УДК 342.843:003.26:004.056

Яркова О. Н., Осипова А. А.

ЗАЩИЩЕННАЯ СИСТЕМА ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ НА ОСНОВЕ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

В статье рассматривается актуальная проблема внедрения дистанционного голосования в существующий избирательный процесс. Авторами разработана система электронного голосования, защита которой построена на основе криптографических алгоритмов. Предложенная система подходит для проведения референдумов, а также выборов с большим количеством кандидатов.

Ключевые слова: *система электронного голосования; интернет-голосование.*

Yarkova O. N., Osipova A. A.

SECURE ELECTRONIC VOTING SYSTEM BASED CRYPTOGRAPHIC ALGORITHMS

The article deals with the actual problem of implementation distance voting in the existing electoral process. The authors have developed an electronic voting system with protection which based on cryptographic algorithms. The proposed system is suitable for holding elections with two or more candidates.

Keywords: *electronic voting system; Internet voting.*

Информатизация коснулась всех сфер общественной жизни и стала визитной карточкой XXI века. Переход процессов производства в автоматизированный режим, создание электронных ресурсов, развитие средств вычислительной техники свидетельствуют о научно-техническом прогрессе и позволяют называть современное общество информационным.

В развитых странах стали осуществляться целевые программы по автоматизации работы государственных служб. Одной из наиболее актуальных проблем является организация выборов через глобальную сеть Интернет. В США, Великобритании, Ирландии, Швейцарии и Эстонии для избрания членов центральных и местных органов власти используются системы электронного голосования (СЭГ), позволяющие избирателям дистанционно сделать свой выбор.

В России существует государственная автоматизированная система «Выборы», в рам-

ках которой реализуется процесс электронного голосования с помощью сенсорных устройств. Но на данный момент эти технологии используются только для проведения муниципальных выборов некоторых регионов страны; в большинстве случаев применяется система бумажно-электронного голосования. Развитие системы интернет-голосования только начинает набирать обороты.

Преимущества проведения выборов через сеть общего пользования очевидны. Среди них можно выделить:

• отсутствие необходимости появления на избирательном участке;

• осуществление подсчета голосов в более короткие сроки;

• увеличение явки на выборы «молодого» электората, пользующегося мобильными устройствами.

Наряду с достоинствами СЭГ возникают трудности ее внедрения. Так, для внедрения удаленного электронного голосования в России необходимо[1]:

• внедрение электронных удостоверений личности и соответствующей инфраструктуры открытых ключей;

• разработка надежного протокола голосования на основе криптографических алгоритмов;

• разработка ПО и аппаратуры;

• тестирование СЭГ на различном уровне (муниципальный, региональный, федеральный).

По различным экспертным оценкам внедрение системы интернет-голосования в Российской Федерации возможно через 8–10 лет.

Основная цель при организации избирательного процесса – гарантия получения достоверного результата. Поэтому на всех этапах проведения выборов необходимо обеспечить защиту сведений от модификации и уничтожения.

Отличием СЭГ от системы бумажно-электронного голосования является наличие канала передачи данных (КПД) между избирателем и счетной комиссией. При бумажном голосовании нарушению целостности информации препятствуют наблюдатели и система видеоконтроля на избирательном участке. Проведение дистанционного голосования должно сопровождаться иными мерами безопасности, направленными на защиту КПД. Наиболее эффективным методом защиты информации при передаче по каналу связи является шифрование.

Целью создания СЭГ является повышение уровня защищенности информации, циркулирующей при организации и проведении дистанционных выборов.

Для достижения поставленной цели в ходе работы решены следующие задачи:

• определение общих требований к СЭГ;

• определение этапов избирательного процесса и разработка схемы работы СЭГ;

• проведение анализа СЭГ, защита которой реализована на основе криптографиче-

Рис. 1. Упрощенная схема системы электронного голосования

Рис. 2. – Алгоритм работы системы электронного голосования

ских алгоритмов, предлагаемых источником[2], выделение достоинств и недостатков;

• предложение варианта модификации защищенной СЭГ для устранения выявленных недостатков.

В различных источниках можно найти перечни требований к интернет-выборам, отличающиеся формулировкой, но схожие по смыслу. Проанализировав сведения из[2-4], выделим основные свойства, которыми должна обладать система электронного голосования (СЭГ):

1) Контроль над избирателями (голосовать имеют право только уполномоченные избиратели; один человек имеет лишь один голос);

2) анонимность, тайна голосования (нельзя узнать выбор конкретного избирателя);

3) индивидуальный контроль (каждый избиратель может убедиться, что его голос учтен);

4) универсальный контроль (каждый из участников способен проверить, что результат подсчитан правильно, что не были вброшены лишние бюллетени);

5) устойчивость (некорректные действия избирателей или злоумышленные действия организаторов не должны сорвать выборы);

6) неподтверждаемость (после выборов нельзя доказать, что избиратель проголосовал определенным образом).

Руководствуясь представленными требованиями, были разработаны упрощенная схема работы СЭГ (рис. 1), а также подробный алгоритм функционирования (рис. 2). Участниками выборов являются кандидаты, голосующие и счетные комиссии, сведения о ко-

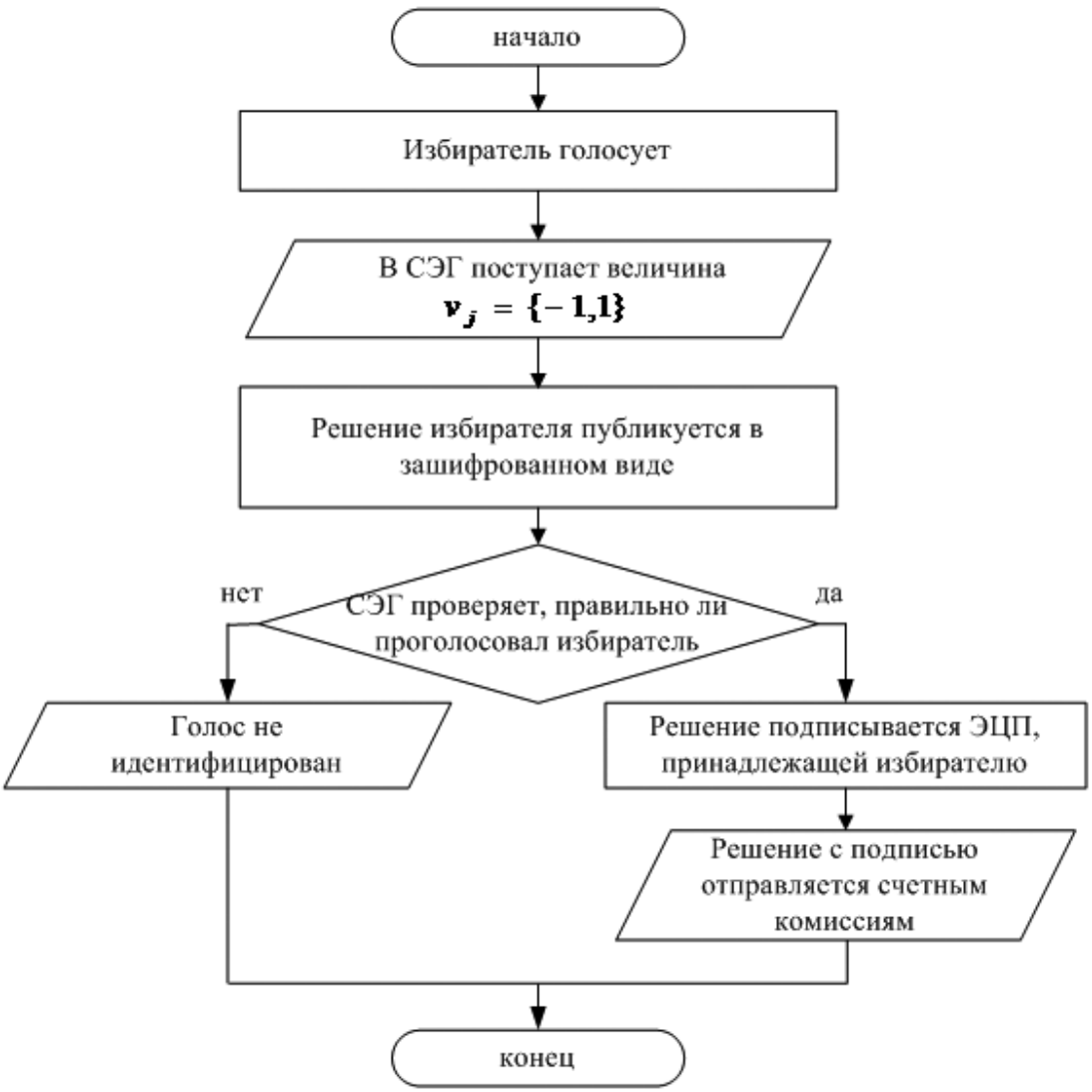

Рис. 3. Алгоритм заполнения бюллетеня в оригинальном варианте СЭГ

торых хранятся в базе данных с подсистемой обработки данных. Избирательный процесс в СЭГ включает в себя четыре этапа: заполнение электронного бюллетеня избирателем; передача бюллетеня счетным комиссиям; проверка достоверности и целостности полученной информации; определение результатов голосования.

Система электронного голосования, предложенная авторами источника[2], работает согласно представленным схемам. На всех этапах избирательного процесса для защиты канала передачи данных и циркулирующей информации применяются криптографические алгоритмы (электронная цифровая подпись (ЭЦП), протоколы идентификации и аутентификации и др.). Подробно они описаны в литературе[2,5].

Достоинством описанной СЭГ является соответствие всем вышеперечисленным требованиям. Но имеется недостаток, препятствующий внедрению данной системы: она применима только на референдумах, т. е. избирательных процессах, где голосующему предлагается выбрать одного кандидата из двух.

Предложим модификацию рассмотренной системы голосования для расширения круга кандидатов. Для этого определим исходные данные и обратимся к первому этапу избирательного процесса.

Пусть в голосовании участвуют m лиц с правом голоса, n счетных комиссий и k кандидатов ($k = 2$). Процедура заполнения бюллетеня избирателем в оригинальном варианте СЭГ представлена на рис. 3.

Как видно из схемы алгоритма заполнения бюллетеня (рис. 3), в СЭГ поступает величина $v = \{-1,1\}$, где $\{-1,1\}$ – множество кандидатов, включающее два элемента.

Увеличим количество кандидатов k ($k \geq 2$). На этапе голосования избирателя с $ID = j, j = \overline{1,m}$ предлагается отправлять в СЭГ вектор (1). Назовем вектор V_j бюллетенем j-ого избирателя:

$$V_j = (v_1, v_2, ..., v_{k+1}) \quad (1)$$

где $v_1 \in \{0,1\}$ – отметка о голосовании избирателя: «0» – не голосовал, «1» – голосовал;

Таблица 1. Бюллетени избирателей в незашифрованном виде и подведение итогов голосования

Номер избирателя	Отметка о факте голосования	Выбор избирателя относительно конкретного кандидата				
		k=1	k=2	k=3	k=4	k=5
1	1	-1	1	-1	-1	-1
2	1	1	-1	-1	-1	-1
3	1	-1	-1	1	-1	-1
4	1	1	-1	-1	-1	-1
5	1	-1	-1	-1	-1	1
6	0	-	-	-	-	-
7	1	1	-1	-1	-1	-1
8	1	1	-1	-1	-1	-1
9	1	1	-1	-1	-1	-1
10	1	-1	1	-1	-1	-1
11	0	-	-	-	-	-
12	1	-1	-1	1	-1	-1
13	1	-1	-1	-1	-1	1
14	1	1	-1	-1	-1	-1
15	1	-1	-1	-1	1	-1
Сумма голосов	13	6	2	2	1	2
Итоги выборов (%)		46,14	15,39	15,39	7,69	15,39

$v_2,...,v_{k+1} \in \{-1,1\}$ – выбор избирателя относительно конкретного кандидата: «-1» – против, «1» – за;

k – количество кандидатов.

Подсчет голосов за кандидата k будет производиться по формуле (2)

$$U_k = \frac{\sum_{j=1}^{m} v_{jk} + \sum_{j=1}^{m} v_{j1}}{2}, \quad (2)$$

где U_k – сумма голосов за кандидата k;

$j = \overline{1,m}$ - порядковый номер избирателя;

$\sum_{j=1}^{m} v_{j1}$ - общее количество проголосовавших.

Несложно подсчитать процент голосов за каждого кандидата:

$$U_{k\%} = \frac{\sum_{j=1}^{m} v_{j1}}{U_k} * 100\%. \quad (3)$$

Проверим работу предложенного алгоритма. Пусть количество избирателей $m = 15$, количество кандидатов $k = 5$. Результат представлен в табл. 1.

Следует отметить, что бюллетени представлены в таблице в открытом виде для наглядности; в процессе работы СЭГ они передаются в виде затемненного обязательства[5].

Как видно из табл. 1, подсчет результатов при обработке незашифрованных бюллетеней корректен. Проблема заключается во внедрении предложенных изменений в СЭГ. Необходима проверка соответствия модифицированной системы требованиям, представленным выше. Особое внимание следует обратить на устойчивость СЭГ (п. 5 требований). Остальные условия будут выполнены, если каждая компонента вектора (1) будет шифроваться своим уникальным ключом в соответствии с алгоритмом, представленным на рис. 3.

Таким образом, в предложенной системе дистанционного голосования, защищенной с помощью криптографических алгоритмов, можно выделить следующие характеристики:

• регистрация пользователей и формирование ЭЦП обеспечивают участие в выборах уполномоченных лиц;

• избиратель не может проголосовать более одного раза, и его голос никто не может дублировать;

• отправка бюллетеня в виде затемненного обязательства гарантирует верифицируемость (позволяет проверить, что данные получены от уполномоченного избирателя, скрывая при этом его личность);

• протокол идентификации совместно с затемненным обязательством обеспечивают соблюдение тайны голосования;

• система обеспечивает корректный подсчет результата.

Реализация аналогичной системы на языках веб-программирования может стать основой защищенного интернет-ресурса для голосования.

Примечания

[1] Гребнев, С. В. Электронное голосование и криптография: проблемы, решения и перспективы. М.: 2011. 17 с.

[2] Смарт, Н. Криптография. М.: Техносфера. 2005. 528 с.

[3] Лифшиц, Ю. Электронные выборы. СПб.: 2005. 9 с.

[4] Алехова Е. Ю. Система тайного электронного голосования на базе локальной сети // Электронное научно-техническое издание «Наука и образование». 2004. URL: http://technomag.edu.ru/doc/44988.html/ (дата обращения: 22.04.2014).

[5] См.: Осипова, А. А. Яркова, О. Н. Модель интерактивной системы электронного голосования // Естественные и математические науки в современном мире. № 11 (11). сборник статей по материалам XII международной научно-практической конференции. Новосибирск: Изд. «СибАК». 2013. 226 с.

References

[1] Grebnev, S.V. Elektronnoe golosovanie i kriptografiya: problemy, resheniya i perspektivy [Electronic Voting and Cryptography: Problems, Solutions, and Perspectives]. Moscow: 2011. 17 p.

[2] Smart, N. Kriptografiya [Cryptography]. Moscow: Tekhnosfera Publ.. 2005. 528 p.

[3] Lifshits, Yu. Elektronnye vybory [Electronic Elections]. St. Petersburg: 2005. 9 p.

[4] Alekhova E.Yu. Sistema tainogo elektronnogo golosovaniya na baze lokal'noi seti [System of Secret Electronic Voting on the Basis of Local Network]// Electronic scientific and technical publication «Science and Education». 2004. URL: http://technomag.edu.ru/doc/44988.html/ (Date of Access: 22.04.2014).

[5] Sm. Osipova, A.A. Yarkova, O.N. Model' interaktivnoi sistemy elektronnogo golosovaniya [Model of Interactive System of Electronic Voting]// Estestvennye i matematicheskie nauki v sovremennom mire. No. 11 (11) sbornik statei po materialam XII mezhdunarodnoi nauchno-prakticheskoi konferentsii. Novosibirsk: «SibAK» Publ., 2013. 226 p.

Яркова Ольга Николаевна, кандидат экономических наук, доцент кафедры математических методов и моделей в экономике Оренбургского государственного университета. E-mail: yarkova_on@mail.ru

Осипова Александра Александровна, студент кафедры вычислительной техники и защиты информации Оренбургского государственного университета. E-mail: sandrenok92@mail.ru

Olga Nikolaevna Yarkova, Cand. Sc. Economics, Associate Professor, Associate Professor of the Department of mathematical Methods and Models in Economics of Orenburg State University. E-mail: yarkova_on@mail.ru

Aleksandra Aleksandrovna Osipova, Student of the Department of Computational Machinery and Information Security of Orenburg State University. E-mail: sandrenok92@mail.ru