DOI 10.34185/1562-9945-6-155-2024-06
УДК 004.056.5

Д.О. Остапець, В.А. Мотиленко

АНАЛІЗ ПІДХОДІВ ДО РЕАЛІЗАЦІЇ СИСТЕМ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

Анотація. У роботі розглядаються сучасні підходи для побудови систем електронного голосування, такі як блокчейн, а також традиційні криптографічні методи, що включають гомоморфне шифрування, сліпий підпис та докази нульового розголошення. Метою роботи є вибір підходу до побудови систем електронного голосування на основі порівняльного аналізу їх основних характеристик. Вирішувані задачі: огляд вимог, узагальненої структури та основних процедур систем електронного голосування; аналіз існуючих видів систем електронного голосування та їх порівняльна характеристика. Виділено список вимог до систем електронного голосування, представлено узагальнені структури основних їх видів. Проведено порівняльний аналіз видів систем електронного голосування на основі відповідності вимогам. Зроблено вибір підходу для подальшої побудови системи.
Ключові слова: електронне голосування, гомоморфне шифрування, блокчейн, докази з нульовим розголошенням, сліпий підпис.

Постановка проблеми. При проектуванні систем електронного голосування важливим аспектом постає формулювання вимог до програмної частини. Рада Європи [1] випустила директиву, яка описує формальні вимоги до таких систем. Директиви описують юридичні аспекти та залишають питання реалізації і криптобезпеки не вирішеними. З розвитком цифрових технологій з’являється значний потенціал для вдосконалення процесів голосування через впровадження електронних систем. З впровадженням електронних систем приходять і нові виклики, особливо у плані забезпечення безпеки даних та недопущення маніпуляцій з результатами виборів. Криптографія відіграє ключову роль у створенні безпечних електронних систем голосування, дозволяючи забезпечити конфіденційність голосів і верифікацію результатів без розкриття особистості виборців.

Одним з передових напрямків [2, 3] у розробці безпечних систем електронного голосування є використання технології блокчейн. Ця технологія дозволяє створити децентралізовану і незмінну базу даних голосів, яка може захистити процес від фальсифікацій та несанкціонованого доступу. Водночас, існують і інші технології та підходи, здатні підвищити ефективність та безпеку електронного голосування, включаючи різноманітні криптографічні протоколи які можуть забезпечити анонімність виборців, верифікацію результатів та неможливість подвійного голосування.

© Остапець Д.О., Мотиленко В.А., 2024

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Аналіз останніх досліджень і публікацій. Гомоморфне шифрування використовується у системах електронного голосування для проведення операції підрахунку голосів без розкриття ідентифікатора голосуючого [4, 5]. Сучасні технології доказів з нульовим розголошенням дозволяють неінтерактивно провести операції над зашифрованими даними, зберігаючи криптографічний доказ, що вихідні данні не було змінено [6, 7]. Змішані сітки за допомогою спеціальних протоколів маршрутизації дозволяють сховати ідентифікатор голосуючого [8]. Блокчейн системи використовуються для забезпечення децентралізованого сховища і інфраструктурної організації систем електронного голосування [2, 9].

Системи електронного голосування активно досліджуються, як з боку використання сучасної криптографії [10, 11], так і з боку організації віддаленого доступу та забезпечення державних вимог [12].

Мета дослідження. Метою роботи є вибір підходу до побудови систем електронного голосування на основі порівняльного аналізу їх основних характеристик. Результати аналізу можуть бути використані при реалізації відповідних систем. В роботі відповідно до мети поставлені такі задачі: огляд вимог, узагальненої структури та основних процедур систем електронного голосування; аналіз існуючих видів систем електронного голосування та їх порівняльна характеристика. У роботі не розглядаються конкретні реалізації систем, а тільки підходи до їх реалізацій.

Основний матеріал дослідження. У системах електронного голосування є кілька ключових діючих сторін, кожна з яких має свої функції та права. Основні діючі сторони включають [12]:

- ***Виборці*** – це особи, які мають право голосу і беруть участь у виборах.
- ***Кандидати*** – це особи та організації, які беруть участь у виборах і змагаються за голоси виборців.
- ***Адміністратори (або посадові особи)*** – це органи та особи, відповідальні за організацію і проведення виборів
- ***Спостерігачі (Аудитор)*** – це особи, які контролюють виборчий процес, забезпечуючи його прозорість та чесність.
- ***Реєстратор*** – відповідальний за автентифікацію виборців. Вони видають виборцям дані для доступу до системи, такі як приватні та публічні ключі.

Вимоги до системи. Аналіз існуючих підходів до побудови систем доцільно почати з формування списку формальних вимог до систем, за якими можна якісно або кількісно порівняти існуючі системи.

Як пише Ліав Х. [14], в існуючих дослідженнях часто використовують різні терміни для одних і тих самих сутностей. Не всі системи електронного голосування задовольняють однаковий набір властивостей безпеки, в силу їх протиріччя. Наприклад питання перевіряємості (verifiability) та ревізійність (auditability) завжди протиставляється питанню приватності та анонімності. Базуючись на дослідженнях Лі Б. [14] є доцільним вимагати наступні властивості безпеки:

- ***Анонімність голосування*** - система повинна гарантувати, що ніхто не може простежити, за кого проголосував конкретний виборець.

- ***Універсальна перевіряємість*** - будь-який зацікавлений учасник процесу (виборець, спостерігач, незалежна організація) може переконатися в правильності підрахунку голосів. Перевіряємість також може бути індивідуальною, коли система дозволяє перевірити кожному голосуючому що його голос був врахований.
- ***Чесність*** (fairness) - часткові результати не повинні бути опубліковані.
- ***Надійність*** (robustness) - стійкість системи до зловмисної поведінки учасників процесу.
- ***Відсутність квитанцій*** (receipt-freeness) - система не повинна надавати виборцю документ який би підтверджував за кого він голосував.

Структура системи електронного голосування. Алгоритм роботи систем електронного голосування можна розбити на три основні фази: початкове налаштування (див. рис. 1), збір голосів (див. рис. 2) та підрахунок і оприлюднення голосів (див. рис. 3).

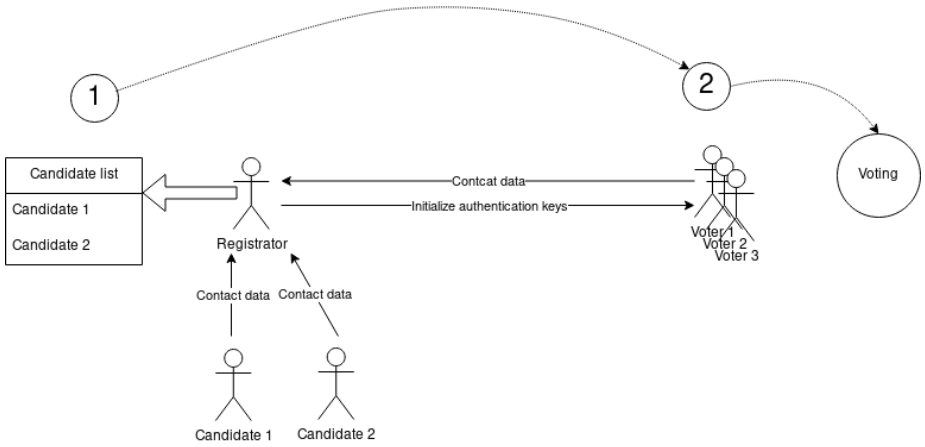

Рисунок 1 - Узагальнена схема процедури ініціалізації системи електронного голосування

У ході початкового налаштування виставляються параметри системи, такі як максимальна кількість кандидатів, строки виборів, а також проходять наступні процеси:

1. ***Реєстрація кандидатів (Candidate Registration)*** – подача заявок кандидатами для участі у виборах, реєстратор перевіряє дані кандидатів і додає до списку кандидатів.

2. ***Реєстрація виборців (Voter Registration)*** – збір і верифікація даних виборців, забезпечення їхньої автентифікації в системі. У ході цього шагу також проходить розповсюдження криптографічних ключів, або інших даних необхідних для автентифікації користувачів.

Далі система може переходити до наступного етапу.

Основні кроки (див. рис. 2):

1. У ході процесу збору голосів, важливо щоб усі голосуючі мали доступ до списку кандидатів та параметрів системи.

2. Далі, голосуючі формують свої голоси та автинтифікуються у регістратора для відправки цього голосу, в деяких схемах цей процес автентифікації голосуючого та

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

відправки голосу може бути реалізований в рамках одного кроку.

3. Після надсилання голосу, голосуючі отримують підтвердження, що їх голос опрацьований.

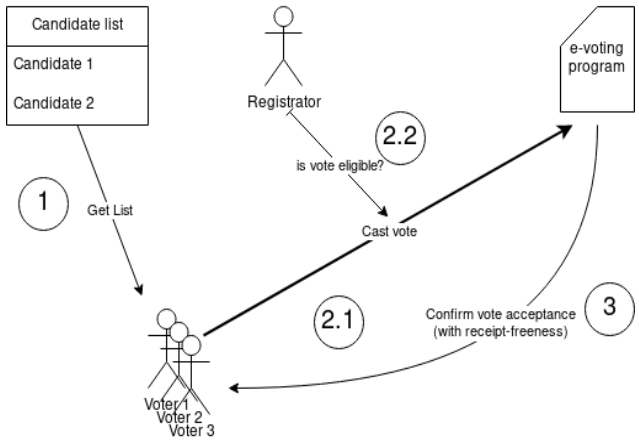

Рисунок 2 - Узагальнена схема процедури збору голосів

На цьому етапі важливо дотримання деяких властивостей:

1. ***Анонімність голосу*** - сам голос не має містити інформації про ідентифікатор користувача. При цьому очевидним є вимога до системи щодо захисту від подвійного голосування.

2. ***Анонімність голосуючих*** - система повинна використовувати деякі методи, наприклад змішування [8] щоб відв’язати ідентифікатор користувача від його голосу.

Відсутність квитанцій - при підтверджені голосу, голосуючі не повинні отримувати так звані “квитанції” - підтвердження за кого саме із кандидатів вони голосували.

У ході процедури фіналізації (див. рис. 3) зашифровані голоси дешифруються сервером, і кожен голосуючий може перевірити що їх голос було враховано.

Програма також формує список результат з фінальною кількістю голосів за кожного кандидата. Спостерігачі можуть перевірити що голоси були чесно підраховані.

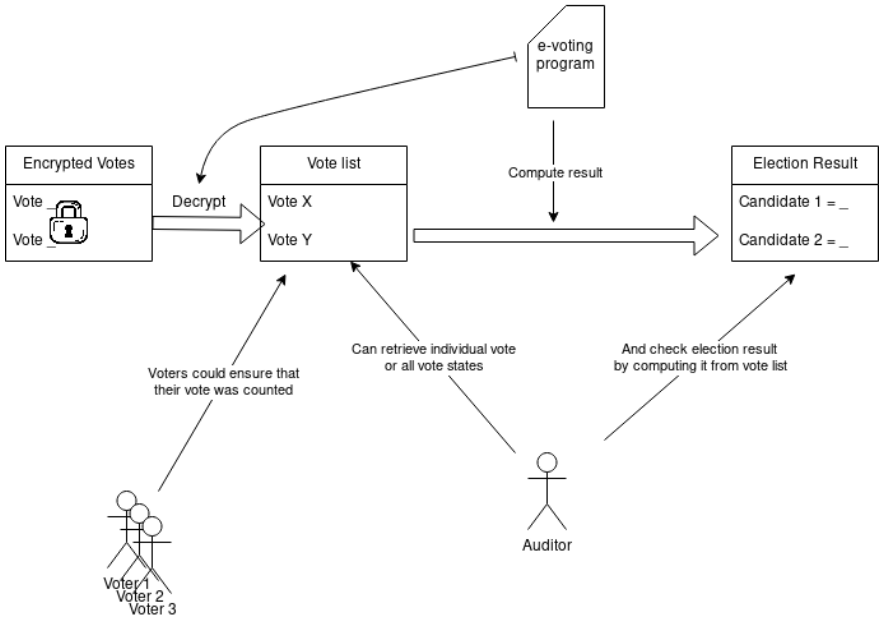

Рисунок 3 - Узагальнена схема підрахунку і оприлюднення голосів

Основні види систем електронного голосування. ***Гомоморфне шифрування*** дозволяє учасникам шифрувати свої голоси таким чином, що сервер голосування зможе підрахувати загальний результат без необхідності розшифровувати окремі голоси.

Тобто, для заданих E(v1), E(v2), можна підрахувати E(v1 ⊗ v2) без дешифровки v1 та v2.

У схемі (див. рис. 4) голосуючими є Alice та Bob - вони відправляють свої зашифровані голоси. Система може підрахувати голоси та видати результат. Системи на основі гомоморфного шифрування потребують додатково схеми доказу. Це може бути або доказ нульового розголошення, або довіри до адміністратора під час збору даних, або додаткових схем часткового розшифрування [3].

Система на базі гомоморфного шифрування має наступні властивості:

- ***Анонімність голосування*** - усі голоси зашифровані на стороні відправника, а отже залишається тільки питання доставки голосу.
- ***Універсальна перевіряємість*** - після підрахунку голосів, усі голоси доступні у зашифрованому вигляді, а отже усі небайдужі можуть повторити підрахунок самотужки.
- ***Відсутність квитанцій*** - залежить від схем доказу.
- ***Надійність*** - стійкість системи до зловмисної поведінки залежить від схем доказу унікальності голосу.
- ***Чесність*** - можливе тільки при довірі до серверу електронного голосування, лежить за межами питання підходу гомоморфного шифрування.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

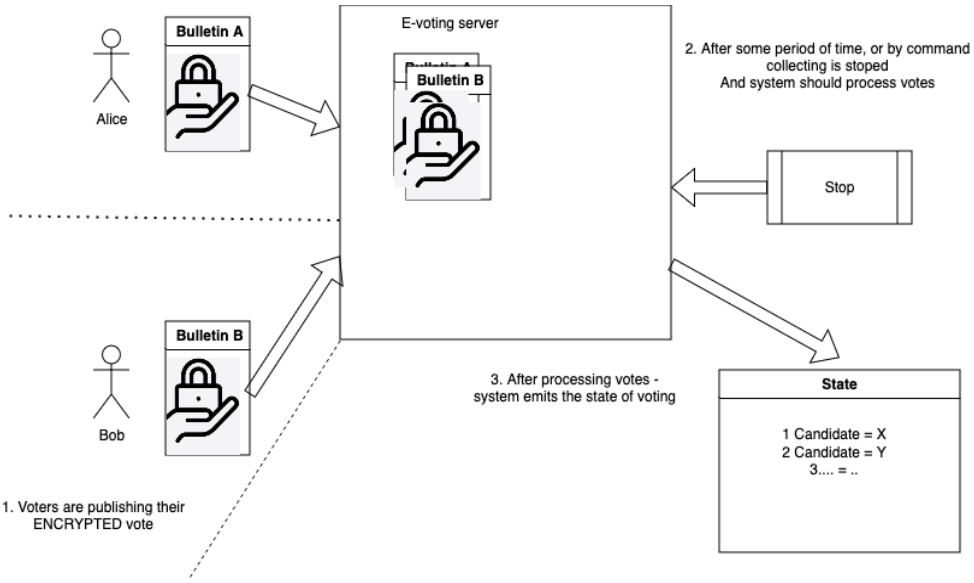

Рисунок 4 – Спрощена структура взаємодії з сервером у системі на базі гомоморфного шифрування

Сліпий підпис дозволяє учасникам довести своє право на голосування без розкриття своєї ідентичності, що допомагає забезпечити анонімність та запобігти подвійному голосуванню (див. рис.5).

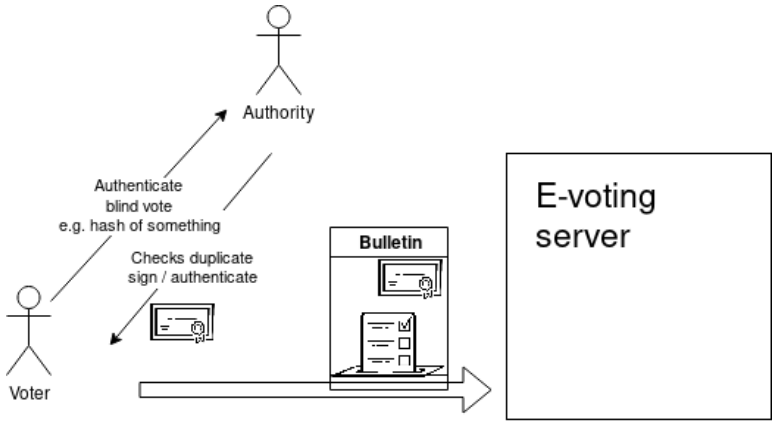

Рисунок 5 – Спрощена структура взаємодії з сервером у системі на базі сліпого підпису

Система на базі сліпого підпису має наступні властивості:

- ***Анонімність голосування*** - сліпі підписи дозволяють виборцеві засліпити свій бюлетень перед відправкою. Після отримання підпису виборець знімає засліплення, і кінцевий підписаний бюлетень не містить ідентифікатор виборця. Виборчий орган підписує бюлетень без знання його вмісту, тому анонімність виборця зберігається.
- ***Універсальна перевіряємість*** - сліпі підписи забезпечують, що бюлетені були підписані виборчим органом, але не розкривають інформацію про те, хто подав конкретний бюлетень. Це дозволяє будь-якому учаснику перевірити, що всі бюлетені підписані легітимним органом. Однак, універсальна перевіряємість також вимагає можливості перевірки правильності підрахунку голосів без компрометації анонімності, що потребує додаткових механізмів, таких як криптографічне доказування з нульовим

розголошенням (Zero-Knowledge Proofs).

- ***Відсутність квитанцій*** - виборець не отримує жодного доказу свого голосу після відправки підписаного бюлетеня до системи. Це унеможливлює ситуацію, коли виборець може довести третій стороні, за кого він голосував, що запобігає примусу або купівлі голосів.
- ***Надійність*** - тільки з іншими криптографічними методами.
- ***Чесність*** - тільки при довірі до адміністратора.

Блокчейн дозволяє побудувати децентралізовану систему, в якій немає довіри до єдиного сервера (див. рис. 6). У цій схемі - Alice та Bob, це учасники, вони публікують свої голоси у блокчейн. Стан системи може в режимі реального часу підраховувати голоси, або робити це за командою адміністратора.

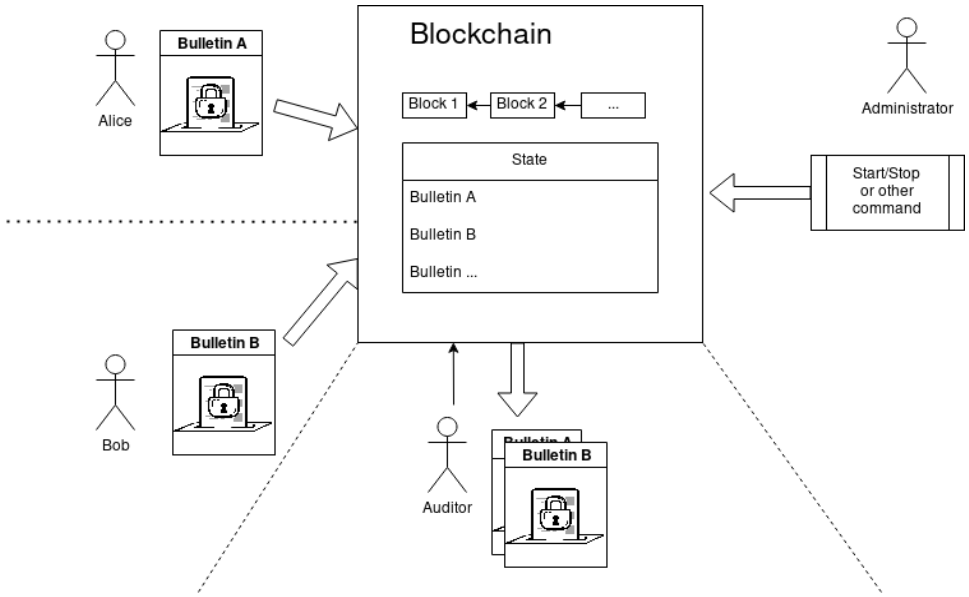

Рисунок 6 – Спрощена структура реалізації системи електронного голосування на базі блокчейну

Система на базі блокчейну має наступні властивості:

- ***Анонімність голосування*** - може бути забезпечена лише за умови використання псевдонімів або інших методів, що приховують справжню особистість виборців. Без додаткових методів для забезпечення анонімності, таких як шифрування або змішування, блокчейн не може гарантувати анонімність.
- ***Універсальна перевіряємість*** - кожна транзакція на блокчейні є незмінною і доступною для перевірки. Це дозволяє будь-якому учаснику перевірити, що кожен голос був зарахований правильно і не змінений після подання.
- ***Відсутність квитанцій*** -для забезпечення відсутності квитанцій потрібні додаткові методи, такі як сліпі підписи або інші криптографічні протоколи.
- ***Надійність*** - блокчейн забезпечує високу надійність завдяки своїй децентралізованій природі і криптографічному захисту. Всі транзакції є незмінними і захищеними від фальсифікації. Консенсусні механізми, такі як Proof of Work або Proof of Stake, забезпечують цілісність і достовірність даних.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

- ***Чесність*** - блокчейн забезпечує прозорість і неможливість зміни результатів після подання голосу. Проте, без додаткових механізмів автентифікації і контролю, блокчейн не може повністю гарантувати, що кожен голос є легітимним (тобто, поданий дійсним виборцем). Потрібні додаткові заходи для перевірки правомірності виборців і запобігання подвійного голосування.

Докази нульового розголошення використовуються для верифікації того, що голоси відповідають правилам голосування (наприклад, належать до допустимого набору варіантів) без необхідності розкривати голоси (див. рис. 7). У цій схемі Alice та Bob генерують докази для шифрованих голосів. Сервер прийому голосів точно знає що голос ще не був врахований, і належить до належного користувача, а також те що бюлетень не був зіпсований.

Сучасні системи доказів нульового розголошення такі як zk-SNARK та zk-STARK є універсальними та можуть бути повною заміною гомоморфного шифрування [6, 7], тому вони майже повністю копіюють властивості систем на бази гомоморфного шифрування доповнюючи деякі питання автентифікації.

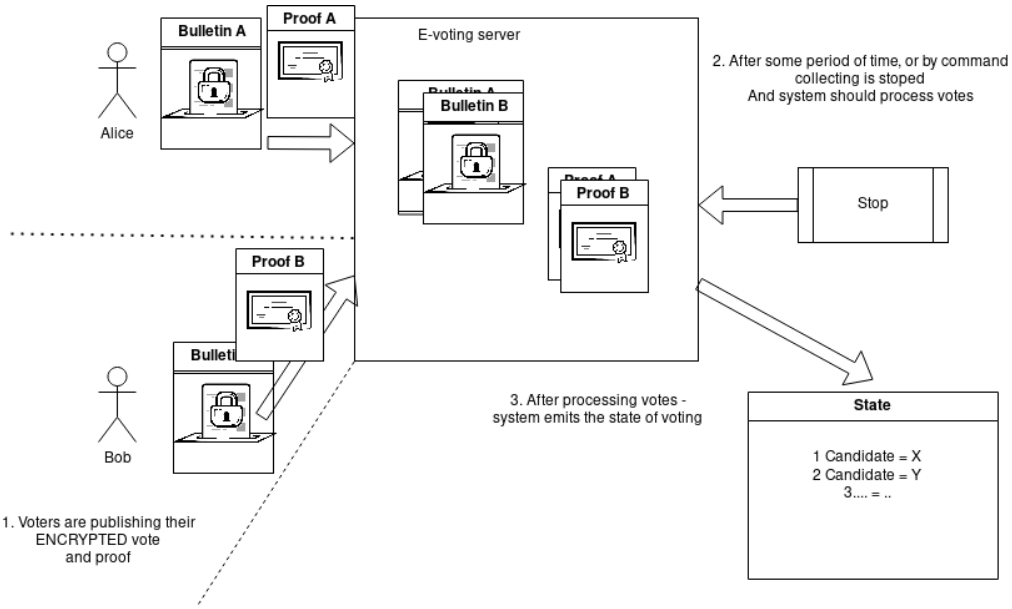

Рисунок 7 – Спрощена структура реалізації системи електронного голосування на базі доказів нульового розголошення

Система на базі доказів нульового розголошення має наступні властивості:

- ***Анонімність голосування*** - усі голоси зашифровані на стороні відправника, а отже залишається тільки питання доставки голосу.
- ***Універсальна перевіряємість*** - після підрахунку голосів, усі голоси доступні у зашифрованому вигляді, а отже усі небайдужі можуть повторити підрахунок самотужки.
- ***Відсутність квитанцій*** - залежно від реалізації, але більшість систем на базі ZKP повністю задовольняють цю вимогу.
- ***Надійність*** - доказ також автентифікує голосуючого, що можна використовувати для фільтрації небажаних голосів.

- ***Чесність*** - можливе тільки при довірі до серверу електронного голосування, лежить за межами питання підходу доказів з нульовим розголошенням.

За результатами аналізу відомих видів систем електронного голосування проведено їх порівняльну характеристику (див. табл. 1).

Таблиця 1

Порівняльна характеристика відомих видів систем електронного голосування

	Анонімність	Перевіряємість	Чесність	Надійність	Відсутність квитанцій
Гомоморфне шифрування	+	+	*	-	-
Сліпий підпис	+	+	*	-	+
Блокчейн системи	-	+	-	+	-
Докази нульового розголошення	+	+	*	+	+

Примітка: символами «+» відмічена повна відповідність, «-» невідповідність, «*» часткова відповідність.

За результатами порівняльного аналізу виходить, що системи на базі гомоморфного шифрування та сліпого підпису потребують додаткових механізмів криптографічних доказів, що робить їх використання без доказів нульового розголошення непрактичним. Також, з порівняння видно, що технологія блокчейн може бути використана тільки при використанні інших криптографічних методів. Сучасні докази нульового розголошення забезпечують майже усі властивості. Єдиним питанням у таких систем залишається питання довіри до серверу. Технологія блокчейн вирішує проблему довіри до серверу та робить процес децентралізованим, саме тому доцільним є використання гібридної системи блокчейну та сучасних доказів з нульовим розголошенням.

Висновки. У роботі проаналізовані існуючі підходи до побудови систем електронного голосування. Виділено список вимог до систем електронного голосування, побудовані узагальнені структури основних видів систем. На основі характеристик видів систем проведено їх порівняльний аналіз. Для забезпечення усіх властивостей в кожному з видів систем потрібна реалізація додаткових механізмів. В результаті запропоновано гібридну систему, яка може задовольнити усі необхідні властивості.

ЛІТЕРАТУРА / REFERENCES

1. Recommendation on legal, operational and technical standards for e-voting: Rec of 30.09.2004. URL: https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/00Rec(2004)11_rec_adopted_en.asp.

2. Hajian M. Berenjestanakiet al, Blockchain-Based e-voting systems: a technology review // Electronics. 2023. Vol. 13, no. 1. P. 17.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

3. Y. Zhan et al. Efficient Electronic Voting System Based on Homomorphic Encryption // Electronics. 2024. Vol. 13, no. 2. P. 286.
4. A. Abu Aziz A., N.Qunoo H., A. Abu Samra A. Using Homomorphic Cryptographic Solutions on E-voting Systems // International Journal of Computer Network and Information Security. 2018. Vol. 10, no. 1. P. 44–59.
5. Shinde S. S., Shukla S., Chitre D. K. Secure E-voting Using Homomorphic Technology // International Journal of Emerging Technology and Advanced Engineering. 2013. Vol. 3, no. 8. P. 203–206.
6. Panait A.-E., F. Olimid R. On Using zk-SNARKs and zk-STARKs in Blockchain-Based Identity Management // Innovative Security Solutions for Information Technology and Communications. 2020. T. 12596. URL: https://link.springer.com/chapter/10.1007/978-3-030-69255-1_9.
7. Ashur T., Dhooghe S. MARVELlous: a STARK-friendly family of cryptographic primitives // International Association for Cryptologic Research. 2018. No. 1098. URL: https://eprint.iacr.org/2018/1098.
8. Bibiloni P., Escala A., Morillo P. Vote Validatability in Mix-Net-Based eVoting // E-Voting and Identity. 2015. URL: https://link.springer.com/chapter/10.1007/978-3-319-22270-7_6.
9. Jafar U., Ab Aziz M. J., Shukur Z. Blockchain for electronic voting system–review and open research challenges // Sensors. 2021. Vol. 21, no. 17.
10. Kho Y.-X., Heng S.-H., Chin J.-J. A Review of Cryptographic Electronic Voting // Symmetry. 2022. Vol. 14, no. 5. P. 858.
11. K. M. AboSamra et al. A practical, secure, and auditable e-voting system // Journal of information security and applications. 2017. Vol. 36. P. 69–89.
12. Li H., Kankanala A. R., Zou X. A Taxonomy and Comparison of Remote Voting Schemes. IEEE. 2014. No. 23.
13. Liaw H.-T. A secure electronic voting protocol for general elections. Computers & Security. 2004. Vol. 23, no. 2. P. 107–119.

Received 03.09.2024.
Accepted 09.09.2024.

Analysis of approaches of electronic voting systems implementation

The work examines modern approaches to building electronic voting systems, such as blockchain, which promises to revolutionize the process due to its immutability and decentralization properties, as well as traditional cryptographic methods, including homomorphic encryption, which allows vote counting without the need to decrypt each individual vote. Blind signatures ensure the ability to confirm a vote without disclosing the user's identity, and zero-knowledge proofs allow voting without interacting with the server. The goal of the work is to select an approach for building electronic voting systems based on a comparative analysis of their key characteristics. The solved tasks include reviewing the requirements, generalized structures, and main procedures of electronic voting systems; analyzing the existing types of electronic voting systems and their comparative characteristics. During the work, existing systems and other literature were thoroughly analyzed. The article provides a detailed analysis of the advantages and limitations of these technologies, as well as their suitability for dif-

ferent electoral systems, considering important aspects such as scalability, efficiency, and protection against potential threats. Throughout the work, a list of requirements for electronic voting systems was compiled, the main procedures present in electronic voting systems were outlined, a set of actors in typical electronic voting systems was defined, and the generalized structures of their main types were presented. A comparative analysis of the types of electronic voting systems based on compliance with the requirements was conducted. An approach was chosen for further system development.

Остапець Денис Олександрович – к.т.н., доцент, доцент кафедри «Електронні обчислювальні машини» Українського державного університету науки і технологій, ORCID: 0000-0003-1778-7770
Мотиленко Володимир Артемович – аспірант Українського державного університету науки і технологій, ORCID: 0000-0003-3337-9945

Ostapets Denys – candidate of technical sciences, associate professor, associate professor of «Electronic computers» department of Ukrainian State University of Science and Technologies, ORCID: 0000-0003-1778-7770
Motylenko Volodymyr – graduate student of Ukrainian State University of Science and Technologies, ORCID: 0000-0003-3337-9945

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)