ru
Васан Давуд Салман, salman.vd@sut.ru

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

Аннотация: *Анализируется система дистанционного электронного голосования, основанная на гомоморфном шифровании бюллетеня и применении блокчейн-технологий. Исследуются существующие способы защиты системы голосования от атаки, связанной с неправильным заполнением избирателем бюллетеня. Разработан способ защиты от атаки нарушения правила заполнения бюллетеня в целом, повышающий безопасность системы голосования, за счет обеспечения скрытности суммарного числа голосов, переданных избирателем в ходе проверки корректности заполнения бюллетеня.*

Ключевые слова: *система дистанционного электронного голосования, проверка доказательства корректности заполнения бюллетеня, доказательство с нулевым разглашением секрета, схема Эль-Гамаля*

Ссылка для цитирования: Яковлев В.А., Салман В.Д. Способ защиты от атаки некорректного заполнения избирательного бюллетеня в системе дистанционного электронного голосования // Труды учебных заведений связи. 2023. Т. 9. № 4. С. 114–121. DOI:10.31854/1813-324X-2023-9-4-114-121

Defense Method against an Attack of Incorrect Ballot Filling in a Remote Electronic Voting System

Victor Yakovlev, yakovlev.va@sut.ru
Vasan Salman, salman.vd@sut.ru

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Abstract: *The remote electronic voting system based on homomorphic encryption and blockchain technologies is analyzed. The existing methods of protecting the voting system from an attack related to incorrect filling a ballot by the voter are studied. The method to protect against an attack of violation of the rules for filling a ballot as a whole is developed, which increases the security of voting system by ensuring secrecy of total number of votes given by voter during the verification correctness of filling a ballot.*

Keywords: *remote electronic voting system, verification proof the correctness of filling the ballot, zero-knowledge proof system, El-Gamal scheme*

For citation: Yakovlev V., Salman V. Defense Method against an Attack of Incorrect Ballot Filling in a Remote Electronic Voting System. *Proceedings of Telecommun. Univ.* 2023;9(4):114–121. DOI:10.31854/1813-324X-2023-9-4-114-121

Введение

Система дистанционного электронного голосования (ДЭГ) предоставляет возможность избирателям отдавать свои голоса удаленно с любого компьютера или цифрового устройства, подключенного к общедоступной сети Интернет из дома или с работы [1]. Для этого от избирателя требуются элементарные навыки работы на персональном компьютере, смартфоне, планшете или другом устройстве. ДЭГ – подход к системе онлайн-голосования, основанный на криптографических методах [2]. Основными преимуществами применения системы ДЭГ являются: повышение точности и скорости подсчета голосов; обеспечение тайны голосования и анонимности избирателей. Для построения защищенной системы ДЭГ используются такие методы как: микс-сети (МС); слепая подпись (СП) и гомоморфное шифрование (ГШ) [1–3].

Примером системы ДЭГ, основанной на МС, является Гелиос (США) [1]. Избиратель выбирает кандидата, используя два значения: 1 – «ЗА» или 0 – «ПРОТИВ». После чего шифрует выбор с помощью открытого ключа и отправляет его на сервер. После получения бюллетеней от избирателей сервер маскирует их, перемешивает и отправляет следующему серверу. Данная процедура проводится несколько раз. Последняя МС передает бюллетени в избирательную комиссию, где она их расшифровывает. Из-за того, что бюллетени были неоднократно перемешаны, обеспечивается анонимность голосующего. Тайна голосования обеспечивается шифрованием бюллетеня. МС должны доказывать правильность перемешивания бюллетеней.

В системе ДЭГ, основанной на применении СП [2], для обеспечения анонимности голосующего выполняется следующий протокол: избиратель выбирает кандидата, заполняет избирательный бюллетень (ИзБ), шифрует его секретным ключом и маскирует. После этого он подписывает свой ИзБ и отправляет его в избирательную комиссию (ИК), которая проводит проверку принадлежности подписи зарегистрированному избирателю, который еще не отдал свой голос. ИК подписывает этот документ своей подписью и возвращает его избирателю. Затем он удаляет маскировку, получая таким образом подписанный избирательной комиссией зашифрованный бюллетень. Далее, он отправляет этот ИзБ в комиссию по анонимному каналу. ИК проверяет на этом документе свою подпись. В случае, если ИзБ действителен, ИК размещает его в списке, который будет издан после того, как завершится голосование. Затем избиратель посылает свой ключ расшифровки в ИК, которая им расшифровывает ИзБ и добавляет голос к общему количеству голосов, отданных за кандидата.

В системе голосования на основе ГШ [3] избиратели зашифровывают свои ИзБ открытым ключом ИК. Далее они отправляют свои зашифрованные ИзБ на сервер, который перемножает их, как числа, и посылает получившийся результат в ИК, которая расшифровывает произведение бюллетеней и объявляет победителя выборов. В силу гомоморфного свойства результат расшифровки произведения криптограмм равен сумме голосов, отданных за кандидата. Анонимность голосования каждого избирателя обеспечивается тем, что происходит расшифровка сразу всех агрегированных ИзБ. Основными преимуществами ГШ являются простота внедрения и эффективный подсчет голосов, так как нет необходимости расшифровывать бюллетени отдельно. Безопасность этих систем голосования обеспечивается вычислительной стойкостью применяемых криптосхем [3].

Современные системы ДЭГ активно используют технологию блокчейн [4–6] как средство надежной передачи и хранения транзакций. Примерами таких систем голосования являются системы: ДЭГ России [7]; «Криптовече» разработки Санкт-Петербургского Государственного университета [8]; Provotum (Швейцария) [3] и другие [9–11].

В настоящее время большое внимание уделяется вопросу автоматической проверки правильности заполнения избирательного бюллетеня. Специфика такой проверки в том, что она должна выполняться без раскрытия для проверяющего информации о том, как проголосовал тот или иной избиратель.

Возможны два вида атак на систему ДЭГ со стороны избирателя, которые могут проводиться умышленно и неумышленно. Первый вид атаки заключается в том, что избиратель указывает некорректное число, соответствующее его выбору «ЗА» или «ПРОТИВ» по конкретному кандидату. Наиболее часто для защиты от этой атаки используется схема доказательства с нулевым разглашением секрета, предложенная в [12] Крамером, Дамгардом, Шоенмакером (*аббр.* CDS). Такая схема применяется в российской системе ДЭГ [7]. Второй вид атаки заключается в нарушении избирателем установленного избирательной комиссией правила голосования по количеству поданных голосов «ЗА» в одном бюллетене. То есть помимо проверки корректности заполнения бюллетеня по каждому кандидату необходима проверка корректности заполнения бюллетеня в целом. Другими словами, число голосов m, поданных «ЗА», должно быть в интервале: $m_{\min} \le m \le m_{\max}$, где $m_{\min}$, $m_{\max}$ – минимальное и максимальное число кандидатов, за которых может проголосовать избиратель согласно правилу голосования, установленному ИК.

Заметим, что в литературе содержится недостаточно сведений о способах проверки корректности заполнения ИзБ в целом. Известный способ [13] решает такую задачу, однако посторонние лица могут получить информацию об общем числе

голосов, отданных избирателем (без конкретизации его выбора по кандидатам). Это, на взгляд авторов, является уязвимостью способа, поскольку позволяет на основе анализа сумм голосов, содержащихся в ИзБ, отслеживать интенсивность хода голосования.

Способ, разработанный авторами, расширяет класс способов проверки корректности заполнения ИзБ, так как, помимо проверки корректности, обеспечивает скрытность суммарного количества голосов, поданных избирателем.

Целью статьи является разработка способа контроля корректности заполнения ИзБ по всем кандидатам (проверка в целом) для системы ДЭГ, построенной на основе криптосистемы Эль-Гамаля (ЭГ) [14].

В п. 1 приведен анализ системы ДЭГ на основе криптосистемы ЭГ, описаны существующие способы защиты от некорректного заполнения избирательного бюллетеня по каждому кандидату и для всех кандидатов, приведены оценки сложности выполнения соответствующих операций для этих способов. В п. 2 представлено описание предлагаемого способа защиты от некорректного заполнения ИзБ в целом, а также даны оценки его сложности.

1. Система ДЭГ, основанная на криптосистеме гомоморфного шифрования

Данная система включает в себя: избирателей, сервер, технологию блокчейн (БЧ) и ИК (рисунок 1).

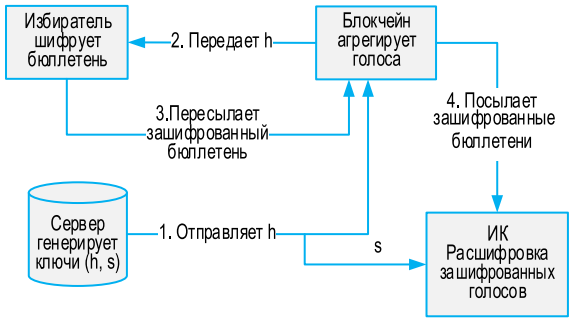

Рис. 1. Система ДЭГ

Fig. 1. Remote Electronic Voting System

Все участники избирательного процесса (избиратель, БЧ, ИК) выполняют необходимые математические преобразования с использованием программно-аппаратных средств и соответствующего программного обеспечения. Для краткости изложения будем полагать, что все участники непосредственно осуществляют необходимые вычисления без упоминания использования соответствующих программно-аппаратных средств.

Функционирование системы ДЭГ включает:

– *инициализация системы* – заключается в выборе системных параметров и генерации ключей. Сервер генерирует ключи шифрования и дешифрования, используя схему ГШ; после этого отправляет ключ шифрования в БЧ, который передает его всем избирателям; ключ дешифрования хранится на сервере или может быть разделен на доли и находится у хранителей ключа до завершения выборов [3];

– *аутентификация избирателей* – в случае успешной проверки данных избиратель получает разрешение на участие в голосовании (в данной работе этап идентификации и аутентификации избирателя не рассматривается);

– голосование – каждый избиратель выбирает кандидата (кандидатов) из списка и шифрует свой выбор, используя ключ шифрования; далее он посылает зашифрованный бюллетень в БЧ; в БЧ происходит агрегирование голосов, результат передается в ИК [3];

– *подсчет голосов и объявление результатов* – ИК расшифровывает результаты голосования с помощью ключа дешифрования и объявляет его итог [3].

Рассмотрим детально основные этапы применительно к гомоморфной системе ЭГ.

Этап 1. Генерация ключей шифрования и дешифрования на сервере

Закрытый ключ s выбирается случайным образом в диапазоне $1 \le s \le p-1$, а открытый ключ h генерируется следующим образом:

$$h = g^s \bmod p, \qquad (1)$$

где g – примитивный элемент над полем Галуа $GF(p)$; p – простое число.

Этап 2. Шифрование избирательного бюллетеня

Зашифрованный бюллетень по схеме ЭГ можно записать как:

$$C_i = (A_i, B_i) = (g^{ri}, h^{ri} \cdot G^{v_i}) \bmod p, \qquad (2)$$

где $v_i \in \{0,1\}$ – голос избирателя; r_i – случайное число, $1 \le r_i \le p-1, i = 1,2 \ldots k$; k – число кандидатов; G – примитивный элемент над полем Галуа $GF(p)$.

Далее, все избиратели отправляют свои зашифрованные бюллетени и доказательства корректности ИзБ в БЧ.

Этап 3. Агрегирование криптограмм

После завершения голосования в БЧ осуществляется агрегирование криптограмм всех избирателей, отданных за каждого кандидата:

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

Далее криптограмма T_j отправляется в ИК.

Этап 4. Расшифровка избирательного бюллетеня

ИК, используя ключ s, осуществляет дешифрование агрегированных бюллетеней:

$$\frac{h^{(\sum r_i)} \cdot G^{\sum v_i}}{g^{\sum r_i \cdot s}} = \frac{g^{(\sum r_i)^s} \cdot G^{\sum v_i}}{g^{(\sum r_i)^s}} = G^{\sum v_i} \bmod p. \quad (3)$$

Этап 5. Подсчет голосов

Для гомоморфной схемы ЭГ сумма всех голосов, отданных за *j*-го кандидата, вычисляется как:

$$\sum_{i=1}^{n} v_{ij} = \log_G G^{\sum v_{ij}} \bmod p.$$

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

В описанной выше системе ДЭГ существует угроза атаки со стороны избирателя, поскольку им может быть некорректно заполнен (умышленно или неумышленно) ИзБ, что, в свою очередь, может повлиять на результаты голосования. Для предотвращения этой угрозы применяются разные способы проверки корректности заполнения ИзБ.

Способы проверки корректности ИзБ, как уже было сказано, различаются на способы проверки корректности голосования по каждому кандидату и заполнения ИзБ в целом [12, 15]. Сравнительный анализ способов [16] показал, что они отличаются большой сложностью, зачастую превышающей сложность процедур шифрования и дешифрования. Рассмотрим данные способы подробнее.

Предположим, что ключи шифрования и дешифрования сгенерированы. Избиратель выполняет следующие операции [16]:

– выбирает своего кандидата;

– шифрует ИзБ, используя ключ шифрования h;

– формирует доказательство корректности ИзБ за каждого кандидата [13], как показано в таблице 1.

ТАБЛИЦА 1. Процедура формирования доказательства корректности заполнения избирательного бюллетеня

TABLE 1. The Procedure for Forming a Proof of Correctness a Voter's Ballot

В случае $v_i = 1$	В случае $v_i = 0$
Выбирает числа случайным образом:	
$r_i, w, u_1, d_1 \in \mathbb{Z}_q$	$r_i, w, u_2, d_2 \in \mathbb{Z}_q$
Шифрует ИзБ:	
$A_i = (g^{r_i}) \bmod p$ $B_i = h^{r_i} G^{v_i} \bmod p$	$A_i = (g^{r_i}) \bmod p$ $B_i = h^{r_i} / G^{v_i} \bmod p$
Формирует доказательства:	
$a_1 = g^{u_1} A_i^{d_1} \bmod p$ $b_1 = h^{u_1}(B_i G^{v_i})^{d_1} \bmod p$ $a_2 = g^{w} \bmod p$ $b_2 = h^{w} \bmod p$	$a_1 = g^{w} \bmod p$ $b_1 = h^{w} \bmod p$ $a_2 = g^{u_2} A_i^{d_2} \bmod p$ $b_2 = h^{u_2}(B_i / G^{v_i})^{d_2} \bmod p$
Находит хэш-функцию $c = H(A, B, a_1, b_1, a_2, b_2) \bmod q$, где q – простое число	
$d_2 = c - d_1 \bmod q$ $u_2 = w - r_i d_2 \bmod q$	$d_1 = c - d_2 \bmod q$ $u_1 = w - r_i d_1 \bmod q$

Далее избиратель отправляет значения (A_i, B_i, a_1, b_1, a_2, b_2, d_1, d_2, u_1, u_2) контролирующему органу (БЧ), который проверяет корректно ли избиратель заполнил ИзБ.

БЧ проверяет следующие сравнения:

$$c = d_1 + d_2 \bmod q, \quad (4)$$

$$a_1 = g^{u_1} A_i^{d_1} \bmod p, \quad (5)$$

$$b_1 = h^{u_1}(B_i g^{vi})^{d_1} \bmod p, \quad (6)$$

$$a_2 = g^{u_2} A_i^{d_2} \bmod p, \quad (7)$$

$$b_2 = h^{u_2}(B_i / g^{vi})^{d_2} \bmod p. \quad (8)$$

Таким образом контролирующий орган (БЧ) может провести проверку корректности голосования избирателем по каждому кандидату («0» или «1»), при этом он не знает, как проголосовал избиратель. Данная проверка основана на методе доказательства с нулевым разглашением секрета [17].

Здесь необходимо отметить, что БЧ, проводя проверку корректности заполнения бюллетеня по каждому кандидату, не проверяет корректность выполнения избирателем правил голосования по заданному варианту голосования. Например, избиратель выбрал трех кандидатов из k, хотя разрешено выбрать только одного или двух. Такого рода задача решается проверкой корректности заполнения ИзБ в целом.

Рассмотрим способ [12, 15] формирования доказательства корректности заполнения ИзБ для всех кандидатов.

1) Избиратель находит произведение всех криптограмм, содержащихся в бюллетене:

$$C = \left(\prod C_i\right) = \left(\prod A_i, \prod B_i\right) = \left(g^{\sum ri}, h^{\sum ri} \cdot G^{\sum v_i}\right),$$

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

2) Выбирает случайное число $t \in Z_p$ и вычисляет:

$$X = h^t. \quad (9)$$

3) Находит хэш-функцию:

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

4) Находит:

$$z = t + r \cdot c, \quad (10)$$

где $r = \sum r_i$; r_i – числа, ранее использованные при формировании криптограмм.

5) Посылает (X, z, m') в БЧ.

При такой атаке, избиратель указывает общее количество голосов «ЗА», отданных за всех кандидатов (m'); которое может отличаться от фактической суммы отданных голосов m, $m \neq m'$.

БЧ выполняет проверку следующим образом:

– находит хэш-функцию:

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

– проверяет сравнение:

$$h^z =^? X \cdot \left(\frac{\prod_i B_i}{g^{m'}}\right)^c. \quad (11)$$

Рассмотрим правую часть сравнения:

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

Если $m = m'$, то $h^{t+r \cdot c} = h^z$. Значит сравнение (11) выполняется.

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

На основе анализа операций в таблице 1 и соотношений (4–10) несложно получить количество операций:

– по формированию доказательства корректности заполнения ИзБ на стороне избирателя – $10k + 1$;

– проверки доказательства корректности заполнения ИзБ на стороне БЧ – $8k + 3$.

Отметим, что в способе проверки корректности заполнения ИзБ по всем кандидатам (в целом), избиратель указывает общее количество голосов «ЗА» (m'), что, на взгляд авторов, является слабостью этого способа, так как позволяет посторонним лицам проводить оценку интенсивности хода голосования. В этой связи рассмотрим следующий способ предотвращения некорректного заполнения бюллетеня.

2. Разработка способа предотвращения некорректного заполнения бюллетеня

Предположим, что ключи шифрования и дешифрования ИзБ сгенерированы. Избиратель сделал свой выбор, криптограммы (A_i, B_i) ИзБ сформированы и переданы в БЧ. Доказательство корректности ИзБ за каждого кандидата осуществляется так же, как в рассмотренном способе (см. п. 1). Тогда представляем способ проверки корректности заполнения ИзБ в целом, без раскрытия общего количества поданных голосов. Операции, выполняемые избирателем и БЧ, приведены в таблице 2.

Дадим пояснение к проверке (18):

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

Если избиратель проголосовал правильно ($m = m'$), то:

$$\sum_{i=1}^k v_i - \left(\sum_{i=1}^{k+1} v_i\right) + v_{k+1} = m - (m' + v_{k+1}) + v_{k+1} = 0,$$

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

ТАБЛИЦА 2. Способ формирования и проверки доказательства корректности заполнения ИзБ в целом

TABLE 2. The Method for Forming and Verifying a Proof of Correctness Filling the Voter's Ballot as a Whole

Избиратель	БЧ
Формирование доказательства	
–	1) Генерирует: $A_{k+1} = g^{r_{k+1}}, r_{k+1} \in Z_p$ и $f \in Z_p$
← Посылает $(g^{r_{k+1}}, f)$	
2) Находит числа y_i, $i = 1, \ldots, k$: $y_i = \frac{\prod_{j<i} A_j}{\prod_{j>i} A_j}$ (12)	–
3) Вычисляет: $U_{D_i} = y_i^{r_i} g^{v_i}$ (13)	–
4) Находит произведение: $U'_\Sigma = \prod_{i=1}^k U_{Di} = \prod_{i=1}^k y_i^{r_i} g^{v_i}$ (14)	–
5) Вычисляет, где e ∈ Z_p: $X' = h^e$, $x = e + \sum_{i=1}^k r_i \cdot f$ (15)	–
Посылает в БЧ U'_Σ, X' и x →	
Проверка доказательства	
	Первая проверка
–	6) Вычисляет: $y_{k+1}^{r+1} = A_1 A_2 \ldots A_k$ 7) Находит: $U_{Dk+1} = y_{k+1}^{r_{k+1}} \cdot g^{v_{k+1}}$ (16)
–	8) Вычисляет: $U_\Sigma = U'_\Sigma U_{Dk+1} = g^{\sum_{i=1}^k v_i + v_{k+1}}$ (17)
–	9) Методом подбора находит такое $-v_{k+1}$, при котором: $U_\Sigma = 1$
	10) Проверяет неравенство: $m_{\min} \le v_{k+1} \le m_{\max}$. Выполнение неравенства свидетельствует о том, что число поданных голосов лежит в заданном интервале
	Вторая проверка
–	11) Проверяет сравнение: $h^x =^? X \cdot V$, (18) 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

В этом способе число m' в явном виде не передается, а число v_{k+1} в (17) известно только БЧ, поэтому посторонний пользователь, в том числе ИК, не может узнать общее количество голосов «ЗА», содержащихся в бюллетене, что, в свою очередь, повышает безопасность голосования в целом. Сложность такого метода можно оценить на основе вышеприведенных соотношений, как показано в таблицах 3 и 4. При оценке сложности учитывались только операции возведения числа в степень по модулю.

ТАБЛИЦА 3. Оценка сложности формирования доказательства корректности заполнения бюллетеня предлагаемым способом на стороне избирателя

TABLE 3. The Evaluation of Complexity for Forming a Proof of Correctness Filling a Ballot in the Proposed Method on a Voter's Side

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

ТАБЛИЦА 4. Оценка сложности проверки доказательства корректности голосования на стороне БЧ

TABLE 4. The Evaluation of Complexity for Verifying of Correctness Voting on Blockchain's Side

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

В таблице 5 представлены результаты сравнения сложности вычислений известного (X) [12, 15] и предложенного (Y) способов для избирателя (доказывающей стороны) и БЧ (проверяющей стороны). Оценка сложности вычислений проведена по наиболее трудоемкой операции – возведению числа в степень по mod p. Для n избирателей принимающих участие в выборах эти значения очевидно нужно умножить на n.

В таблице 6 приведены оценки сложности вычислений в БЧ для существующего и предлагаемого способов для разного количества кандидатов и избирателей.

ТАБЛИЦА 5. Сравнение сложности вычислений для двух способов доказательства корректности заполнения бюллетеня

TABLE 5. The Comparison of Computational Complexity for Two Methods to Proving Correctness Filling a Ballot

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

ТАБЛИЦА 6. Оценки сложности способов контроля корректности заполнения бюллетеня в зависимости от количества кандидатов и избирателей

TABLE 6. The Evaluation of Complexity for Methods to Verify Correctness Filling a Ballot Depending on the Number of Voters

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

Как видно из таблиц 5 и 6, предлагаемый способ на стороне избирателя приблизительно на 20 % сложнее известного, а на стороне БЧ они приблизительно имеют одинаковую сложность. Однако предлагаемый способ является более безопасным, так как в ходе проверки правильности заполнения ИзБ в целом не раскрывается для посторонних лиц общая сумма голосов, отданных за кандидатов.

Заключение

Рассмотрена система ДЭГ, построенная на основе криптосистемы ЭГ. Для доказательства корректности заполнения бюллетеня в этой системе использовались два варианта: один – для каждого кандидата, а второй – для всех кандидатов вместе.

Разработан способ контроля некорректного заполнения бюллетеня в целом, позволяющий контролирующему органу (БЧ) убедиться в том, что избиратель корректно выбрал количество кандидатов из диапазона возможных значений.

Данный способ при примерно одинаковой сложности вычислений в сравнении с известным повышает безопасность системы ДЭГ, поскольку в ходе проверки не раскрывается суммарное число голосов, отданных за нескольких кандидатов, тем самым обнаруживается и блокируется атака на систему, позволяющая нарушителю во время контроля проводить анализ и оценку статистики хода голосования до окончания выборов.

Список источников

1. Adida B. Helios: Web-based open-audit voting // Proceedings of the 17th USENIX Security Symposium (San Jose, USA, 28–29 July 2008). 2008. PP. 335–348.

2. Fujioka A., Okamoto T., Ohta K. A practical secret voting scheme for large scale elections // Proceedings of the Advances in Cryptology – AUSCRYPT '92 (Gold Coast, Queensland, Australia, 13–16 December 1992). Lecture Notes in Computer Science. Vol. 718. Berlin, Heidelberg: Springer, 1993. PP. 245–251. DOI:10.1007/3-540-57220-1_66

3. Killer C., Rodrigues B., Scheid E.J., Franco M., Eck M., Zaugg N. Provotum: A Blockchain-based and End-to-end Verifiable Remote Electronic Voting System // Proceedings of the 45th Conference on Local Computer Networks (LCN, Sydney, Australia, 16–19 November 2020). IEEE, 2020. PP. 172–183. DOI:10.1109/LCN48667.2020.9314815

4. Suganya R., Sureshkumar A., Alaguvathana P., Priyadharshini S., Jeevanantham K. Blockchain Based Secure Voting System Using Iot // International Journal of Future Generation Communication and Networking. 2020. Vol. 13. Iss. 3. PP. 2134–2142.

5. Rasid N.H. Blockchain Technology in e-Voting: Comparative Study. 2020.

6. Ayed A.B. A Conceptual Secure Blockchain Based Electronic Voting System // International Journal of Network Security & Its Applications. 2017. Vol. 9. Iss. 3. PP. 1–9. DOI:10.5121/ijnsa.2017.9301

7. Программно-технический комплекс, обеспечивающий дистанционное электронное голосование избирателей (участников референдума) вне зависимости от места их нахождения. Описание ПТК ДЭГ. 2021. URL: https://evoting.digitaldem.ru/wp-content/uploads/sites/2/2021/07/ptkdeg_general_description_2021-07-15.pdf (дата обращения 07.09.2023)

8. КриптоВече. Инструкция к системе Базовое описание информационной системы «КриптоВече».

9. Dagher G.G., Marella P.B., Milojkovic M., Mohler J. BroncoVote: Secure Voting System Using Ethereum's Blockchain // Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP, Funchal, Portugal, 22–24 January 2018). Vol. 1. 2018. PP. 96–107. DOI:10.5220/0006609700960107

10. Yu B., Liu J., Sakzad A., Nepal S., Rimba P., Steinfeld R., Au M.H. Platform-Independent Secure Blockchain-Based Voting System // Cryptology ePrint Archive. 2018. URL: https://eprint.iacr.org/2018/657 (дата обращения 07.09.2023)

11. Hsiao J.-H., Tso R., Chen C.-M., Wu M.-E. Decentralized E-Voting Systems Based on the Blockchain Technology // Proceedings of the International Conference on Computing Systems and Applications on Advances in Computer Science and Ubiquitous Computing (Taichung, Taiwan, 18–20 December 2017). Lecture Notes in Electrical Engineering. Vol. 474. Singapore: Springer, 2018. PP. 305–309. DOI:10.1007/978-981-10-7605-3_50

12. Cramer R., Damgård I., Schoenmakers B. Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols // Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '94, Santa Barbara, USA, 21–25 August 1994). Lecture Notes in Computer Science. Vol. 839. Berlin, Heidelberg: Springer, 1994. PP. 174–187. DOI:10.1007/3-540-48658-5_19

13. Cramer R., Gennaro R., Schoenmakers B. A secure and optimally efficient multi- authority election scheme // European Transactions on Telecommunications. 1997. Vol. 8. Iss. 5. PP. 481–490. DOI:10.1002/ett.4460080506

14. Elgamal T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Transactions on Information Theory. 1985. Vol. 31. Iss. 4. PP. 469–472. DOI:10.1109/TIT.1985.1057074

15. Chaum D., Pedersen T.P. Wallet Databases with Observers // Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '94, Santa Barbara, USA, 16–20 August 1992). Lecture Notes in Computer Science. Vol. 740. Berlin, Heidelberg: Springer, 1994. PP. 89–105. DOI:10.1007/3-540-48071-4_7

16. Яковлев В.А., Салман В.Д. Методы защиты от угрозы неправильного заполнения избирательного бюллетеня в системе дистанционного электронного голосования // Труды учебных заведений связи. 2023. Т. 9. № 2. С. 128–142. DOI:10.31854/1813-324X-2023-9-2-128-142

17. Mohr A. A Survey of Zero-Knowledge Proofs with Applications to Cryptography. URL: http://austinmohr.com/ Work_files/zkp.pdf (дата обращения 07.09.2023)

References

1. Adida B. Helios: Web-based open-audit voting. *Proceedings of the 17th USENIX Security Symposium, 28–29 July 2008, San Jose, USA*. 2008. p.335–348.

2. Fujioka A., Okamoto T., Ohta K. A practical secret voting scheme for large scale elections. *Proceedings of the Advances in Cryptology – AUSCRYPT '92, 13–16 December 1992, Gold Coast, Queensland, Australia. Lecture Notes in Computer Science, vol.718*. Berlin, Heidelberg: Springer; 1993. p.245–251. DOI:10.1007/3-540-57220-1_66

3. Killer C., Rodrigues B., Scheid E.J., Franco M., Eck M., Zaugg N. Provotum: A Blockchain-based and End-to-end Verifiable Remote Electronic Voting System. *Proceedings of the 45th Conference on Local Computer Networks, LCN, 16–19 November 2020, Sydney, Australia*. IEEE; 2020. p.172–183. DOI:10.1109/LCN48667.2020.9314815

4. Suganya R., Sureshkumar A., Alaguvathana P., Priyadharshini S., Jeevanantham K. Blockchain Based Secure Voting System Using Iot. *International Journal of Future Generation Communication and Networking*. 2020;13(3):2134–2142.

5. Rasid N.H. *Blockchain Technology in e-Voting: Comparative Study*. 2020.

6. Ayed A.B. A Conceptual Secure Blockchain Based Electronic Voting System. *International Journal of Network Security & Its Applications*. 2017;9(3):1–9. DOI:10.5121/ijnsa.2017.9301

7. *Software and Hardware Complex Providing Remote Electronic Voting of Voters (Referendum Participants) Regardless of Their Location*. 2021. URL: https://evoting.digitaldem.ru/wp-content/uploads/sites/2/2021/07/ptkdeg_general_description_2021-07-15.pdf [Accessed 07.09.2023]

8. CryptoVeche. Instructions for the system Basic description of the information system "KriptoVeche".

9. Dagher G.G., Marella P.B., Milojkovic M., Mohler J. BroncoVote: Secure Voting System Using Ethereum's Blockchain. *Proceedings of the 4th International Conference on Information Systems Security and Privacy, ICISSP, 22–24 January 2018, Funchal, Portugal*. 2018. vol.1. p.96–107. DOI:10.5220/0006609700960107

10. Yu B., Liu J., Sakzad A., Nepal S., Rimba P., Steinfeld R., Au M.H. Platform-Independent Secure Blockchain-Based Voting System. *Cryptology ePrint Archive*. 2018. URL: https://eprint.iacr.org/2018/657 [Accessed 07.09.2023]

11. Hsiao J.-H., Tso R., Chen C.-M., Wu M.-E. Decentralized E-Voting Systems Based on the Blockchain Technology. *Proceedings of the International Conference on Computing Systems and Applications on Advances in Computer Science and Ubiquitous Computing, 18–20 December 2017, Taichung, Taiwan. Lecture Notes in Electrical Engineering, vol.474*. Singapore: Springer; 2018. p.305–309. DOI:10.1007/978-981-10-7605-3_50

12. Cramer R., Damgård I., Schoenmakers B. Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. *Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '94, 21–25 August 1994, Santa Barbara, USA. Lecture Notes in Computer Science, vol.839*. Berlin, Heidelberg: Springer; 1994. p.174–187. DOI:10.1007/3-540-48658-5_19

13. Cramer R., Gennaro R., Schoenmakers B. A secure and optimally efficient multi- authority election scheme. *European Transactions on Telecommunications*. 1997;8(5):481–490. DOI:10.1002/ett.4460080506

14. Elgamal T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*. 1985;31(4):469–472. DOI:10.1109/TIT.1985.1057074

15. Chaum D., Pedersen T.P. Wallet Databases with Observers. *Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '94, 16–20 August 1992, Santa Barbara, USA. Lecture Notes in Computer Science, vol.740*. Berlin, Heidelberg: Springer; 1994. p.89–105. DOI:10.1007/3-540-48071-4_7

16. Yakovlev V., Salman V. Methods of Protection against Threat: Incorrect Ballot Filling by Voter in the Remote Electronic Voting System. *Proc. of Telecom. Universities.* 2023;9(2):128–142. DOI:10.31854/1813-324X-2023-9-2-128-142

17. Mohr A. A Survey of Zero-Knowledge Proofs with Applications to Cryptography. URL: http://austinmohr.com/ Work_files/zkp.pdf [Accessed 07.09.2023]

Статья поступила в редакцию 14.08.2023; одобрена после рецензирования 20.08.2023; принята к публикации 20.08.2023.
The article was submitted 14.08.2023; approved after reviewing 20.08.2023; accepted for publication 20.08.2023.

Информация об авторах:

ЯКОВЛЕВ Виктор Алексеевич — доктор технических наук, профессор, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0009-0007-2861-9605

САЛМАН Васан Давуд — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0000-0003-4454-7844