Харківський національний університет імені В. Н. Каразіна

Міністерство освіти і науки України

Кваліфікаційна наукова

праця на правах рукопису

Ісірова Катерина Володимирівна

УДК 004.056.5

ДИСЕРТАЦІЯ

МОДЕЛІ І МЕТОДИ ПОБУДОВИ ДЕЦЕНТРАЛІЗОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ НА ОСНОВІ ТЕХНОЛОГІЇ BLOCKCHAIN ТА ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

Спеціальність 122 — Комп'ютерні науки

(Галузь знань 12 — Інформаційні технології)

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

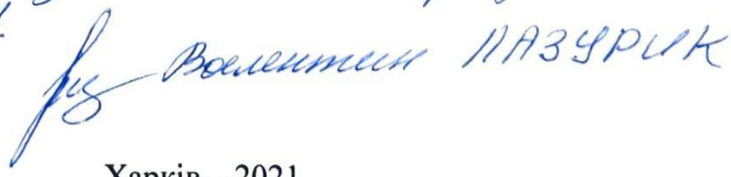
_____ К. В. Ісірова

Науковий керівник: Потій Олександр Володимирович, доктор технічних наук, професор.

Усі примірники дисертації ідентичні за змістом

Голова спеціалізованої вченої ради

ДФ 64.051.021



Валентин ПАЗУРИК

Харків – 2021

АНОТАЦІЯ

Ісірова К. В. Моделі і методи побудови децентралізованих електронних довірчих послуг на основі технології blockchain та постквантової криптографії. — Кваліфікаційна наукова праця на правах рукопису

Дисертація на здобуття ступеня доктора філософії за спеціальністю 122 — Комп'ютерні науки (Галузь знань 12 — Інформаційні технології). – Харківський національний університет імені В. Н. Каразіна Міністерства освіти і науки України, Харків, 2021.

В сучасних умовах стрімкого розвитку електронних технологій, а також різкого збільшення користувачів відповідних систем, побудова довіри в online-середовищі виступає одним із ключових питань для забезпечення соціального та економічного розвитку суспільства. Основною метою України є не тільки впровадження повного спектру електронних довірчих послуг, а також забезпечення їхньої інтероперабельності та транскордоності з міжнародними системами. З іншого боку, прогрес у сфері квантових обчислень обумовлює значне зростання швидкості, що формує нові виклики для сучасних систем безпеки інформації.

Дисертаційна робота присвячена розв'язанню актуальної задачі: розробка моделей і методів забезпечення стійкості та резильєнтності систем електронних довірчих послуг у постквантовий період.

Мета і завдання дослідження. Метою дисертаційної роботи є розробка методів забезпечення надійної і безпечної роботи систем електронних довірчих за рахунок використання технології blockchain та постквантової криптографії.

Для досягнення поставленої мети були розв'язані наступні задачі.

1. Аналіз міжнародних вимог до криптоалгоритмів постквантового періоду.
2. Аналіз можливості використання децентралізованих технологій, зокрема технології blockchain, для забезпечення резильєнтності систем у постквантовий період.

3. Розробка моделі децентралізованої інфраструктури відкритих ключів на основі технології blockchain для використання у постквантовий період.
4. Розробка моделі децентралізованої системи електронного голосування на основі технології blockchain для використання у постквантовий період.
5. Аналіз методів криптографічних перетворень типу електронний підпис, на основі геш-функцій, що можуть бути застосованими у постквантовий період.
6. Розробка методу одноразових ключів на основі схеми Winternitz для постквантового періоду.

У першому розділі дисертації (*Електроні довірчі послуги у сучасному світі*) на основі проведеного аналізу показано, що успіхи в галузі квантових обчислень формують нові виклики для сучасної криптографії та обумовлюють необхідність пошуку нових шляхів забезпечення безпеки інформації. Обґрунтовані основні напрямки розробок нових квантово-захищених алгоритмів. Показано, що на сьогоднішній день визначені основні напрямки розробок нових квантово-захищених алгоритмів: криптографічні перетворення на основі завадостійких кодів (CB-криптографія), перетворення на основі геш-функцій (HB-криптографія), криптографічні перетворення на решітках (LB-криптографія), мультіваріативно-квадратичні криптографічні перетворення (MQ-перетворення), а також використання ізогеніїв еліптичних кривих. Розкрито, що безпека систем може забезпечуватися не лише за рахунок криптостійкості примітивів, які покладені в її основу, а також шляхом впровадження відповідних організаційних, організаційно-технічних рішень та методів. Сформульоване поняття резильєнтності систем, а також показано як вона пов’язана із можливістю системи продовжувати функціонування навіть в умовах кібератак. Розкрита сутність моделей загроз для постквантового періоду, таких як IND-CCA2 (Indistinguishability under Adaptive Chosen Ciphertext Attack для алгоритмів шифрування та EUF-CMA (Existentially unforgeable under adaptive chosen message attacks для алгоритмів електронного підпису.

У другому розділі дисертації *(Принципи використання розподілених технологій для забезпечення надійного надання електронних довірчих послуг)* показано, що децентралізовані системи здатні краще забезпечити функціонування електронних систем в умовах збільшення спектру електронних послуг та зростання кількості користувачів. Обґрунтовано, що для надійного функціонування децентралізованих систем, в тому числі у критичних інфраструктурах, можливе використання технології blockchain із децентралізованими протоколами консенсусу. Сформульовані рекомендації щодо використання децентралізованих протоколів консенсусу в залежності від типу та призначення цільової системи.

У третьому розділі дисертації *(Принципи побудови децентралізованої інфраструктури відкритих ключів)* розкриті основні недоліки існуючих інфраструктур відкритих ключів (ІВК), переважна більшість яких побудована за ієрархічним принципом із реалізацією відповідного ланцюга уповноважених органів (центрів сертифікації ключів). Базуючись на основі проведеного аналізу у розділі 2, у даному розділі наведена *удосконалена* модель децентралізованої інфраструктури відкритих ключів із використанням технології blockchain, яка відрізняється від існуючих тим, що дозволяє надійно реалізувати модель довіри, сконцентрованої навколо користувача, що дозволяє використовувати її для побудови системи електронного голосування. Описані переваги запропонованої децентралізованої системи, розроблені алгоритми для її функціонування, а саме: алгоритм первинної ідентифікації за умови генерації ключової пари в межах контрольованої зони довіреного вузла, алгоритм первинної ідентифікації за умови самостійної генерації ключової пари користувачем, алгоритм перевірки підпису, алгоритм оновлення статусу сертифіката та алгоритм оновлення сертифікату. Наведені результати часових оцінок для формування децентралізованої ІВК для двох топологій мереж.

В четвертому розділі дисертації *(Електронна система таємного голосування з використанням принципів розвитку децентралізованих технологій)* проаналізовані основні та додаткові вимоги до електронних систем

голосування, а також висвітлені загрози для систем такого типу. Обгрунтовано, що система електронного голосування охоплює процеси на чотирьох рівнях: правовий, організаційний, рівень процесів та технологічний. Наведена *удосконалена* модель системи електронного голосування, яка відрізняється від існуючих тим, що забезпечує формування деперсоналізованого списку виборців без використання сліпих підписів, що дозволяє спростити алгоритми взаємодії між сторонами. Запропонована дворівнева архітектура системи електронного голосування, яка дозволяє забезпечити процеси електронної ідентифікації за допомогою вже існуючих засобів, таких як BankID, MobileID, електронний підпис. Показано, що такий підхід дозволяє забезпечити інтероперабельність системи електронного голосування із розгорнутими в Україні системами електронної ідентифікації. Розроблені алгоритми та протоколи для децентралізованої системи електронного голосування, які впроваджені у комплексі для проведення досліджень криптографічних властивостей технології blockchain.

У п’ятому розділі дисертації *(Методи та механізми електронного підпису на геш-функціях для постквантового періоду)* наведені результати порівняльного аналізу алгоритмів квантово-захищенних електронних підписів (ЕП) на основі геш-функцій. Отримані експериментальні результати використання національного стандарту гешування ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування» в алгоритмі XMSS. Розкриті особливості одноразового механізму ЕП Lamport, особливості одноразового механізму ЕП Lamport-Diffie, а також ЕП Вінтерніц. Наведений удосконалений метод одноразових ключів Winternitz для постквантового періоду на основі геш-функцій, який відрізняється від існуючого модифікованими функціями зашифрування та перевірки, що дозволяє зменшити розміри особистого та відкритого ключів у 100 разів.

Ключові слова: постквантовий період, електронний підпис, децентралізована інфраструктура відкритих ключів, децентралізована система електронного голосування, технологія blockchain

ABSTRACT

Isirova K. V. **Models and Methods of Development of Decentralized Electronic Trust Services Based on Blockchain Technology and Post-Quantum Cryptography** – Qualification scholarly paper: a manuscript.

Thesis submitted for obtaining the Doctor of Philosophy degree in Information Technologies, Speciality 122 – Computer Science. – V. N. Karazin Kharkiv National University, Ministry of Education and Science of Ukraine, Kharkiv, 2021.

In modern conditions of electronic technologies rapid development, as well as a sharp increase in users of relevant systems, building trust in the online environment is one of the key issues to ensure society's social and economic development. The main goal of Ukraine is not only to introduce a full range of electronic trust services but also to ensure their interoperability and cross-border with international systems. On the other hand, advances in quantum computing have led to a significant increase in calculation speed. These formes new challenges for modern information security systems.

The dissertation is devoted to the actual problem solution: models and methods of ensuring the stability and resilience of electronic trust services in the post-quantum period development.

The purpose and objectives of the study. The dissertation’s purpose is to develop methods to ensure reliable and secure electronic trust systems operation through the use of blockchain technology and post-quantum cryptography.

To achieve this purpose the following tasks were solved:

1. Analysis of international requirements for cryptographic algorithms of the post-quantum period.
2. Analysis of the possibility of using decentralized technologies, in particular blockchain technology, to ensure the systems' resilience in the post-quantum period.
3. Development of the decentralized public key infrastructure model based on blockchain technology for the post-quantum period

4. Development of the decentralized electronic voting system model based on blockchain technology for the post-quantum period.

5. Analysis of methods of cryptographic transformations such as electronic signature, based on hash functions that can be used in the post-quantum period.

6. Development of the One-time keys method based on the Winternitz scheme for the post-quantum period.

The first section *(Electronic Trust Services in the Modern World)* shows that advances in quantum computing form new challenges for modern cryptography and force the necessity of the search for new ways to ensure information security. The main directions of new quantum-safe algorithms development are substantiated. It is demonstrated that today the main directions of new quantum-protected algorithms development are defined. They are code-based cryptography, hash-based cryptography, lattice-based cryptography, multivariate-based cryptography, as well as the use of isogenies of elliptic curves. It is showed that the systems' security can be ensured not only thanked to the cryptographic security of the primitives that underlie it, but also through the implementation of appropriate organizational, and technical solutions and methods. The concept of system resilience is formulated. As well, it is shown how it is related to the ability of the system to continue to function even in cyber attacks. The essence of post-quantum threat models, such as IND-CCA2 (Indistinguishability under Adaptive Chosen Ciphertext Attack for encryption algorithms and EUF-CMA (Existentially unforgivable under adaptive chosen message attacks for electronic signature algorithms), is revealed.

The second section of the dissertation *(Principles of Using Distributed Technologies to Ensure the Reliable Electronic Trust Services Provision)* shows that decentralized systems are able to better ensure the functioning of electronic systems in terms of increasing the range of electronic services and increasing the number of users. It is substantiated that for the reliable operation of decentralized systems, including in critical infrastructures, it is possible to use blockchain technology with decentralized consensus protocols. Recommendations for the use of decentralized consensus protocols depend on target system features are formulated.

The third section of the dissertation *(Principles of Building a Decentralized Public Key Infrastructure)* reveals the main shortcomings of existing public key infrastructures (PKI), the vast majority of which are built on a hierarchical principle with the implementation of the relevant chain of authorities (key certification centers). Based on the analysis performed in Section 2, this section provides an improved model of decentralized Public Key Infrastructure using blockchain technology, which differs from the existing ones in that it allows reliably implement a trust model around the user as well as be used for electronic voting systems development. The advantages of the proposed decentralized system are described, algorithms for its operation are developed, namely: primary identification algorithm for key pair generation within the controlled zone of the trusted node, primary identification algorithm for key pair generation by the user itself, signature verification algorithm, certificate status update algorithm, and certificate update algorithm. The results of time estimates for a decentralized PKI formation are presented for two topologies types.

In the fourth section of the dissertation *(Electronic Secret Voting System Using the Principles of Decentralized Technologies)* the basic and additional requirements to electronic voting systems are analyzed. Threats for systems of this type are named as well. It is substantiated that the electronic voting system covers processes at four levels: legal, organizational, process level, and technological. An improved model of the electronic voting system, which differs from the existing ones in that it forms a depersonalized voter list without using blind signatures, which simplifies interaction algorithms between users is presented in this section of the dissertation. A two-level architecture of the electronic voting system is proposed, which allows providing electronic identification processes by means that already exist, such as BankID, MobileID, electronic signature. It is shown that this approach allows ensuring the interoperability of the electronic voting system with the electronic identification systems deployed in Ukraine. Algorithms and protocols for the decentralized electronic voting system have been developed and implemented in the complex for research of blockchain technology cryptographic properties.

The fifth section of the dissertation *(Methods and Mechanisms of the Electronic Hash-based Signature for the Post-quantum Period)* presents the results of a comparative analysis of quantum-safe electronic signature (ES) algorithms based on hash functions. Experimental results of using the national hashing standard DSTU 7564: 2014 “Information technologies. Cryptographic information protection. Hashing function" in the XMSS algorithm are obtained. Features of the Lamport ES one-time mechanism, Lamport-Diffie ES one-time mechanism, and Winternitz one-time mechanism are described. An improved method of Winternitz one-time keys for the post-quantum period based on hash functions, which differs from the existing one by modified encryption and authentication functions, which allows reducing the size of private and public keys by 100 times is presented.

Keywords: post-quantum period, electronic signature, decentralized public key infrastructure, decentralized electronic voting system, blockchain technology.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукова публікація у періодичному науковому виданні держави, яка входить до Організації економічного співробітництва та розвитку, включеному до наукометричної бази Scopus

1. Gorbenko Yu. I., Isirova K. V. Improved Mechanism of One-Time Keys for Post-Quantum Period Based on the Hashing Functions // Telecommunications and Radio Engineering. 2018. Vol. 77, Is. 14. P. 1277–1296. DOI: 10.1615/TelecomRadEng.v77.i14.50 (Scopus, United States of America).
   URL: https://www.scopus.com/record/display.uri?eid=2-s2.0-85053395224&origin=resultslist
   (Особистий внесок здобувача: удосконалена математична модель постквантового електронного підпису POTS).

Наукові публікації у фахових виданнях України

2. Потій О. В., Ісірова К. В. Аналіз вимог та моделей безпеки для постквантової криптографії // Математичне та комп'ютерне моделювання. Серія: Технічні науки. 2017. Вип. 15. С. 192–197.
   DOI: https://doi.org/10.32626/2308-5916.2017-15
   URL: http://mcm-tech.kpnu.edu.ua/article/view/112043/106880
   (Особистий внесок здобувача: обґрунтування моделей безпеки для постквантової криптографії, модель безпеки IND-CCA2, модель безпеки EUF-CMA).
3. Исирова Е. В., Потий А. В., Семенец В. В. Принципы построения децентрализованной инфраструктуры открытых ключей // Радиотехника. 2018. Вып. 193. С. 82–93.
   URL: http://rt.nure.ua/article/view/175717
   (Особистий внесок здобувача: опис існуючої інфраструктури відкритих ключів, проблемні питання побудови, концепція побудови PKI на основі технології blockchain).

4. Ісірова К. В., Потій О. В. Децентралізовані протоколи консенсусу: можливості та рекомендації щодо використання // Радиотехника. 2018. Вып. 195. С. 203–208. DOI: https://doi.org/10.30837/rt.2018.4.195.20 URL: http://rt.nure.ua/article/view/175202 *(Особистий внесок здобувача: призначення протоколів консенсусу, порівняльний аналіз протоколів консенсусу)*.
5. Isirova K., Potii O., Claussen J. C. Establishing trust protocols in mutual distrust network by consensus formation // Радиотехника. Вып. 198. С. 96–104. DOI: https://doi.org/10.30837/rt.2019.3.198.07 URL: http://rt.nure.ua/article/view/184662 *(Особистий внесок здобувача: формування довіри у комп'ютерних мережах, принципи розробки децентралізованої PKI, протокол встановлення консенсусу в ієрархічній структурі, протокол встановлення консенсусу в децентралізованій структурі)*.
6. Ісірова К. В., Потій О. В. Принципи побудови електронної системи таємного голосування з використанням децентралізованих технологій // Радіотехніка. 2019. Вип. 199. С. 121–129. DOI: https://doi.org/10.30837/rt.2019.4.199.15 URL: http://rt.nure.ua/article/view/194028 *(Особистий внесок здобувача: принципи електронних систем голосування, система електронного голосування на основі децентралізованих принципів, принципи побудови децентралізованої системи електронного голосування)*.
7. Горбенко І. Д., Онопрієнко В. В., Горбенко Ю. І., Кузнецов О. О., Ісірова К. В., Родінко М. Ю. Проблеми, принципи побудови та перспективи розвитку національної системи електронного голосування в Україні // Радіотехніка. 2020. Вип. 200. С. 85–97. DOI: https://doi.org/10.30837/rt.2020.1.200.08 URL: http://rt.nure.ua/article/view/210067 *(Особистий внесок здобувача: обґрунтування вимог та умов застосування національної системи електронного голосування в Україні, обґрунтування структури та основних складових національної системи електронного голосування в Україні)*.

Публікації, які додатково відображають наукові результати дисертації

8. Isirova K. Blockchain Technology as the Prospective Instrument for Ensuring Electronic Trust Services in Conditions of Cyberthreats // European Cybersecurity Journal. 2018. Vol. 5. Is. 1. P 34-43
   URL: https://cybersecforum.eu/wp-content/uploads/2020/08/ECJ-VOLUME-5-2019-ISSUE-1.pdf
9. Горбенко Ю. І., Ісірова К. В. Удосконалений механізм одноразових ключів для постквантового періоду на основі геш-функцій // Радіотехніка. 2017. Вип. 191, С. 24–39.
   URL: https://nure.ua/wp-content/uploads/2017/Scientific_editions/191/5.pdf
   (Особистий внесок здобувача: постановка проблеми та можливості її вирішення, дослідження захищеності механізму POTS).
10. Gorbenko Yu., Isirova K. Improved mathematical model of the post-quantum eletronic signature mechanism // COMPUTER SCIENCE AND CYBERSECURITY. 2018. Is. 4(12). P. 22–28.
    URL: https://periodicals.karazin.ua/cscs/article/view/12249/11723
    (Особистий внесок здобувача: удосконалений механізм одноразових ключів для постквантового періоду POTS).

Наукові праці, які засвідчують апробацію матеріалів дисертації

11. Isirova K., Potii O. Requirements and Security Models for Post-Quantum Cryptography Analysis // ICTERI PhD Symposium : Proccedings of ICTERI PhD Symposium, 16–17 May 2017. Kyiv, 2017. P. 36–41. (SCOPUS).
    URL: http://ceur-ws.org/Vol-1851/paper-6.pdf
    (Особистий внесок здобувача: обґрунтування моделей безпеки для крипто алгоритмів у постквантовий період, модель безпеки для шифрування, модель безпеки для електронного підпису).
12. Isirova K., Potii O., Gorbenko Yu. Post Quantum Hash Based Digital Signatures Comparative Analysis. Features of their Implementation and Using in Public Key Infrastructure // Problems of infocommunications-science and technology

(PIC S&T): Proccedings of International scientific-practical conference, 10–13 October 2017. Kharkiv, 2017. P. 105–109. (SCOPUS).

(Особистий внесок здобувача: результати порівняння алгоритмів квантово-захищених цифрових підписів на основі геш-функцій).

13. Isirova K., Potii O. Decentralized public key infrastructure development principles // Dependable Systems, Services and Technologies (DESSERT) : Proccedings of International Conference, 24–27 May 2018. Kyiv, 2018. P. 305–310. (SCOPUS).

(Особистий внесок здобувача: принципи побудови децентралізованої інфраструктури відкритих ключів).

14. Isirova K., Potii O. Development Principles for Electronic Voting System Using Distributed Ledger Technology // Dependable Systems, Services and Technologies (DESSERT) : Proccedings of International Conference on Dependable Systems, Services and Technologies (DESSERT), 14–18 May 2020. Kyiv, 2020.
P. 446–450. (SCOPUS).

(Особистий внесок здобувача: принципи побудови децентралізованої системи електронного голосування).

15. Isirova K., Kiian A., Rodinko M., Kuznetsov A. Decentralized electronic voting system based on blockchain technology developing principals // Computer Modeling and Intelligent Systems (CMIS) : Proccedings International Workshop,
27 April – 1 May 2020. Zaporizhzhia, 2020. P. 211–223. (SCOPUS).

(Особистий внесок здобувача: архітектура децентралізованої системи електронного голосування, протокол голосування у децентралізованій системі електронного голосування).

16. Горбенко Ю. І., Ісірова К. В. Сценарії створення та перевірки вдосконалених електронних підписів в мобільному середовищі // Теоретичні та прикладні аспекти побудови програмних систем : Збірник матеріалів XI Міжнародної науково-практичної конференції, 15–17 грудня 2014 р. Київ, 2014. С. 75.

(Особистий внесок здобувача: сценарії створення та перевірки вдосконалених електронних підписів в мобільному середовищі).

17. Ісірова К. В. Бизнес модель информационной безопасности // Інформаційна безпека України : Збірник матеріалів науково-технічної конференції, 12–13 березня 2015 р. Київ, 2015. С. 109.
18. Ісірова К. В. Застосування електронних підписів для забезпечення кібернетичної безпеки // Проблеми кібербезпеки інформаційно-телекомунікаційних систем : Збірник матеріалів Науково-практичної конференції, 10–11 березня 2016 р. Київ, 2016. С. 42.
19. Потій О. В., Горбенко І. Д., Ісірова К. В. Міжнародні вимоги до криптоалгоритмів у постквантовий період // Теоретичні та прикладні аспекти побудови програмних систем : Збірник матеріалів XII Міжнародної науково-практичної конференції, 5–9 грудня 2016 р. Київ, 2016. С. 215.
(Особистий внесок здобувача: аналіз міжнародних вимог до криптоалгоритмів у постквантовий період).
20. Потій О. В., Ісірова К. В. Аналіз вимог та моделей безпеки для постквантової криптографії // Проблеми кібербезпеки інформаційно-телекомунікаційних систем : Збірник матеріалів II Науково-практичної конференції, 23–24 березня 2017 р. Київ, 2017. С. 163.
(Особистий внесок здобувача: аналіз моделей безпеки для постквантової криптографії).
21. Потій О. В., Ісірова К. В., Карпенко А. С. Особливості реалізації квантово-захищених цифрових підписів на основі геш-функцій // Безпека інформації в інформаційно-телекомунікаційних системах : Збірник матеріалів XIX міжнародної науково-практичної конференції, 25–26 травня 2017 р. Київ, 2017. С. 84–85.
(Особистий внесок здобувача: порівняльний аналіз алгоритмів квантово-захищенних цифрових підписів на основі геш-функцій та особливості їхньої реалізації).
22. Ісірова К. В., Потій О. В. Принципи побудови децентралізованої інфраструктури відкритих ключів // Безпека інформації в інформаційно-

телекомунікаційних системах : Збірник матеріалів XX міжнародної науково-практичної конференції, 22 травня 2018 р. Київ, 2018. С. 110–112. *(Особистий внесок здобувача: принципи побудови інфраструктури відкритих ключів із використання технології blockchain).*

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

БД	–	база даних
ІВК	–	інфраструктура відкритих ключів
PKI	–	Public Key Infrastructure
CA	–	Certification Authority
CRL	–	Certificate Revocation Lists
ЕП	–	Електронний підпис

ВСТУП

Обґрунтування вибору теми дослідження.

Суспільство активно впроваджує електронні технології в своє життя більше 20 років. В Європейському Союзі відповідна Директива [1] була прийнята у 1999 році. В 2012 році перший Регламент [2] був запропонований, а в 2014 році він був вдосконалений та прийнятий Регламентом (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та скасування Директиви 1999/93/ЄС [3]. Головним елементом підтвердження автентичності в системах електронних довірчих послуг виступає цифровий, а в термінології Регламенту-2014, електронний підпис.

В умовах набрання популярності електронних довірчих послуг, а також зважаючи на переваги, які вони надають кінцевим користувачам, побудова довіри в он-лайн середовищі – це ключ до економічного та соціального розвитку суспільства. Оскільки відсутність довіри змушує стейкхолдерів вагатися при здійсненні транзакцій електронно або при впровадженні нових сервісів [35]. Окрім того, необхідно звертати увагу не лише на побудову довіри між користувачами, але і на забезпечення довіри до самої технології. Основною метою України є не тільки впровадження повного спектру електронних довірчих послуг (сервісів), а також забезпечення їхньої інтероперабельності та транскордоності. Виходячи з цієї перспективи важливо забезпечити правову, функціональну та технологічну інтероперабельність українських систем із європейськими. Більше того, важливо зазначити, що вирішення цих завдань та забезпечення надійного функціонування систем електронних довірчих послуг систем виступає однією із ключових вимог для забезпечення кібернетичної безпеки держави. Оскільки системи електронних довірчих послуг, а зокрема система електронної ідентифікації та інфраструктура відкритих ключів входять до переліку критичних інфраструктур країни.

Стрімкий розвиток квантових технологій, а разом з ними і квантових обчислень формують нові виклики для сучасних систем безпеки інформації. А

відповідно і тих систем, які забезпечують надійне та безпечне функціонування критичних систем. Традиційні методи забезпечення безпеки, які сьогодні реалізовані в таких системах будуть не спроможні забезпечувати достатній рівень безпеки та враховувати «загрози нульового дня» найближчим часом. Класично, безпека системи оцінюється за показнимаки стійкості криптографічних примітивів, які покладені в її основу. Найпоширенішими криптопримітивами виступають шифрування та електронний підпис. На національному рівні прийнятий держаний стандарт симетричного шифрування ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення», який вважається стійким до атак із використанням квантових комп'ютерів. Проте, питання щодо стійкості діючого національного стандарту електронного підпису ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка» є відкритим, оскільки без додаткового збільшення параметрів за умови використання криптоаналітиком квантового комп'ютера, стійкість знижується до поліноміальної. На світовому просторі питання переходу на нові постквантові крипто перетворення також активно досліджується та готуються відповідні пропозиції.

Таким чином, можна зробити висновок, що сучасні потреби та стан розвитку електронного цифрового світу, надання електронних довірчих послуг та у цілому обробки інформації у інформаційно-телекомунікаційних системах різного призначення потребують розробки нових методів забезпечення стійкості та резильєнтності відповідних систем. Під резильєнтністю системи розуміється здатність системи буди надійною не лише за рахунок використання надійних (стійких) криптопримітивів, а також за рахунок розгорнутих архітектурних рішень, наприклад перехід на децентралізовані системи, та вроваджених нових технологій, таких як технологія blockchain.

Зв'язок роботи з науковими програмами, планами, темами.

Дослідження, результати яких знайшли відображення в дисертаційній роботі, виконані на кафедрі безпеки інформаційних систем і технологій Харківського національного університету імені В. Н. Каразіна. Напрям дисертаційних досліджень тісно пов'язаний з роботами, виконаними у рамках науково-дослідної роботи № 1-41-18 «Аналіз, дослідження, розробка та стандартизація криптографічних систем для захисту інформації в постквантовому середовищі, в умовах інформаційних і гібридних війн» (№ ДР 0118U002024) (акт від 10.09.2020 р.). Результати дисертаційних досліджень були використані при підготовці та читанні лекцій за темами 3-розділу «Питання безпеки децентралізованих систем» по дисципліні «Технології блокчейн» для спеціальності «Кібербезпека» (акт від 10.09.2020 р.).

Мета і завдання дослідження.

Мета дослідження: розробка методів забезпечення надійної і безпечної роботи систем електронних довірчих за рахунок використання технології blockchain та постквантової криптографії.

Для досягнення поставленої мети були розв'язані такі задачі:

- аналіз міжнародних вимог до криптоалгоритмів постквантового періоду;
- аналіз можливості використання децентралізованих технологій, зокрема технології blockchain, для забезпечення резильєнтності систем у постквантовий період;
- розробка моделі децентралізованої інфраструктури відкритих ключів на основі технології blockchain для використання у постквантовий період;
- розробка моделі децентралізованої системи електронного голосування на основі технології blockchain для використання у постквантовий період;
- аналіз методів криптографічних перетворень типу електронний підпис, на основі геш-функцій, що можуть бути застосованими у постквантовий період;
- розробка методу одноразових ключів на основі схеми Winternitz для постквантового періоду.

Об'єкт дослідження: процеси надання електронних довірчих послуг.

Предмет дослідження: вимоги безпеки, моделі та методи надання децентралізованих електронних довірчих послуг.

Методи дослідження: методи системного аналізу та прийняття рішень, методи прикладної криптографії, зокрема методи теорії чисел, теорії груп, полів, кілець, методи структурного та математичного моделювання.

Наукова новизна отриманих результатів.

Удосконалена модель децентралізованої інфраструктури відкритих ключів на основі технології blockchain, яка відрізняється від існуючих тим, що дозволяє надійно реалізувати модель довіри, сконцентрованої навколо користувача, що дозволяє використовувати її для побудови системи електронного голосування.

Удосконалена модель системи електронного голосування, яка відрізняється від існуючих тим, що забезпечує формування деперсоналізованого списку виборців без використання сліпих підписів, що дозволяє спростити алгоритми взаємодії між сторонами.

Удосконалений метод одноразових ключів Winternitz для постквантового періоду на основі геш-функцій, який відрізняється від існуючого модифікованими функціями зашифрування та перевірки, що дозволяє зменшити розміри особистого та відкритого ключів у 100 разів.

Практичне значення отриманих результатів.

Розроблене програмне забезпечення для проведення симуляцій для визначення часу формування децентралізованої інфраструктури відкритих ключів для різних топологій мереж.

Розроблені алгоритми та протоколи для децентралізованої системи електронного голосування впроваджені у комплексі для проведення досліджень криптографічних властивостей технології blockchain.

Отримані експериментальні результати використання національного стандарту гешування ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування» в алгоритмі XMSS.

Результати дисертаційних досліджень впровадженні у Приватному акціонерному товаристві «Інститут інформаційних технологій», м. Харків (акт від 11.09.2020 р.).

Особистий внесок здобувача.

У наукових статтях, опублікованих у співавторстві, автору належать наступні результати:

- удосконалена математична модель постквантового електронного підпису POTS [62, 63];
- дослідження захищеності механізму POTS [64];
- обґрунтування моделей безпеки для постквантові криптографії, модель безпеки IND-CCA2, модель безпеки EUF-CMA [10];
- опис існуючої інфраструктури відкритих ключів, проблемні питання побудови, концепція побудови PKI на основі технології blockchain [33];
- призначення протоколів консенсусу, порівняльний аналіз протоколів консенсусу [20];
- формування довіри у комп'ютерних мережах, принципи розробки децентралізованої PKI, протокол встановлення консенсусу в ієрархічній структурі, протокол встановлення консенсусу у децентралізованій структурі [34];
- принципи електронних систем голосування, система електронного голосування на основі децентралізованих принципів [50];
- обґрунтування вимог та умов застосування національної системи електронного голосування в Україні, обґрунтування структури та основних складових національної системи електронного голосування в Україні [51].

Апробація результатів дисертації здійснювалася на XI Міжнародній науково-практичній конференції «Теоретичні та прикладні аспекти побудови програмних систем» 15-17 грудня 2014 року, м. Київ; на Науково-технічній конференції «Інформаційна безпека України» 12-13 березня 2015 року, м. Київ; на Науково-практичній конференції «Проблеми кібербезпеки інформаційно-

телекомунікаційних систем», 10-11 березня 2016 року, м. Київ; на XII Міжнародній науково-практичній конференції «Теоретичні та прикладні аспекти побудови програмних систем», 5-9 грудня 2016 року, м. Київ; на II Науково-практичній конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем», 23-24 березня 2017 року, м. Київ; на ICTERI PhD Symposium 16-17 травня 2017 року, м. Київ; на XIX Міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах», 25-26 травня 2017 року, м. Київ; на 4th International scientific-practical conference problems of infocommunications-science and technology (PIC S&T) 10-13 жовтня 2017 року, м. Харків; на XX Міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах», 22 травня 2018 року, м. Київ; на IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT) 24-27 травня 2018 року, м. Київ; на 4th European Cybersecurity Forum CYBERSEC, 8-9 жовтня 2018 року, м. Краков; на Third International Workshop on Computer Modeling and Intelligent Systems (CMIS) 27 квітня-1травня 2020 року, м. Запоріжжя; на IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT) 14-18 травня 2020 року, м. Київ.

Публікації. Основні наукові результати за темою дисертації опубліковані у 10 статтях, із яких 6 статей у фахових наукових журналах, які входять до переліку МОН України, та 1 стаття в науковому зарубіжному виданні, включеному до наукометричної бази Scopus.

Структура та обсяг дисертації. Дисертація містить вступ, п’ять розділів, висновки, п’ять додатків, список використаних джерел. Загальний обсяг дисертації складає 165 сторінки, у тому числі 4 таблиці на окремих сторінках, 13 сторінок додатків, 10 сторінок списку використаних джерел в кількості 83 найменувань.

РОЗДІЛ 1

ЕЛЕКТРОННІ ДОВІРЧІ ПОСЛУГИ У СУЧАСНОМУ СВІТІ

1.1 Аналіз нових виклики, які мають бути враховані при наданні електронних довірчих послуг

Успіхи в сфері квантових обчислень такі як, квантовий ефект Холла, а також розвиток концепції побудування квантової системи на квантових точках, разом із розвитком оптоволоконних технологій є важливим викликом сучасній криптографії. Швидка еволюція квантових комп'ютерів, а як наслідок зростання швидкості обчислень обумовлюють нові ризики для існуючих криптографічних систем. Зокрема алгоритми Шора та Гровера становлять реальну загрозу для асиметричних систем, побудованих на основі RSA, Diffie-Hellman, Elliptic Curves [5-7].

В найближчий час довіра до інформаційних систем, які обробляють критичну інформацію, без засобів квантово-захищеної криптографії буде неможлива [11].

Раніше, зв'язок та транзакції розглядалися як надійні у тому випадку, коли використовувалися стійкі криптосистеми, але завдяки новим досягненням складність криптоаналізу стійких сьогодні систем знизиться до поліноміальної. Можна припустити, що з'являться сучасні інструменти криптоаналізу асиметричних систем RSA та ECC. В такому випадку, все що було стійким до цього часу, можна буде вважати незахищеним [10].

Необхідно враховувати не лише те, як швидко з'явиться програмована модель квантового комп'ютера, а і те, який проміжок часу інформація має бути конфіденційна, а також скільки часу необхідно на оновлення існуючої інфраструктури. Відповідь на питання «Коли нам потрібно хвилюватися відносно прийняття рішення щодо переходу на нові квантово-захищені алгоритми?» дає теорема Mosco [4, 6] (рисунок 1.1), яка формулюється у наступному вигляді.

Перед нами стоять три питання:

1) Наскільки довго ми маємо вважати шифрування безпечним (або як довго нам потрібно зберігати у таємниці інформацію) –*X років.*

2) Скільки часу нам необхідно витратити на те, щоб критична інформаційна інфраструктура була квантово-захищена – параметр *Y років*.

3) Коли будуть побудовані large-scale квантові комп'ютери – *Z років*.

Тоді, якщо *X*+*Y* > *Z*, нам потрібно хвилюватися.

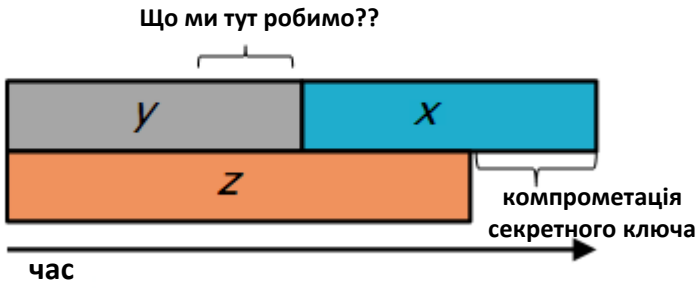


Рис. 1.1. Теорема Mosco [4]

Якщо квантовий комп'ютер буде побудований (Z) до того, як існуюча інфраструктура стане стійкою до квантового криптоаналізу, а необхідний час забезпечення таємниці ще не минув (X+Y), тоді дані будуть незахищені.

Квантово-захищені алгоритми мають бути стандартизовані органами стандартизації. По-перше, міжнародними та національними органами зі стандартизації - ASC X9, IEEE 1363, ISO/IEC JTC 1/SC 27/WG 2, ETSI SAGE. По-друге, органами промислової стандартизації SEC, PKCS, CEES, IETF тощо. Стандартизація квантово-захищених крипто примітивів забезпечить відповідний рівень довіри до нових алгоритмів з боку споживачів, а також відповідний рівень відкритості розробки алгоритмів. По-третє, квантово-захищені крипто примітиви мають бути базовими елементами стандартних протоколів - TLS, IPSec, S/MIME, OpenPGP тощо.

Квантово-захищені крипто примітиви мають підлягати сертифікації на відповідність стандартів FIPS 140-X, NIST Special Publications та Common Criteria (ISO/IEC 15408) [12].

Для прийняття ґрунтовних рішень, необхідне визнання проблеми. По-перше, необхідно визнати, що квантово-захищена криптографія вже існує. Це необхідно визнати як на національному рівні так і на світовому. Провідні держави світу вже декілька років активно працюють в цьому напрямі. В США, ЄС та Японії проходять спеціалізовані конференції та семінари. В 2015 році NSA офіційно визнала факт цієї проблеми. По-друге, всебічне вивчення нової задачі академічною спільноти виступатиме потужним драйвером для вирішення цієї проблеми. На рисунку 1.2 наведені результати контент-аналізу публікацій із ресурсу IACR.

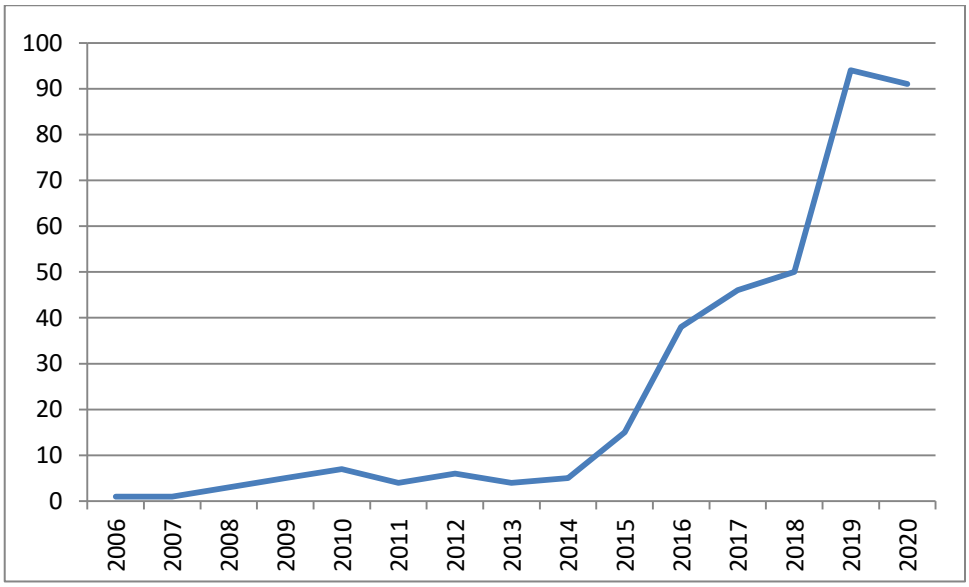


Рис. 1.2. Результати контент-аналізу публікацій із ресурсу IACR

Як ми бачимо, з 2009 року кількість статей у галузі постквантової криптографії різко та невпинно зростає, що свідчить про ріст зацікавленості в даних питаннях серед провідних науковців світу [10, 13].

Важливо розуміти, що безпека систем може забезпечуватися не лише за допомогою використання стійких алгоритмів, а також за допомогою організаційних, організаційно-технічних рішень та методів. В першому випадку

мова йде про стійкість систем, коли вся безпека залежить виключно від складності криптоаналізу алгоритмів, які покладені в її основу. Проте можуть виникати ситуації, коли використання, наприклад ключів більшої довжини або використання більш стійкого алгоритму шифрування чи електронного підпису, може призводити до значного ускладнення протоколів взаємодії між користувачами або взагалі вносити надмірність в розгорнуту систему захисту. В такому випадку виходом може бути не підвищення стійкості криптоалгоритмів, а забезпечення безпеки інформації, яка обробляється в системі, не лише криптографічними методами, а також шляхом використання додаткових технологій або модифікованих архітектурних рішень. В такому випадку вести мову виключно про стійкість системи недоречно.

Далі під резильєнтністю системи будемо розуміти здатність системи бути надійною не лише за рахунок використання надійних (стійких) криптопримітивів, а також за рахунок розгорнутих архітектурних рішень та впроваджених нових технологій. Прикладом архітектурного рішення може бути перехід на децентралізовані системи, оскільки вони позбавлені головного недоліку класичних централізованих систем, а саме: в них відсутня головна вразлива точка (або точки) збою, на яку зазвичай направлені зловмисні атаки. У випадку дійсно децентралізованої системи порушник змушений атакувати всю мережу (систему) або принаймні більшу її частину, оскільки вихід з ладу одного або навіть декількох вузлів не призведе до порушення роботи решти системи. Можливість системи продовжувати функціонувати в умовах кібератак, а також швидко відновлювати роботу після виступає ще однією характеристикою резильєнтності, яка не може бути забезпечена виключно за рахунок параметрів стійкості криптопримітивів. Прикладом технології, яка може забезпечити надійне функціонування децентралізованих систем виступає технологія blockchain. На додаток, вона здатна забезпечувати довіру між користувачами системи в умовах взаємної недовіри без залучення сторонніх гарантів, тим самим значно зменшуючи ймовірність загрози підкупу або зловмисної змови між можливими внутрішніми порушниками.

1.2 Аналіз міжнародних вимог до криптоалгоритмів постквантового періоду

На шляху побудови нових рішень важливим етапом є розробка та формування вимог та характеристик, що мають бути пред'явлені до нових кандидатів та можливих умов їхнього застосування. Наразі міжнародна наукова спільнота активно обговорює вимоги, яким мають відповідати криптографічні примітиви для того, щоб вони були придатними для застосування у постквантовий період. Найпотужніші організації зі стандартизації: NIST та ETSI розгорнули активні роботу в цьому напрямку [5, 6]. NIST оголосив відкритий конкурс Post-Quantum Crypto Project [5], в рамках якого планується відібрати алгоритми направленого шифрування та електронного підпису, які після досліджень та випробувань можуть бути стандартизовані на міжнародному рівні. Європейська організація ETSI випустила технічний звіт ETSI GR QSC 001 V.1.1.1 (2016-07) [6]. Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework, який охоплює вимоги та критерії відбору серед можливих кандидатів на постквантові алгоритми.

1.2.1 Аналіз вимог NIST до постквантових алгоритмів

Проведений аналіз [5, 7] показав, що NIST розуміє необхідність пошуку нових примітивів, які будуть актуальні у постквантовий період. За планами NIST у 2016 році розпочалася підготовка до проведення конкурсу на нові постквантові криптографічні стандарти. Був підготовлений проект вимог до кандидатів. До осені 2017 року приймалися пропозиції та алгоритми кандидатів. Ці роботі здійснюються у рамках відкритого конкурсу Post-Quantum crypto Project [5]. У таблиці 1.1 наведені основні вимоги до кандидатів. Всі вимоги можна поділити на такі групи [12-13]:

- вимоги з безпеки;
- техніко-економічні вимоги;
- техніко-експлуатаційні вимоги.

Таблиця 1.1

Основні вимоги NIST до кандидатів

Вимога	Специфікація
Вимоги з безпеки	
Використання криптографії з відкритим ключем	Заміна стандарту електронного підпису FIPS 186 Заміна стандартів розподілу ключів SP 800-56A, SP 800-56B Використання нового стандарту в протоколах: TLS, SSH, IPsec, DNSSEC
Модель безпеки для шифрування та розподілу ключів	Схема «семантично безпечного шифрування». Модель безпеки - IND-CCA2. Умови безпеки: доступ зловмисника менше ніж до 2^{64} обраних шифротекстів.
Модель безпеки для електронного підпису	Модель безпеки EUF-CMA. Умови безпеки: доступ зловмисника менше ніж до 2^{64} обраних повідомлень.
Вимоги до стійкості	1) 128 біт класичної безпеки / 64 біт квантової захищеності (запас стійкості AES-128) 2) 128 біт класичної безпеки / 80 біт квантової захищеності (запас стійкості SHA-256/ SHA3-256) 3) 192 біт класичної безпеки / 96 біт квантової захищеності (запас стійкості AES-192) 4) 192 біт класичної безпеки / 128 біт квантової захищеності (запас стійкості SHA-384/ SHA3-384) 5) 256 біт класичної безпеки / 128 біт квантової захищеності (запас стійкості AES-256)
Додаткові властивості безпеки	«Perfect forward secrecy». (удосконалена випереджаюча безпека). Стійкість до атак сторонніми каналами. Стійкість до мультиключових атак. Стійкість до відмов.
Інші вимоги	Прозорі математичні рішення. Обґрунтованість стійкості
Техніко-економічні вимоги	
Вимога	Сутність вимоги
Розміри (довжини) відкритого ключа, шифротексту, підпису	Орієнтація на розмір пакетів інтернет-протоколів. Гешування ключової інформації. Для «perfect forward secrecy» використання менших довжин ключа.
Обчислювальна ефективність операцій відкритого (шифрування перевірки підпису) та особистого ключів (дешифрування, підписання)	Забезпечення ефективності як апаратної, так і програмної реалізації.
Обчислювальна ефективність процесу генерації ключів	Відповідність розмірів ключа до обраної системи.
Помилки шифрування	Низький відсоток помилок шифрування. Багаторазове шифрування.
Техніко-експлуатаційні вимоги	
Гнучкість	Додаткові можливості схеми (оптимізація, неявний обмін ключами тощо). Кросплатформеність. Можливість розпаралелювання.
Простота	Зрозумілість побудови.

У таблиці 1.2 Наведені критерії відбору серед запропонованих кандидатів. Оцінювання проводиться в два етапи. Визначена основна платформа для тестування, але за необхідності також можуть проводитися додаткові тестування за інших умов [5].

Таблиця 1.2

Критерії відбору серед запропонованих кандидатів

Критерій	Пояснення
Технічна оцінка	
Перевірка на коректність	Перевірка правильності опорних та оптимізованих реалізацій.
Перевірка на ефективність	Обчислення часу, необхідного для генерації ключа, шифрування, дешифрування, електронного підпису, перевірки підпису, або встановлення ключів, а також розмір ключів, зашифрованого тексту і підпису. (Тестування проводиться на оптимізованих версіях).
Інші перевірки	Додаткові випробування.
Умови випробувань	Основна платформа: NIST PQC Reference Platform, Intel x64, Windows or Linux, the GCC compiler. Також можуть проводитися додаткові тестування за інших умов (8-бітових процесорів, цифрових сигнальних процесорів, виділених CMOS, тощо)

1.2.2 Аналіз вимог ETSI до постквантових алгоритмів

Проведений аналіз [14-17] показав, що Європейський союз також розпочав активну роботу з підготовки нових постквантових стандартів. Європейською організацією зі стандартизації ETSI у кластері «Безпека» сформований новий напрямок «Квантово-захищена криптографія» («Quantum-Safe Cryptography»). Група спеціалістів активно веде дослідження в таких напрямках [6, 9]:

- оцінка загроз квантовій безпеці;
- приклади та сценарії реалізації квантово-захищених примітивів;
- фундаментальні межі квантових обчислень стосовно криптографії;
- квантово-безпечний алгоритм обміну ключами;
- квантово-захищений електронний підпис.

За результатами даних досліджень прогнозується прийняття групи стандартів для постквантового періоду. Вже зараз готові попередні версії кожного із проектів.

ETSI опублікувала груповий звіт «Квантово-захищена криптографія.

Квантово-безпечна інфраструктура» [6], в якому закріплені основи перспективної інфраструктури, представлені механізми, описані типи примітивів, що будуть використовуватися. Окремо висунуті вимоги та сформовані критерії оцінки майбутніх кандидатів.

За результатами досліджень були визначені п’ять сімейств примітивів (Табл. 1.3).

Таблиця 1.3

Сімейства примітивів для постквантового періоду, визначених за результатами ETSI

Сімейство	Математична задача, від вирішення якої залежить безпека
Lattice-based primitives	Безпека залежить від складності розв’язання рівняння на решітках
Multivariate primitives	Безпека залежить від складності рішення системи багатовимірних поліноміальних рівнянь
Code-based primitives	Безпека залежить від складності виконання завдання декодування лінійного коду
Hash-based primitives	Безпека залежить від складності знаходження колізій або прообразів в криптографічних геш-функцій
Isogeny-based key primitives	Безпека залежить від складності знаходження невідомого ізогена між парою суперсінгулярних еліптичних кривих

Проведений аналіз показав, можливі класифікації примітивів розподілу ключів та автентифікації в кожному із сімейств (Табл. 1.4).

ETSI в [7] також розробила вимоги для кандидатів та планує об’явити Європейський конкурс на нові постквантові алгоритми.

До основних вимог з безпеки відносяться наступні [7, 13]:

— проходження громадського контролю та визнання науковим співтовариством;
— надійне підтвердження стійкості;
— актуальність моделі безпеки;
— висока складність можливих атак;
— можливість використання в безпечному протоколі розподілу ключів;
— можливість поєднання кількох функцій безпеки (наприклад,

встановлення ключів і схеми автентифікації);

— зручність кількісної оцінки заявлених класичних і квантових рівнів безпеки;

— визначеність рекомендованих ключових розмірів для заданого рівня безпеки (наприклад, 80-біт, 112 біт, 128 біт або 256 біт).

Таблиця 1.4

Класифікація постквантових примітивів

Тип примітиву	Пояснення
Примітиви узгодження ключів (key agreement primitives)	Дві сторони надійно генерують загальний симетричний ключ від інформації, що вноситься обома сторонами; наприклад, шляхом обміну відкритими ключами один з одним
Примітиви транспортування ключів (key transport primitives)	Одна зі сторін генерує симетричний ключ і надійно розділяє його з іншою стороною; наприклад, шляхом відправки його зашифровану копію на відкритому ключі іншої стороні
Схеми підпису типу Fiat-Shamir (Fiat-Shamir signature schemes)	Будуються на базі інтерактивних протоколів доказів правильності знань
Схеми підпису на основі геш-функцій (hash-and-sign signature schemes)	Будуються на основі використання односторонніх геш-функцій

Були визначні п’ять видів вимог для безпеки (таблиця 1.5), які мають бути математично доведені при впровадженні примітивів для постквантового періоду.

У таблиці 1.6 наведені додаткові вимоги ETSI для оцінювання кандидатів постквантових примітивів [13].

Таблиця 1.5

Види вимог безпеки ETSI для оцінювання кандидатів постквантових примітивів

Вид безпеки	Пояснення
Класична безпека	Стійкість проти класичних атак.
Квантова безпека	Стійкість проти «квантових» атак. Зокрема, стійкість до алгоритму Гровера (подвоєння розміру ключа).
Доказова безпека	Базування на задачах, які мають високу складність обчислення. Можливе ігнорування зниження рівня складності, за умови, що практична стійкість не зміниться.
Довгострокова безпека	Можливість використання у протоколах типу TLS 1.3 з підтримкою forward secure cipher suites.
Активна безпека	Стійкість проти атак з адаптивним підбором.

Таблиця 1.6

Додаткові вимоги ETSI для оцінювання кандидатів постквантових примітивів

Вимога	Пояснення
Ефективність	Використання рекомендованих параметрів розмірів для заданого рівня безпеки. Незалежність швидкодії та кількості раундів перетворень від платформи реалізації. Швидкість генерації ключів і часу, необхідного для поширення нового ключа. Інші практичні вимоги (наприклад, стійкість до відмов).
Реалізація та розгортання	Простота впровадження не фахівцями. Відносно малий обсяг (у сенсі ресурсу) реалізації (зокрема, можливість реалізації на FPGA та вбудований пристроях). Відносно малий об’єм необхідної пам'яті під час виконання (можливість реалізації на пристрої з обмеженими ресурсами). Практичність розмірів ключа і підпису для передачі або зберігання в ряді платформ, включаючи пристрої з обмеженими ресурсами. Простота інтеграції в існуючі протоколи або системи. Низька вартість заміни або модернізації. Повторне використання базового коду (наприклад, для забезпечення автентифікації, а також розподілу ключів). Сумісність (наприклад, гнучкість у виборі геш-функції в схемах дерева Меркле).

1.2.3 Загальна характеристика нових напрямків розробки криптографічних примітивів. Обґрунтування моделей безпеки для постквантової криптографії.

Проведений аналіз [16,17] показав, що вимоги до стійкості мають бути сформульовані у відповідності до таких моделей загроз:

– для шифрування – в умовах моделі IND-CCA2 (Indistinguishability under Adaptive Chosen Ciphertext Attack) – стійкість до адаптивної атаки на основі обраного шифротексту [17];

– для електронного підпису – в умовах моделі EUF-CMA (Existentially unforgeable under adaptive chosen message attacks), тобто забезпечення захисту від екзістенціональної підробки в умовах адаптивного вибору повідомлення [69].

Обґрунтування стійкості криптографічних примітивів має базуватися на складних обчислювальних задачах для квантових комп'ютерів.

Сьогодні вже виявлені можливі прикладні області, де можуть бути отримані ґрунтовні рішення у новій сфері криптографії – квантово-безпечних (quantum-safe) або квантово-захищених (quantum-resistance) алгоритмів, особливо у сфері електронного підпису та асиметричного шифрування.

До таких областей відносяться такі [11-13, 77]:

Hash-based cryptography (HB-криптографія). Класичний приклад HB-криптографії є геш-дерево Мерклі (Merkle) для системи підпису (1979), що побудовано на ідеї Lamport та Diffie про підпис одного повідомлення (n a one-message-signature).

Code-based cryptography (CB-криптографія). Класичним прикладом є схема асиметричного шифрування McEliece з кодами Goppa (1978).

Lattice-based cryptography (LB-криптографія). Найбільший інтерес у цьому класі являє схема асиметричного шифрування Hoffstein–Pipher–Silverman "NTRU" (1998).

Multivariate-quadratic-equations cryptography (MQE-криптографія) однією з перспективних схем електронного підпису у цьому класі є схема Patarin

“HFEv−цифровий підпис” (1996), що є узагальненням запропонованого Matsumoto та Imai підходу.

1.2.4 Модель безпеки IND-CCA2

Для алгоритму асиметричного шифрування стійкість до атаки на основі обраного шифротексту/до адаптивної атаки на основі обраного шифротексту (IND-CCA1/ IND-CCA2) визначається «грою» між претендентом (легітимним користувачем) та противником (криптоаналітиком). Необхідно ввести наступне визначення: $E(PK, M)$ – шифрування повідомлення M ключем PK. Умова: противник моделюється поліноміальним часом машини Тюрінга. Він має доступ до відкритого ключа (оракула за шифрування у симетричному випадку), а також до оракула розшифрування, який розшифровує довільні шифротексти на вимогу противника, повертаючи відкритий текст [69].

«Гра» складається з таких кроків:

1. Претендент генерує ключову пару *PK*, *SK*, що базується на параметрі безпеки *k* (наприклад, розмір ключа у бітах), та видає *PK* противнику. Претендент зберігає *SK*.

2. Противник може виконувати будь-яке число зашифрувань, викликати оракула розшифрування, що заснований на довільних шифротекстах або інших операціях.

3. Зрештою, противник представляє два різні обрані відкриті тексти M_0, M_1 претенденту.

4. Претендент обирає біт $b \in \{0, 1\}$ рівномірно у випадковому порядку та відправляє «виклик» шифротексту C=E(PK, M_b) назад противнику.

5. Противник може вільно виконувати будь-яку кількість додаткових обчислень або зашифрувань.

a) У *неадаптивному* випадку (IND-CCA1) порушник може *не* виконувати подальших викликів оракула розшифрування.

b) У *адаптивному* випадку (IND-CCA2) порушник може виконувати подальші виклики оракула розшифрування, але може не відправляти виклик шифротексту *C*.

6. Нарешті, противник виводить припущення для значення b.

Схема є IND-CCA1/IND-CCA2 безпечною, якщо жоден противник не має жодної, хоча б малої, переваги для перемоги у грі [10, 11].

1.2.5 Модель безпеки EUF-CMA

Поняття (або рівень) безпеки повністю визначається співвідношенням між метою (ціллю) порушника та моделлю порушника. В залежності від контексту, в якому використовується дана схема підпису (або криптосистема), можна формально визначити поняття безпеки системи, задавши цілі порушника, які він намагатиметься досягти та методи / засоби, які йому доступні (модель порушника) [60].

Вводяться позначення можливих цілей порушника [10].

UB (Стійкість) - зловмисник відновлює секретний ключ ***sk*** з відкритого ключа ***pk*** (або еквівалентного ключа, якщо такий існує). Вона неявно з'явилася з виникненням схем підпису з відкритим ключем (криптографії з відкритим ключем).

UUF (Універсальна нерозрізнювальність) - Зловмисник може згенерувати дійсний підпис ***S*** будь-якого повідомлення ***M*** без розкриття секретного ключа ***sk.***

EUF (Екзистенційна нерозрізнюваність) - Зловмисник створює повідомлення ***M*** і його дійсний підпис ***S*** (хоча не має ніякого контролю над повідомленням).

Моделі порушника можуть бути наступні [10, 11].

KOA (Ключова атака) - зловмисник має доступ тільки до відкритого ключа ***pk***. Цей випадок неминучий для схем підпису з відкритим ключем (криптографії з відкритим ключем).

KMA (Атака на основі відомого повідомлення) - зловмисник має доступ до підписів безлічі відомих повідомлень.

CMA (Атака на основі вибраного повідомлення) - зловмисник має змогу використовувати в якості підписувача Оракул (повний доступ), і може запросити підпис будь-якого повідомлення на свій вибір (кілька запитів одного

і того ж повідомлення дозволені).

Наведемо графічне представлення (рисунок 1.3), для цього перенесемо показники цілей порушника на вісь Y, а показники моделей порушника на вісь X. Таким чином, точки перетину показників цілей порушника та моделей формалізуватимуть поняття безпеки або рівень безпеки.

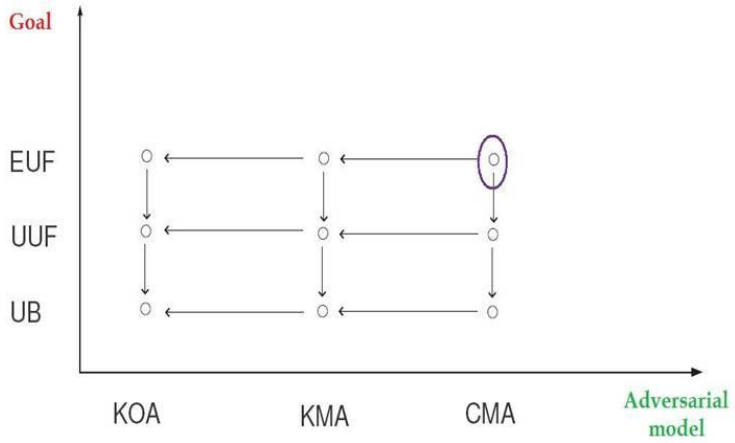


Рис. 1.3. Поняття безпеки схеми електронного підпису

Таким чином, схема підпису є екзистенційно непідробною, якщо зловмисник не може згенерувати будь-яку пару повідомлень підпису.

При реалізації атаки адаптивно підібраного повідомлення, зловмисник має доступ до оракула підпису, за допомогою якого він може підписувати повідомлення за своїм вибором.

Нехай, П=(K,T,V) – код автентифікації повідомлення та, нехай, Aeuf – ймовірнісний алгоритм, який виконується за поліноміальний час. Розглянемо наступну послідовність атаки:

1. Обчислення секретного стану $K \xleftarrow{\$} K(1^k)$.
2. Порушнику Aeuf надається необмежений доступ до міток оракула генерації OT та оракула перевірки OV виконання TK та VK.
3. Зрештою, Aeuf виводить пару повідомлення/мітка (M, T).

Нехай *QueriedEarlier* буде подією, що A^{euf} виводить повідомлення *M*, що буде вже запитувати мітку оракула генерації O_T. Ймовірність успіху A^{euf} $Succ_A^{euf} = Succ_A^{euf}(k)$ визначається :

$$Succ_{Aeuf} = Pr\left[\nu_{pk}(M, \sigma) = true\ and\ \neg QueriedEarlier\right]$$

і ми маємо у вигляді КАП П як безпечне в змісті EUF-CMA, якщо $Succ_A^{euf}$ мізерно мале для всіх імовірнісних порушників поліноміального часу A^{euf}

Висновки до розділу 1

1. Проведений аналіз показав, що успіхи в галузі квантових обчислень формують нові виклики для сучасної криптографії та обумовлюють необхідність пошуку нових шляхів забезпечення безпеки інформації та її основних властивостей - конфіденційності, цілісності, автентичності та неспростовності. Провідні країни світу розпочали роботи з розробки нових квантово-захищених криптографічних алгоритмів, які можуть успішно протистояти атакам у постквантовий період.

2. Показано, що на сьогоднішній день визначені основні напрямки розробок нових квантово-захищених алгоритмів: криптографічні перетворення на основі завадостійких кодів (СВ-криптографія), перетворення на основі геш-функцій (НВ-криптографія), криптографічні перетворення на решітках (LB-криптографія), мультіваріативно-квадратичні криптографічні перетворення (MQ-перетворення), а також використання ізогеніїв еліптичних кривих. Для розробки стандартів електронних підписів більш перспективними є НВ-криптографія та MQE-криптографія, у той час, як для розробки стандартів з асиметричного шифруваня - LB-криптографія та СВ-криптографія.

3. У даному розділі розкрито, що безпека систем може забезпечуватися не лише за рахунок криптостійкості примітивів, які покладені в її основу, а також за рахунок організаційно - технічних методів. Обґрунтоване поняття резильєнтності систем та показано, що за умови забезпечення безпеки інформації, яка обробляється в системі лише за рахунок підвищення параметрів

стійкості, можуть виникати ситуації значного ускладнення протоколів взаємодії між користувачами або внесення надмірності в розгорнуту систему захисту. Додатково зазначено, що поняття резильєнтності системи охоплює також властивості, пов’язані із можливістю продовжувати функціонування системи навіть в умовах кібератак.

4. Обґрунтовано, що важливою задачею для розгортання досліджень та розробки квантво-захищених алгоритмів є визначення вимог до нових алгоритмів. Визначено, що такі вимоги формуються за цільовим призначенням, а саме: вимоги стійкості, техніко-економічні та техніко-експлуатаційні вимоги. Вже сьогодні розпочаті роботи щодо формування таких вимог на рівні національних органів стандартизації США та ЄС.

5. Розкрита сутність моделей загроз для постквантового періоду, таких як IND-CCA2 (Indistinguishability under Adaptive Chosen Ciphertext Attack для алгоритмів шифрування та EUF-CMA (Existentially unforgeable under adaptive chosen message attacks для алгоритмів електронного підпису.

6. Основні положення даного розділу викладені у публікаціях автора [10-13, 80].

РОЗДІЛ 2

ПРИНЦИПИ ВИКОРИСТАННЯ РОЗПОДІЛЕНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ НАДІЙНОГО НАДАННЯ ЕЛЕКТРОНИХ ДОВІРЧИХ ПОСЛУГ

2.1 Технологія blockchain та її особливості, які можуть бути використані для надійної реалізації децентралізованих довірчих послуг

Побудова систем для надійного надання користувачам послуг, пов’язаних із використанням інформаційних технологій стає все більш актуальною задачею. Виникає необхідність побудови систем керування в тому числі критичними інфраструктурами. Такі задачі традиційно вирішувалися за допомогою побудови централізованих систем з центральним "керуючим" або "хабом", на який покладалися обов’язки керування та контролю за системою. Проте, із різким збільшенням спектру електронних систем та кількості користувачів побудова централізованих систем стає менш ефективним рішенням. Будь-яка централізована система має своє максимально допустиме навантаження при перевищені якого, її функціонування стає неефективним. Більше того, необхідно брати до уваги зростаючі ризики з боку кібернетичних атак, які змушують шукати нові стратегії забезпечення безпеки систем. Особливо це стосується систем, які обробляють критичну інформацію. Традиційним "слабким місцем" будь-якої централізованої структури є її вершина (тобто центральний орган управління), вихід із ладу його внаслідок спрямованої атаки фактично означає зупинку функціонування всієї системи. Виходом вбачається перехід на децентралізовані системи. В яких кожен із учасників виконує частину обов’язків керуючого [20].

На сьогодні найпоширенішим прикладом успішного впровадження децентралізованих систем безумовно слугують крипто валюти [21, 24, 81]. Необхідно зазначити, що такий принцип побудови може бути успішно

впроваджений також в інших сферах, в тому числі у сфері електронних довірчих послуг [18-20].

Особливо важливим питання при впровадженні децентралізованих технологій у сферу електроних довірчих послуг є формулювання політик та вимог по яким функціонує децентралізована система. Необхідно забезпечити всім користувачам єдине бачення стану системи в кожен конкретний момент часу. Це можливо із використанням технології blockchain [20].

Blockchain (block chain) - побудований за певними правилами безперервний послідовний ланцюжок блоків, що містять інформацію [19].

Блок транзакцій - спеціальна структура для запису групи транзакцій в системі біткойнов або аналогічних їй. Транзакція вважається завершеною і достовірною («підтвердженою»), коли перевірені її формат і підписи, і коли сама транзакція об'єднана в групу з декількома іншими та записана в спеціальну структуру - блок. Вміст блоків може бути перевірено, так як кожен блок містить інформацію про попередній. Всі блоки зв’язані в один ланцюжок, який містить інформацію про всі вчинені коли-небудь операції в базі. Найперший блок в ланцюжку - первинний блок (англ. Genesis block) - розглядається як окремий випадок, так як у нього відсутній батьківський блок [20].

Блок складається із заголовка і списку транзакцій (рисунок 2.3). Заголовок блоку включає в себе свое геш-значення, геш-значення попереднього блоку, геш-значення транзакцій і додаткову службову інформацію. Для зберігання транзакцій в блоці використовується деревоподібна структура гешування, аналогічна тій, яка використовується для формування геш-суми для файлу в протоколі BitTorrent [25].

Створений блок буде прийнятий іншими користувачами, якщо числове геш-значення заголовка дорівнює або меньше певного числа, величина якого періодично коригується (найчастіше використовується значення SHA-256). Так як результат гешування функції SHA-256 вважається незворотнім, на даний момент немає більш ефективного алгоритму отримання бажаного результату,

крім випадкового перебору. Якщо геш-значення не задовольняє умові, то в заголовку змінюється відповідний параметр nonce і геш-значення перераховується.

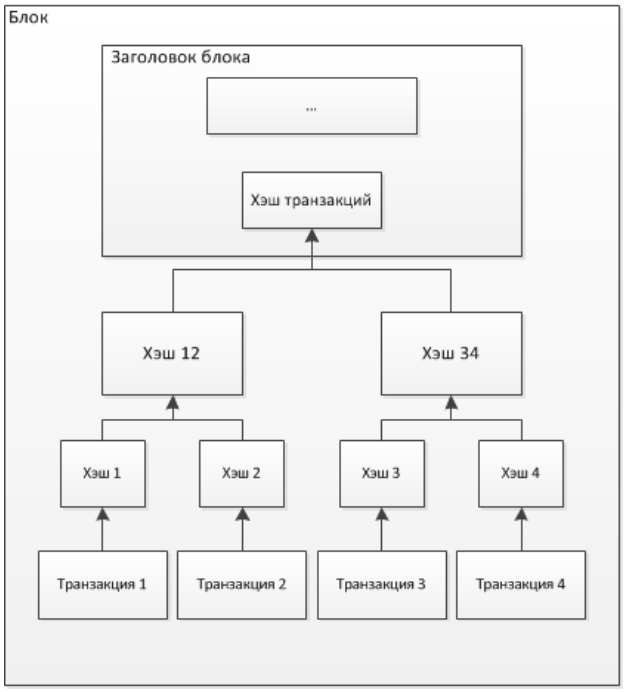


Рис. 2.3 – Структура блока

Зазвичай потрібна велика кількість перерахунків. Коли варіант знайдений, вузол розсилає отриманий блок іншим підключеним вузлам, які перевіряють блок. Якщо помилок немає, то блок вважається включеним у ланцюжок і наступний блок повинен включити в себе його геш-значення [30].

Блоки одночасно формуються безліччю «учасників». Ті, які задовольняють критеріям транслюються в мережу та включаються у розподілену базу блоків. Можуть виникати ситуації, коли кілька нових блоків в різних частинах мережі посилаються на один і той сами попередній блок, тобто ланцюжок блоків може ділитися на гілки. У цьому випадку можлива ситуація паралельного росту різних гілок. У кожному з нових блоків можуть зустрічатися як однакові транзакції, так і різні, що увійшли тільки в один з них. В такому випадку, учасникам необхідно дійти згоди (консенсусу) відносно того, яку з гілок вважати основною. Це можливо за допомогою децентралізованих протоколів консенсусу. Транзакції, що увійшли тільки у

відхилену гілку, втрачають статус підтверджених (рисунок 2.4). Таким чином, ланцюжок блоків містить історію, з якою можна ознайомитися.

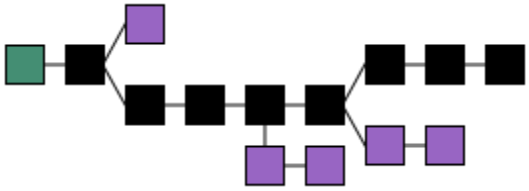


Рис. 2.4 – Ланцюжок блоків

Розподілена база даних blockchain формується як безперервно зростаючий ланцюжок блоків із записами про всі транзакції. Копії бази або її частини одночасно зберігаються на безлічі комп'ютерах (вузлах) і синхронізуються відповідно до формальних правил побудови ланцюжка блоків. Інформація у блоці не зашифрована (в загальному випадку) і доступна у відкритому вигляді, але відсутність змін засвідчується криптографично через геш-значення ланцюжка (елемент електронного підпису) [29].

База публічно зберігає в незашифрованому вигляді інформацію про всі транзакції, що підписуються за допомогою електронного підпису. Для запобігання «багаторазової витрати» (англ. Double spending) використовуються мітки часу, реалізовані шляхом розбиття БД на ланцюжок спеціальних блоків, кожен з яких, в числі іншого, містить в собі геш-значення попереднього блоку і свій порядковий номер. Кожен новий блок виступає підтвердженням для транзакцій, інформацію про які він містить, а також додатковим підтвердженням для транзакцій у всіх попередніх блоках ланцюжка. Змінювати інформацію в блоці, який вже знаходиться в ланцюзі, не практично, так як в такому випадку довелося б редагувати інформацію в усіх попередніх блоках. Таким чином, успішна double-spending атака на практиці вкрай малоймовірна. Оскільки включення транзакції в блок є підтвердженням її достовірності незалежно від наявності інших транзакцій, а кожен новий блок вважається додатковим «підтвердженням» транзакцій з попередніх блоків, у випадку, коли в ланцюжку наявні три блоки, то транзакції з останнього блоку будуть

підтверджені один раз, а ті, які містяться в першому - матимуть троєкратне підтвердження. Досить дочекатися декількох підтверджень, щоб звести ймовірність скасування транзакції до мінімуму [33].

Відкритість ланцюжка блоків дозволяє внести в довільний блок зміни. Але тоді потрібно виконати перерахунок геш-значення не тільки зміненого блоку, але і всіх попередніх. Фактично, для такої операції потрібно потужність не менше тієї, яка була використана для створення зміненого і наступних блоків (тобто всієї поточної потужності), що робить таку можливість вкрай малоймовірною.

2.2 Децентралізовані протоколи консенсусу. Можливості та рекомендації щодо використання

Надійне забезпечення доступності інформації щодо стану системи досягається за допомогою децентралізованих протоколів консенсусу.

Децентралізовані протоколи консенсусу можуть мати досить широкий спектр застосування [20]:

- формування журналу транзакцій цифрових валют;
- кластери;
- контролери баз даних;
- високонадійні обчислювальні системи;
- критичні технічні системи;
- авіоніка (система управління авіаційним обладнанням);
- космічні системи;
- управління ядерними реакторами, тощо.

Призначення протоколів консенсусу

Консенсус – це спосіб, завдяки якому різні вузли мережі досягають згоди про набір даних, який представляє з себе стан цієї мережі. Наприклад, транзакції, баланси на різних рахунках, результати виконання смарт-контрактів. Система на базі технології blockchain може бути представлена у вигляді

машини станів. Протокол консенсусу має забезпечувати послідовність дій, які забезпечують кожному вузлу доступ до актуального поточного стану мережі.

Основними вимогами до таких протоколів є [20]:

– відсутність центральної довіреної сторони (функціонування в середовищі взаємної недовіри: жоден з учасників не довіряє іншому);

– рівноправність вузлів. Мережа складається з рівноправних вузлів при цьому, якщо зовнішня сторона або зловмисник намагається вивести з дії певну кількість вузлів, мережа продовжує нормально функціонувати до тих пір, поки чесні учасники складають необхідну більшість серед працюючих);

– більшість вузлів є «чесними»;

– «чесні» учасники не знають які вузли контролюються зловмисниками. Список збійних ("атакованих") вузлів невідомий чесним учасникам та може динамічно оновлюватися);

– у кожного вузла або їх деякої множини можливі збої, повне відключення, довільна поведінка (в тому числі і скоординована зловмисником для проведення атаки мережі);

– мережа, в якій функціонує система, не є надійною, тобто можливі довільні затримки і втрати (пропуски) повідомлень.

Перші дві вимоги формулюються виходячи із принципу децентралізації системи. Необхідна кількість чесних вузлів залежить від типу протоколу консенсусу (можливі варіанти: >1/2 чесних учасників, >2/3 чесних учасників). При цьому кожний чесний вузол приходить в один і той же стан в умовах збоїв частини вузлів (або скоординованої роботи злочинних вузлів) та працює за наперед відомим формалізованим протоколом (без участі людини або будь-якої додаткової інформації) [20].

Виділяються такі припущення за яких протоколи мають продовжувати функціонувати [18]:

– чесні функціонуючі вузли складають більшість (понад 1/2 або більше 1/3 учасників);

– час прийняття рішення не є фіксованим;

– використовується значна надмірність (можна виконувати ідентичні завдання).

2.2.1 Результати порівняльного аналізу децентралізованих протоколів консенсусу

В залежності від того які правила використовуються для досягнення згоди між учасниками, можна виділити наступні групи протоколів консенсусу.

Proof of Work протоколи [20, 29]

Основні характеристики:

– кількість вузлів-учасників є необмеженою;

– вузли анонімними;

– репутація вузлів невідома;

– необхідна кількість «чесних вузлів» для надійного функціонування протоколу становить 51%;

– існує можливість централізації;

– вразливість до атаки 51%;

– простота масштабування. Додавання нового вузла проходить без змін правил функціонування системи;

– низька пропускна здатність (швидкість формування блоку досягає в деяких випадках 10 хвилин);

– високі енергетичні витрати.

Учасники починають вважати головним ланцюжок з урахуванням рівня складності геш-значення і довжини ланцюжка (правило найдовшого ланцюжка). У разі рівного розподілу складності і довжини перевага віддається тому ланцюжку, кінцевий блок якого з'явився раніше. Найяскравішим прикладом є протокол консенсусу Bitcoin.

Існують також інші правила вибору головного ланцюжку, наприклад кількість блоків у дереві, що утворює певний ланцюжок (як у алгоритмі GHOST) [74] (рисунок 2.5).

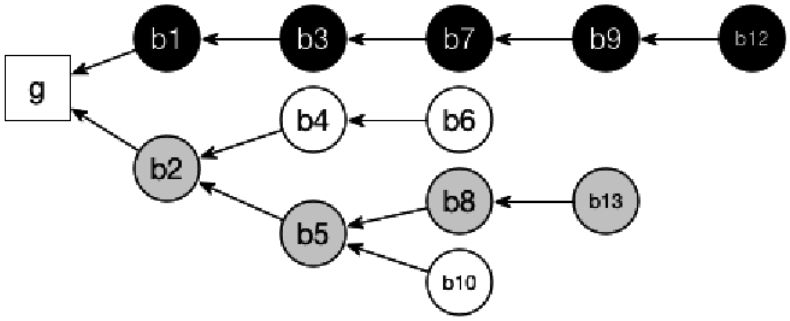


Рис. 2.5 Протокол консенсусу GHOST [74]

Транзакції, що увійшли тільки в відхилений ланцюжок, втрачають статус підтверджених. У 2017-2018 роках були запропоновані нові алгоритми PoW консенсусу такі, як SPECTRE та PHANTOM [20, 22], в яких використовується структура циклічного направленого графу (рисунок 2.6) завдяки чому відсутня втрата блоків. Недоліком протоколів SPECTRE та PHANTOM слід зазначити необхідність зберігання великої кількості інформації.

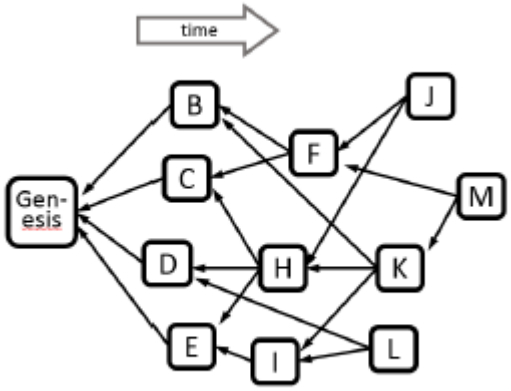


Рис. 2.6 – Протокол консенсусу PHANTOM [22]

Proof of Stake протоколи [20]

Основні характеристики:

– вузли-учасники не анонімні

– вузли-учасники мають репутацію

– монетарна мотивація учасників чесно слідувати протоколу. При спробі атаки, "ставка" учасника-порушника згорає.

По суті відбувається голосування (рисунок 2.7). Новий блок формує учасник, який зробив найбільшу «ставку». Логіка протоколів такого типу полягає в тому, що учасникам, із великою кількістю монет не вигідно робити спроби атак, оскільки успішна атака призведе до знецінення крипто валюти. Таким чином, для учасника немає більш вигідної стратегії, ніж чесно слідувати протоколу [23].

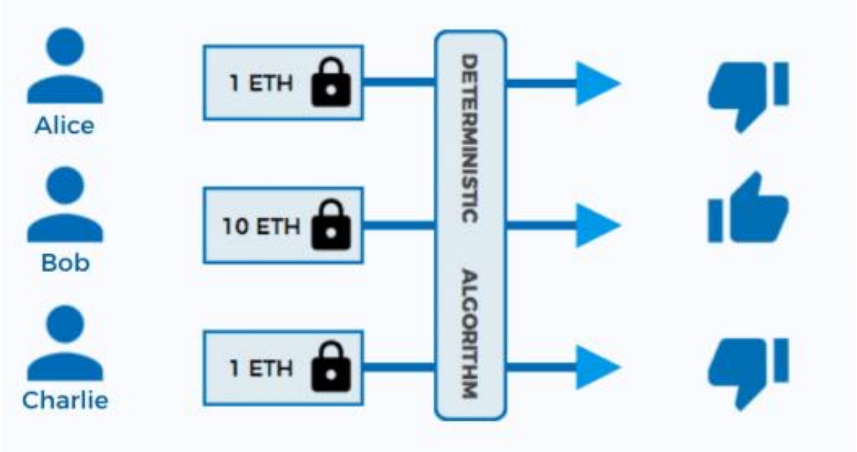


Рис. 2.7 – PoS протокол консенсусу

При цьому вузли можуть передавати свої голоси іншим, які будуть голосувати від їхнього імені, таким чином утворюючи колегію виборців (Delegated PoS) [23].

BFT протоколи

Основні характеристики:

– базуються на проблемі Візантійських генералів;
– вузли-учасники не є анонімними;
– для надійного функціонування чесних учасників має бути >2/3;
– ймовірність відміни рішення є експоненційно спадною;
– для прийняття рішення необхідна кінцева кількість кроків;
– висока пропускна здатність;
– можливі елементи централізації.

Протоколи BFT історично з'явилися першими. Practical BFT [26] протокол являв собою по суті варіант клієнт-серверної архітектури, коли тільки після звернення клієнта до серверу, транзакція могла бути передана іншим учасникам

для підтвердження. Нові протоколи Algorand [27] та Hashgraph [28], наприклад, позбавлені цього недоліку. Згідно з протоколом Algorand серед учасників випадковим чином обирається деякий підкомітет, який приймає рішення про підтвердження транзакції. Підтвердження відбувається у декілька етапів на кожному з яких обирається окремий підкомітет. Протокол має високу пропускну здатність, гарно масштабується. Проте, недоліком є погане функціонування у нестабільних мережах з великими затримками.

Альтернативні протоколи консенсусу.

Такі, наприклад, як Proof of Activity Protocol, Proof of Burn Protocol, а також інші гібридні протоколи [76].

Таблиця 2.1 [20] містить зведені дані порівняння основних груп протоколів консенсусу. Таблиця 2.2 [20] наводить їх у зведеній формі.

Таблиця 2.1

Переваги та недоліки основних груп протоколів консенсусу [20]

	Переваги	Недоліки
PoW протоколи	Доказова стійкість Легка масштабованість Необмежена кількість учасників	Високі енергетичні затрати Втрата частини інформації Необхідність зберігати великий об'єм інформації Низька пропускна спроможність
PoS протоколи	Висока пропускна спроможність	Монетарна мотивація учасників чесно слідувати протоколу
BFT протоколи	Висока пропускна спроможність Рішення, яке отримане не може бути відмінено з часом Для отримання рішення необхідна кінцева кількість кроків	Необхідність 2/3 чесних вузлів Відсутність мотивації учасників чесно слідувати протоколу

Таблиця 2.2

Зведена таблиця порівняння протоколів консенсусу [20]

		Анонімність/ відкритість вузлів-учасників	Наявність репутації вузлів-учасників	Мотивація вузлів-учасників	Математична задача	Необхідна кількість «чесних вузлів»	Простота масштабування
PoW	GHOST	Вузли є анонімні	Репутація Вузлів невідома	Винагородження за вирішення блоку	Пошук прообразу геш-функції	>1/2	Легко масштабувати
	SPECTRE						
	PHANTOM						
PoS	DelPoS DPoS	Вузли не анонімні	Вузли мають репутацію	Мотивація учасників чесно слідувати протоколу полягає в тому, що немає більш вигідної стратегії	Система "голосування"	>1/2	Труднощі у масштабуванні
BFT	Practical BFT	Вузли не анонімні	Вузли мають репутацію	Мотивація учасників чесно слідувати протоколу лежить за межами протоколу	«Проблема Візантійських генералів»	>2/3	Важко масштабувати
	Honey Badger BFT						
	ALGORAND						Легко масштабувати
	HSHGRAPH						

Висновки до розділу 2

1. У другому розділі показано, що децентралізовані системи здатні краще забезпечити функціонування електронних систем в умовах збільшення спектру електронних послуг та зростання кількості користувачів, оскільки вони позбавлені недоліку «традиційних» систем, які зазвичай мають порогове навантаження (тобто максимально допустиму кількість користувачів) після перевищення якого ефективність функціонування системи знижується.

2. У даному розділі обґрунтовано, що для надійного функціонування децентралізованих систем (в тому числі у критичних інфраструктурах) можливе використання технології blockchain із децентралізованими протоколами консенсусу.

3. Проведений аналіз [18-30] дозволив сформулювати наступні рекомендації щодо використання децентралізованих протоколів консенсусу [20]:

— вибір протоколу консенсусу має базуватися насамперед на умовах, в яких передбачається функціонування системи;
— можливе поєднання декількох протоколів в один (так звані гібридні протоколи);
— якщо система має функціонувати в умовах взаємної недовіри без додаткових інструментів контролю за користувачами доцільне використання PoW протоколів не дивлячись на низьку пропускну здатність таких протоколів;
— для систем закритого типу із наперед прогнозованою кількістю вузлів і без перспектив швидкого розширення, використання BFT протоколів є вигідним. При цьому необхідно додатково забезпечувати мотивацію вузлів-учасників чесно слідувати протоколу. Необхідною є первинна ідентифікація учасників;
— для не анонімних систем відкритого типу доцільним є використання PoS протоколів;

— якщо система має специфічну архітектуру та особливі умови функціонування, можливе використання гібридних багатошарових протоколів консенсусу, розроблених відповідно до особливостей даної системи. Одним із прикладів може бути поєднання PoW та PoS протоколу. В якому нові користувачі, які ще не мають попередньої історії транзакцій та, відповідно, особистої репутації користуються PoW протоколом, який в даному випадку забезпечуватиме їх накопиченням репутації. Після проходження "порогу довіри", користувач переходить на використання PoS протоколу;

4. основні положення даного розділу викладені у публікаціях автора [20].

РОЗДІЛ 3

ПРИНЦИПИ ПОБУДОВИ ДЕЦЕНТРАЛІЗОВАНОЇ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

3.1 Опис побудови інфраструктури відкритих ключів

Успішне впровадження сучасних технологій електронного урядування, а також електронних довірчих послуг не можливо без створення відповідної інфраструктури. Такою інфраструктурою реалізації виступає інфраструктура відкритих ключів (ІВК). Використання електронних довірчих послуг із застосування електронного підпису спирається на довіру між суб'єктами взаємодії, інфраструктуру відкритих ключів та направлено на реалізацію моделі довіри.

У 2017 році в Україні був прийнятий Закон України «Про електронні довірчі послуги» [46], який визначає правові та організаційні засади надання електронних довірчих послуг, в тому числі транскордонних, права і обов'язки суб'єктів правових відносин у сфері електронних довірчих послуг, порядок здійснення державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, а також правові та організаційні засади здійснення електронної ідентифікації [46]. Для ефективного використання і якісного надання таких послуг необхідно вирішувати багато технологічно складних завдань і технічних проблем. У 2004 році в Україні була реалізована архітектура ІВК (рисунок 3.1), яка стала базою для використання технології з відкритими ключами і надання послуг управління ними. Дана архітектура являє собою ієрархічну систему. Крім ієрархічної архітектури існує ще ряд можливих для використання, які не були використані через неможливість надійної реалізації моделі довіри.

Інфраструктура відкритих ключів (ІВК, англ. PKI - Public Key Infrastructure) – набір засобів (технічних, матеріальних, людських, тощо),

розподілених служб і компонентів, які в сукупності використовуються для виконання криптозадач на основі особистого та відкритого ключів [32].

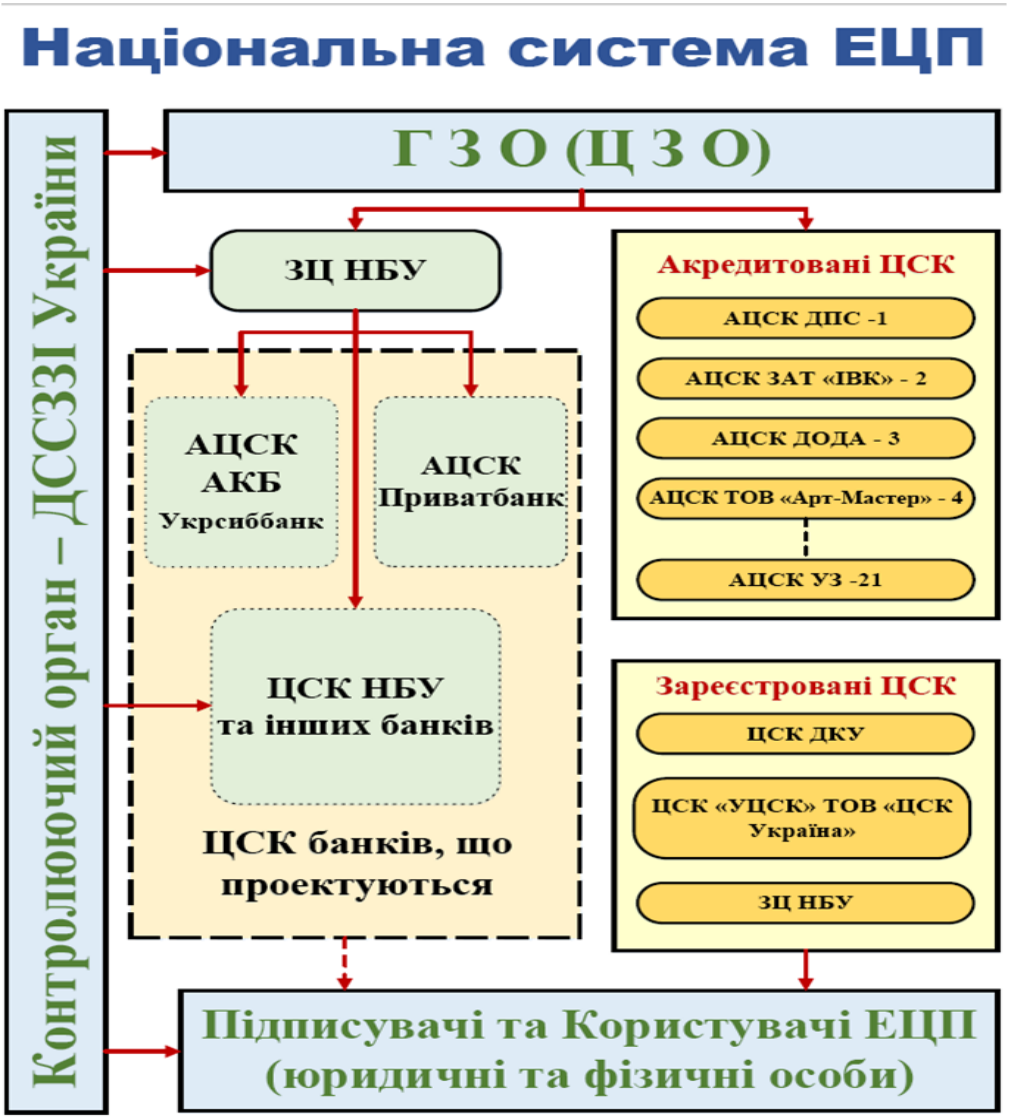


Рис. 3.1 Національна система ЕЦП

Для розгортання PKI необхідними умовами виступають використання криптографічної системи з відкритим ключем, а також забезпечення наступних принципів [32, 33]:

1. Особистий ключ (private key) відомий тільки його власнику.

2. Засвідчувальний центр (уповноважений на сертифікацію, англ. – Certification Authority, CA) генерує електронний документ – сертифікат відкритого ключа, тим самим засвідчуючи факт того, що особистий ключ

(private key) відомий виключно власнику цього сертифіката; при цьому відкритий ключ (public key) міститься у сертифікаті у відкритому вигляді.

3. Функціонування системи в умовах моделі взаємної недовіри, тобто жоден з учасників не довіряє іншому, але всі вони довіряють засвідчу вальному центру.

4. СА підтверджує або спростовує приналежність відкритого ключа особі, яка володіє відповідним особистим ключем.

Основним нормативним документом є стандарт ITU-T X.509 [31] (англ. Privilege Management Infrastructure). У ньому визначені стандартні формати даних та процедури розподілу відкритих ключів, які відбуваються за допомогою сертифікатів з електронними підписами, випущеними центрами сертифікації. Крім того, X.509 визначає формат списку відкликаних сертифікатів (англ. Certificate revocation lists, CRL), формат сертифікатів атрибутів (англ. Attribute certificates) і алгоритм перевірки підпису шляхом побудови ланцюжку сертифікації (англ. Certification path validation algorithm).

Інфраструктура відкритих ключів складається із наступних підсистем [32]:

- організаційно-технічна підсистема, яка включає в себе політики сертифікації, регламент, тощо;
- підсистема управління списками відкликаних сертифікатів, до якої входять: уповноважений на сертифікацію, центр реєстрації, репозиторій, кінцеві користувачі;
- підсистема застосувань ІВК, наприклад, web- захист, захищений email, захищений документообіг, VPN.

Для успішної реалізації технології відкритих ключів необхідно, щоб перевіряюча сторона була впевнена, що особистий ключ (якого вона не знає) належить саме тому віддаленого суб'єкту (користувачеві або системі), який буде використовувати засоби шифрування або електронного підпису. Це можливо забезпечити шляхом використання сертифікатів відкритих ключів. Такий сертифікат має обмежений термін дії. Оскільки перевіряюча сторона

може самостійно перевірити підпис і термін його валідності (дійсності), сертифікати відкритих ключів можуть поширюватися через незахищені канали зв'язку, а також зберігатися в геш-пам'яті незахищених систем [36, 37].

Для побудови ІВК необхідно вирішити проблемні питання на декількох рівнях:

- правовий рівень, який охоплює регулювання взаємовідносин між учасниками процесів сертифікації;
- системний рівень, тобто, обґрунтування вибору архітектури з урахуванням цільових завдань;
- процедурно-функціональний рівень – визначення основних функціональних вимог до системи сертифікації, встановлення переліку послуг центрів сертифікації;
- функціонально-технічний рівень, який передбачає визначення функціональної структури, фізичної топології, обґрунтування вимог безпеки;
- технічний рівень, який передбачає обґрунтування вибору апаратних засобів для центрів сертифікації, в тому числі засобів криптографічного захисту.

Основними загрозами для систем такого типу ІВК є [35]:

- відмова від виконання дій;
- підробка сертифіката.

Для забезпечення довіри в умовах взаємної недовіри, необхідно організувати функціонування системи в рамках актуальної моделі довіри. Відповідно до [31] передбачається використання таких моделей довіри:

- строга ієрархія уповноважених на сертифікацію;
- нестрога ієрархія уповноважених на сертифікацію;
- ієрархія на базі політик;
- модель розподіленого довіри;
- чотирьохстороння модель довіри;
- модель довіри навколо користувача;
- web-модель довіри.

На сьогоднішній день переважна більшість PKI, включаючи українську, побудовані на основі строгої ієрархії уповноважених на сертифікацію (рисунок 3.2).

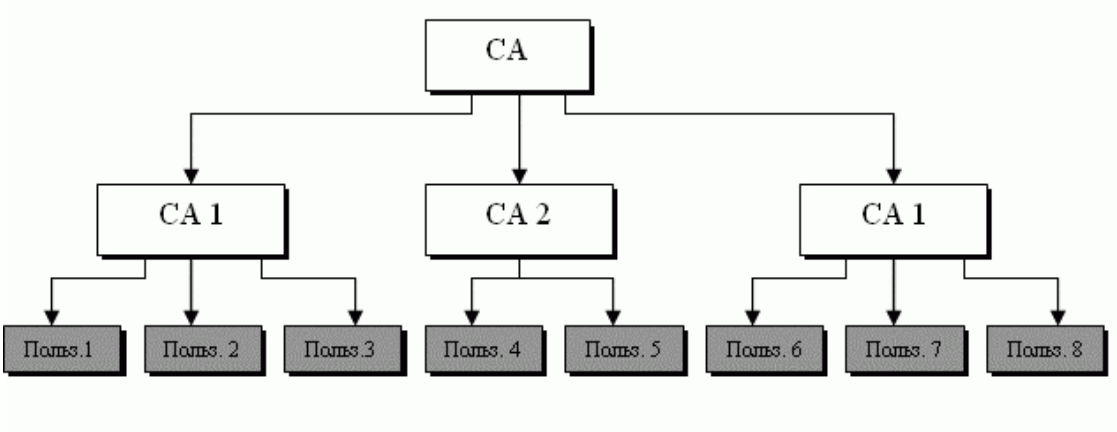


Рис. 3.2 Ієрархічна структура уповноважених на сертифікацію [33]

Однак така структура має наступні недоліки [33-37]:

- безпека всієї системи залежить від кореневого сертифіката головного уповноваженого на сертифікацію. У випадку його компрометації, всі інші сертифікати в системі також будуть скомпрометовані;
- користувачі практично не розпоряджаються своїми ідентифікаційними даними, наприклад, для внесення будь-яких змін, користувачу-власнику даних необхідно звертатися до уповноваженого на сертифікацію;
- відсутність інтероперабельності системи. Полягає в тому, що сертифікати, випущені різними уповноваженими на сертифікацію не завжди можуть бути використані в одній системі;
- відсутність однозначної відповідності між користувачем і сертифікатом, оскільки для одного користувача може бути випущено безліч сертифікатів. Це призводить до росту об’єму інформації, яка зберігається в on-line просторі;
- при масштабуванні системи виникають труднощі.

Решта моделей довіри слабо поширені, або не використовуються зовсім. Проведений аналіз [18-19, 60, 67] показав, що за допомогою використання

технології blockchain може бути надійно реалізована також інша модель довіри – модель довіри навколо користувача [33].

3.1.1 Модель довіри навколо користувача

В основі моделі довіри навколо користувача, він (користувач) самостійно відповідає за рішення яким сертифікатами довіряти, а які вважати ненадійними. Такі рішення залежать від ряду факторів. Первинним джерелом довіри є сертифікати родичів, друзів, знайомих, тобто тих, кого він знає особисто. Таким чином, можна зробити висновок, що первинна ідентифікація проводиться користувачем самостійно.

Довіру, сконцентровану навколо користувача можна зобразити наступним чином (рисунок 3.3). Користувач ***A*** може вирішити довіряти сертифікату користувача ***B*** (ланцюжка сертифікатів від друга користувача ***A*** до користувача ***C*** і ***B***) або відкинути сертифікат користувача ***B***, аргументуючи це тим, що до "невідомого" користувача ***B*** веде занадто мало зв'язків від "знайомих" користувачу ***A*** користувачів.

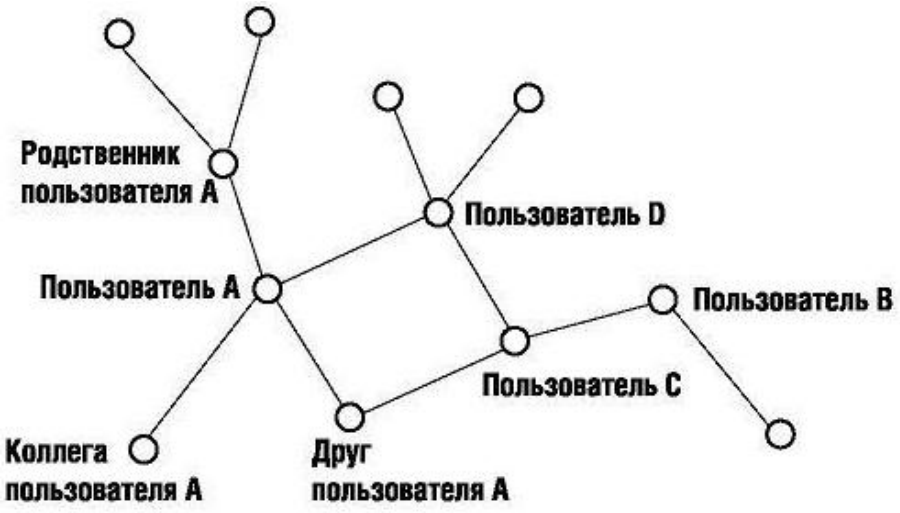


Рис. 3.3 – Модель довіри навколо користувача [33]

В силу своєї залежності від дій і рішень користувачів, модель довіри, сконцентрованої навколо користувача, без допоміжних засобів може використовуватися тільки у вузькому і високотехнологічному співтоваристві, але вона не життєздатна в звичайному співтоваристві, в якому багато

користувачів не мають достатніх знань про безпеку і технології PKI. Більш того, ця модель не підходить для тих сфер (корпоративної, фінансової, урядової), де є потреба у контролі за тим, з ким взаємодіють і кому довіряють користувачі.

3.2 Концепція побудови ІВК з використанням технології blockchain та основні процеси в системі

Аналіз [72, 73] показав, що довіра в системі може бути забезпечена за допомогою технології blockchain. По суті, blockchain – це журнал з фактами (реєстр фактів), який реплікується на декілька комп'ютерів, об'єднаних в мережу рівноправних вузлів (P2P). Фактами може бути що завгодно, від фінансових операцій до підписання контенту. Учасниками мережі є анонімні особи, які називаються вузлами. Всі комунікації всередині мережі використовують криптографію для надійної ідентифікації відправника і одержувача. Коли вузол хоче додати факт в журнал, в мережі формується консенсус для визначення місця цього конкретного факту в журналі. Цей консенсус називається блоком [35, 36].

Ця ідея може бути розширена для розробки децентралізованої ІВК без побудови строгої ієрархії уповноважених на сертифікацію.

Основні принципи децентралізованої ІВК наведені нижче [33].

1. Кожен користувач (користувач виступає вузлом) зберігає свою ключову пару самостійно. Сертифікат відкритого ключа передається разом із підписаним повідомленням.
2. Запис про транзакції зберігається в розподіленої базі за законами blockchain.
3. Блок транзакцій містить реєстр станів сертифіката.
4. При перевірці правильності транзакції, тобто дійсності сертифіката відкритого ключа, стороні-перевірнику необхідно простежити реєстр стану сертифіката відправника до його першої публікації.
5. Первинна ідентифікація нового користувача, однак, є обов'язковою і повинна бути надійно підтверджена. Тільки для цієї мети необхідний

довірений вузол (аналог уповноваженого на сертифікацію в ієрархічній структурі). Його роль буде полягати в первинному випуску сертифіката нового користувача, а також у випадках необхідних для зміни статусу сертифіката. Після першої транзакції, проведеною новим користувачем, звернення до довіреного вузла більше не виникає. Доцільним представляється покласти цю роль на структуру, яка підлягає сертифікації з боку контролюючих державних органів.

Тут і далі введемо наступні умовні позначення [33]:

M- повідомлення

$Sign$ – електронний підпис відправника

H- криптографічна геш-функція

$Sert$- сертифікат відкритого ключа відправника

ID- унікальний ідентифікатор відправника виданий йому на етапі первинної ідентифікації

$Status$- статус сертифіката відкритого ключа відправника

Основні процеси всередині системи децентралізованої ІВК:

- процес первинної ідентифікації користувача та генерації ключової пари;
- процес генерації підпису;
- процес перевірки підпису.

До додаткових процесів відносяться:

- процес оновлення статусу сертифіката;
- процес оновлення сертифікату.

Процес первинної ідентифікації користувача та генерації ключової пари.

Як зазначалося вище первинна ідентифікація (рисунок 3.4) повинна проводитися сертифікованою структурою (довірчим вузлом). При зверненні до якої користувачу видається (генерується) його унікальний ідентифікатор (ID) та відповідний йому сертифікат відкритого ключа ($Sert$), який пов'язаний із

особистим ключем користувача. Слід зазначити, що довічний вузол не зберігає у себе ID користувача, більше того, він його не знає.

Перша транзакція нового користувача повинна бути звернена до довірчого вузла для того, щоб при наступних транзакціях інші користувачі мережі могли прослідкувати реєстр станів даного сертифіката відкритого ключа. Так як для надійного підтвердження транзакції необхідно обчислення 3-5 блоків наступних за блоком з даної транзакцією, рекомендується відправляти транзакцію не тільки до одного представника довіреної структури, а до кількох (наприклад: оператор реєстрації, оператор сертифікації).

Після проходження процедури первинної ідентифікації дані поширюються в розподілену базу, в якій вони зберігаються в наступному вигляді (Табл. 3.1).

Таблиця 3.1

Вигляд розподіленої бази (blockchain) [33, 35]

$H(Sert, ID)$	$H(Sert, Status)$	$Status$

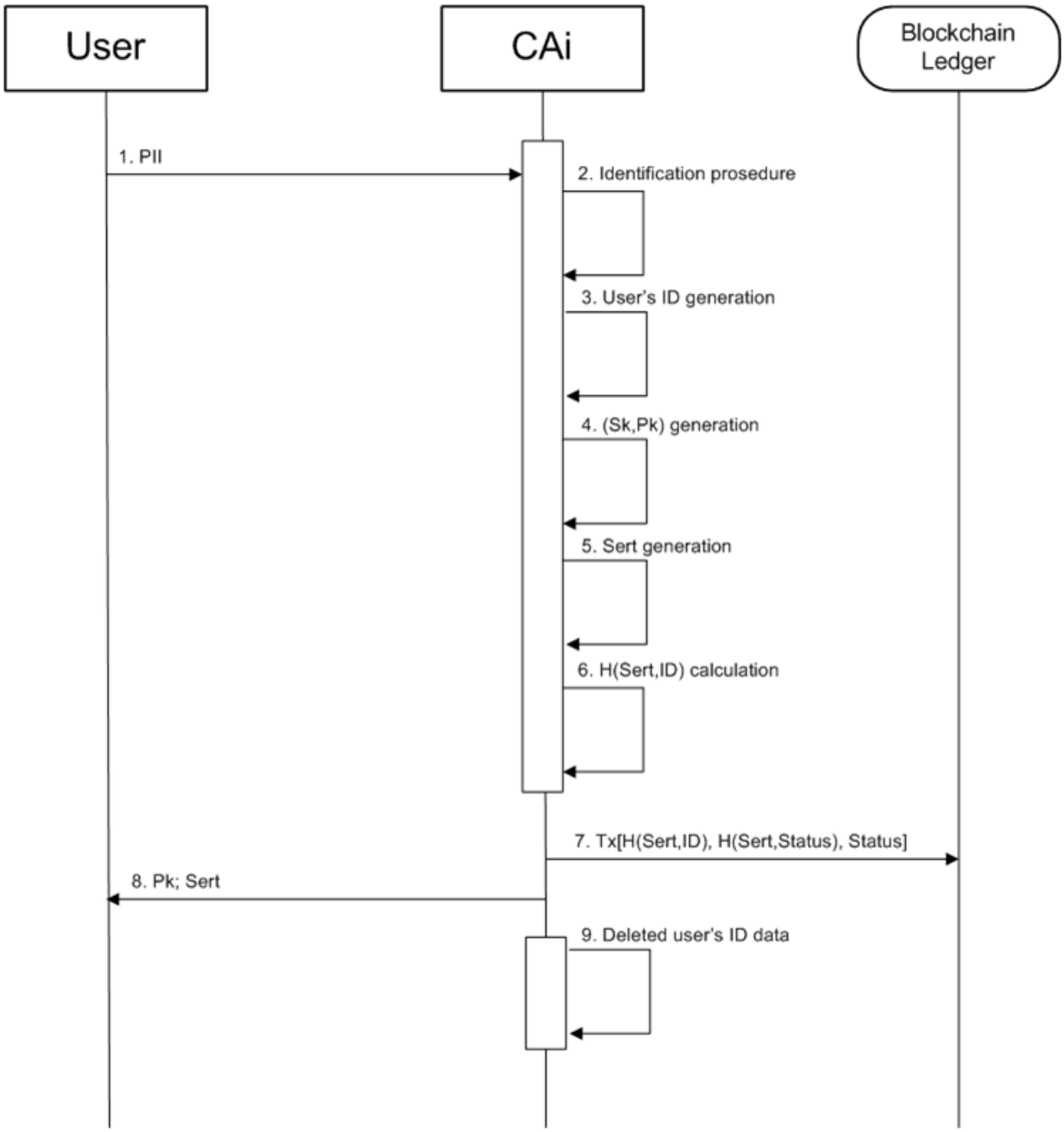


Рис. 3.4 Алгоритм первинної ідентифікації за умови генерації ключової пари в межах контрольованої зони довіреного вузла

Алгоритм первинної ідентифікації за умови генерації ключової пари на стороні довіреного вузла складається із наступних кроків.

1. Користувач звертається до довіреного вузла із запитом на генерацію ключової пари. В даному випадку такий запит робиться в межах контрольованої зони довірчого вузла. Для цього користувач надає свої персональні дані (*PII*).

2. Довірчий вузол проводить процедуру первинної ідентифікації користувача на основі його персональних даних.
3. Після успішної процедури первинної ідентифікації довірчий вузол генерує унікальний ідентифікатор (*ID*) для користувача.
4. Довірчий вузол генерує ключову пару для користувача (*Sk, Pk*). Така процедура генерації відбувається в межах контрольованої зони довіреного вузла. Відповідальність за правильність процедури генерації ключової пари в даному випадку покладається на довірчий вузол. Особистий ключ генерується безпосередньо на носій (файловий носій, апаратний носій, захищений носій ключової інформації) користувача.
5. На основі відкритого ключа користувача довірчий вузол виготовляє сертифікат відкритого ключа.
6. Довірчий вузол обчислює геш-значення від сертифікату відкритого ключа (*H(Sert, ID)*) користувача та його ідентифікатора.
7. Довірчий вузол формує транзакцію, в яку включає геш-значення від сертифікату відкритого ключа користувача та його ідентифікатора (*H(Sert, ID)*), геш-значення від сертифікату відкритого ключа користувача та статусу сертифікату (*H(Sert, Status)*), статус сертифікату (*Status*). Таку транзакцію довірчий вузол підписує власним особистим ключем. Вузли-валідатори (тобто довірені вузли) мережі blockchain досягають консенсусу щодо даної транзакції.
8. Користувач отримує наступний набір інформації: відкритий ключ (особистий ключ був згенерований на носій користувача на кроці 4), сертифікат відкритого ключа (*Pk, Sert*).
9. Довірчий вузол видаляє персональні дані користувача та його ідентифікатор із своєї системи.

При умові виконання вимог до генерації ключової пари та при наявності необхідного обладнання на стороні потенційного користувача, такий користувач може самостійно згенерувати собі ключову пару та надати її разом із своїми персональними даними довірчому вузлу для проходження процедури

первинної ідентифікації. Алгоритм первинної ідентифікації користувача за умови генерації ключової пари на стороні користувача зображено на рисунку 3.5.

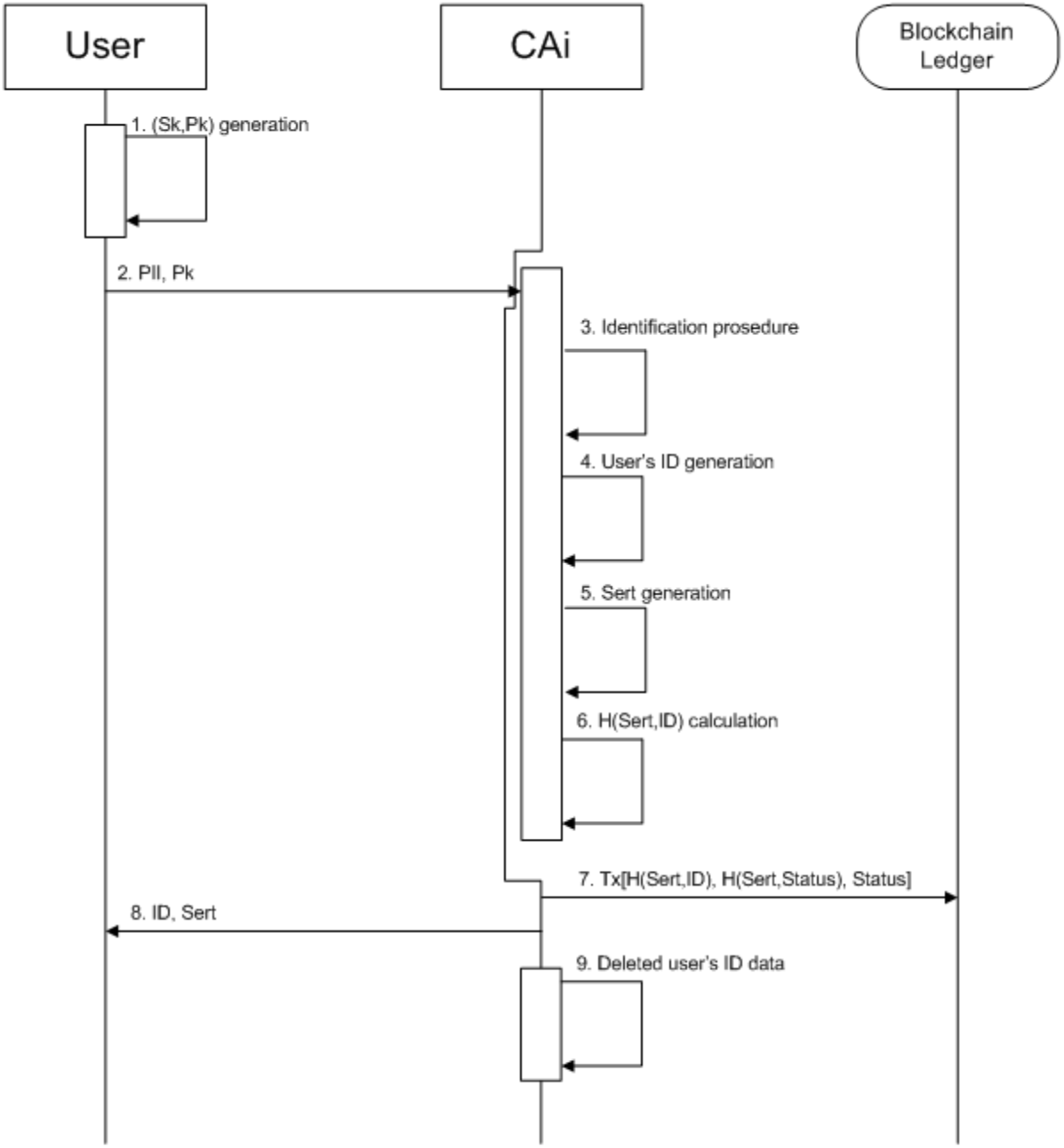


Рис. 3.5 Алгоритм первинної ідентифікації за умови самостійної генерації ключової пари користувачем

Алгоритм первинної ідентифікації користувача за умови генерації ключової пари на стороні користувача включає наступні кроки.

1. Користувач самостійно генерує власну ключову пару (*Sk, Pk*). В залежності від вимог особистий ключ може бути згенерований на файловий/апаратний носій або на захищений носій ключової інформації.
2. Користувач надсилає запит до довірчого вузла. В такий запит він включає свої персональні дані (*PII*) та відкритий ключ (*Pk*). Відповідний запит має бути зроблений через надійний канал зв'язку, оскільки він включає в себе критичну інформацію.
3. На основі отриманих даних довірчий вузол проводить процедуру первинної ідентифікації користувача.
4. Після успішної процедури первинної ідентифікації довірчий вузол генерує унікальний ідентифікатор для користувача (*ID*).
5. Довірчий вузол на основі відкритого ключа користувача виготовляє сертифікат відкритого ключа (*Sert*).
6. Довірчий вузол обчислює геш-значення від сертифікату відкритого ключа користувача та його ідентифікатора (*H(Sert; ID)*).
7. Довірчий вузол формує транзакцію, в яку включає геш-значення від сертифікату відкритого ключа користувача та його ідентифікатора (*H(Sert; ID)*), геш-значення від сертифікату відкритого ключа користувача та статусу сертифікату (*H(Sert, Status)*), статус сертифікату (*Status*). Таку транзакцію довірчий вузол підписує власним особистим ключем. Вузли-валідатори мережі blockchain досягають консенсусу щодо даної транзакції.
8. Користувач отримує наступний набір інформації: ідентифікатор сертифікат відкритого ключа (*ID; Sert*).
9. Довірчий вузол видаляє персональні дані користувача та його ідентифікатор із своєї системи.

Процес генерації підпису.

Алгоритм формування підпису не відрізняється від існуючого у ієрархічній структурі та залежить лише від типу підпису. Необхідно зазначити,

що в даному випадку можуть бути використані будь-які стандарти електронного підпису, включаючи постквантові [33].

Відправник підписує повідомлення електронним підписом, та надсилає отримувачу (стороні-перевірнику) наступний набір даних:

$$M;\ Sign;\ H(Sert, ID);\ Sert;\ Status$$

Процес перевірки (верифікації) підпису.

Алгоритм перевірки підпису зображений на рисунку 3.6.

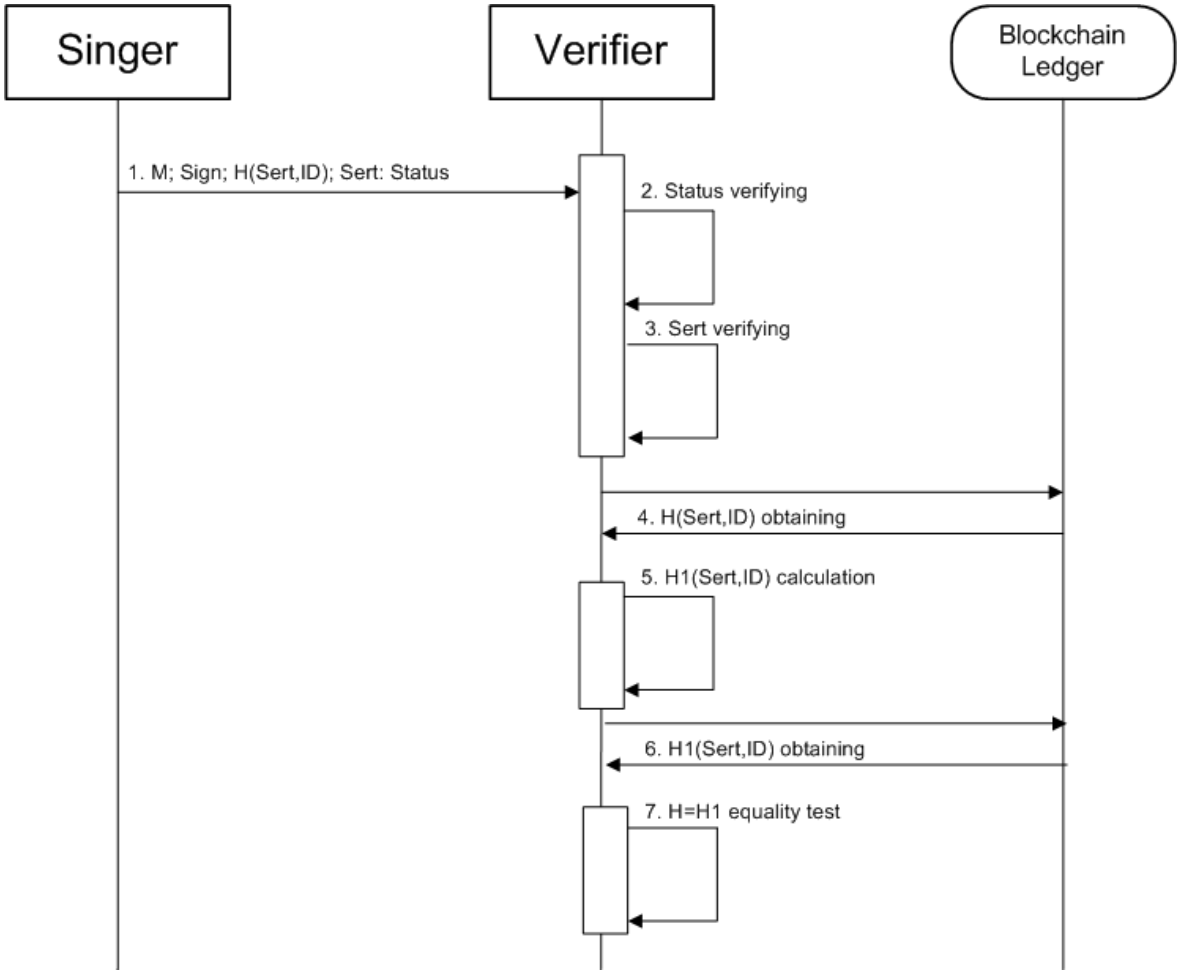


Рис. 3.6 Алгоритм перевірки підпису

Алгоритм перевірки підпису складається з наступних кроків.

1. Перевіряюча сторона отримує від відправника наступний набір даних: повідомлення, підписане електронним підписом, геш-значення від

сертифіката відкритого ключа відправника та його ідентифікатора, сертифікат відкритого ключа відправника у відкритому вигляді, статус сертифіката відкритого ключа відправника у відкритому вигляді (*M; Sign; H(Sert, ID); Sert; Status*).

2. Перевіряюча сторона проводить верифікацію статусу сертифікату відкритого ключа відправника на основі даних ($H(Sert, ID); Status$) із розподіленої бази (Табл. 3.1).
3. Якщо визначено, що сертифікат відкритого ключа відправника дійсний, перевіряюча сторона проводить верифікацію електронного підпису на основі даних, отриманих від відправника ($Sign; Sert$). Якщо верифікація електронного підпису успішна (тобто, електронний підпис накладений саме за допомогою особистого ключа, якому відповідає наданий сертифікат відкритого ключа відправника), перевіряюча сторона має визначити що даний сертифікат відкритого ключа дійсно належить відправнику. Для цього виконуються наступні дії.
4. Перевіряюча сторона отримує значення та адресу поля $Status$ із розподіленої бази даних (Табл. 3.1) на основі отриманого від відправника $H(Sert, ID)$.
5. Перевіряюча сторона самостійно обчислює $H1(Sert, Status)$ на основі даних, отриманих від відправника.
6. Перевіряюча сторона отримує значення та адресу поля $Status1$ із розподіленої таблиці на основі обчисленого на попередньому кроці $H1(Sert, Status)$.
7. Якщо значення та адреса $Status$ та $Status1$ співпадають, перевірка вважається успішною.

Процеси оновлення статусу сертифікату відкритого ключа та оновлення сертифікату відкритого ключа.

У децентралізованій ІВК користувачі самостійно можуть ініціювати зміни щодо статус свого сертифікату відкритого ключа, наприклад, тимчасово його призупинити або відкликати. Алгоритм оновлення статусу сертифікату наведений на рисунку 3.7.

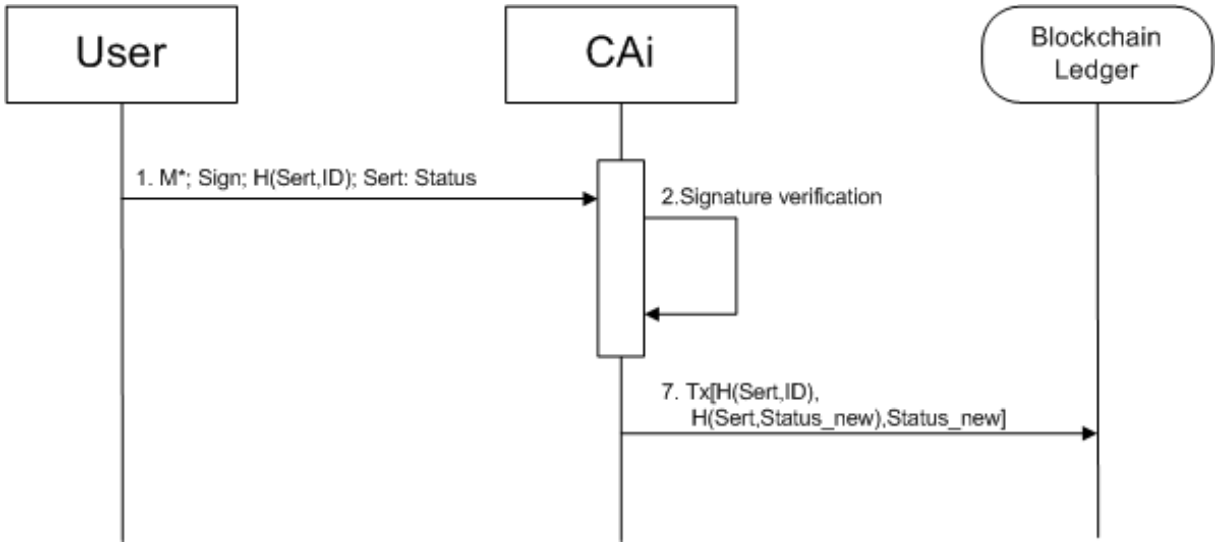


Рис. 3.7 Алгоритм оновлення статусу сертифікату

Алгоритм оновлення статусу сертифікату складається із наступних кроків:

1. Користувач генерує запит до будь-якого довіреного вузла. У такому запиті користувач повідомляє про необхідність зміни статусу його сертифікату відкритого ключа (наприклад про необхідність його блокування / поновлення). Користувач підписує запит власним особистим ключем.
2. Довірчий вузол проводить процедуру перевірки підпису.
3. Якщо перевірка успішна, то довірчий вузол формує транзакцію, у яку включає новий статус сертифіката користувача. Вузли-валідатори мережі blockchain досягають консенсусу щодо даної транзакції.

На рисунку 3.8 наведений алгоритм оновлення (перевипуску) сертифікату відкритого ключа.

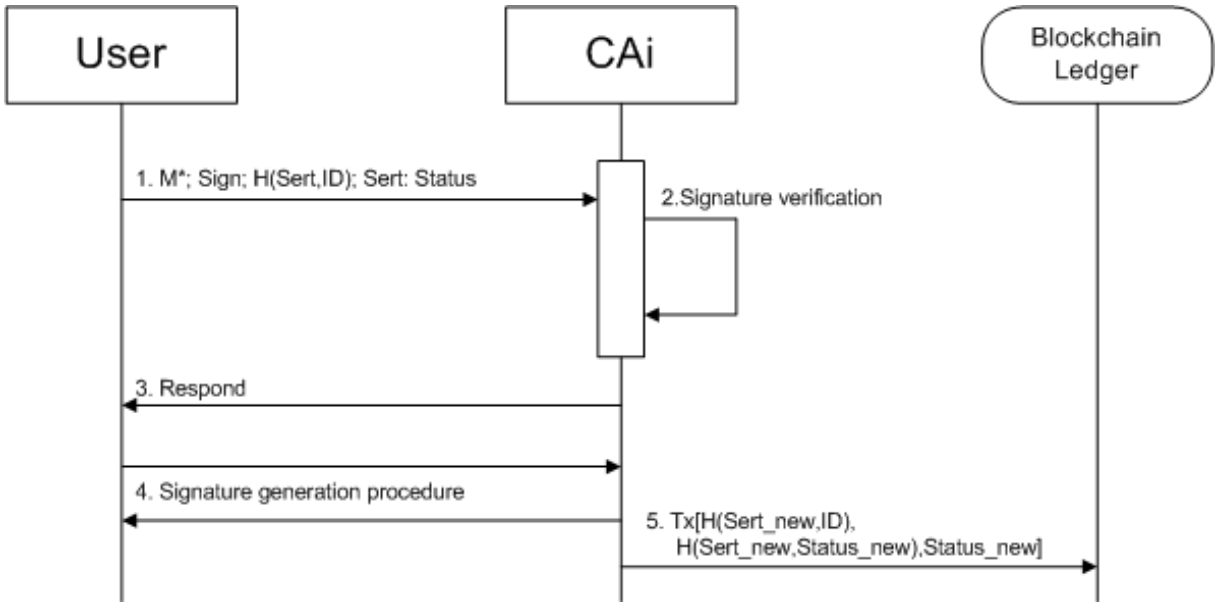


Рис. 3.8 Алгоритм оновлення сертифікату

Алгоритм оновлення сертифікату користувача складається із наступних кроків.

1. Користувач формує запит на оновлення перевипуск сертифікату (наприклад у зв’язку із закінченням терміну дії минулого). Такий запит користувач підписує особистим ключем (за умови, що ключова пара на момент підписання є дійсною).
2. Довірчий вузол проводить процедуру перевірки підпису.
3. Якщо перевірка успішна, довірчий вузол надає інформацію про це користувачу.
4. Користувач ініціює процедуру генерації ключової пари за одним із вище описаних алгоритмів.
5. За результатом процедури генерації ключової пари, довірчий вузол формує транзакцію, яка містить новий сертифікат користувача.

3.3 Результати оцінок часових витрат на формування децентралізованої інфраструктури відкритих ключів

В даному розділі наводяться результати оцінок часових витрат на формування децентралізованої ІВК для двох випадків:

1. початковою архітектурою мережі була ієрархічна ІВК;
2. формування децентралізованої ІВК «з нуля», тобто децентралізована ІВК формується одразу без побудови ієрархії уповноважених на сертифікацію.

Для першого випадку розглянемо результати для мереж зі строгою ієрархією уповноважених на сертифікацію. Для другого випадку розглянемо мережу, представлену повнозв'язним графом (маючи на увазі, що кожен учасник має прямий зв'язок із будь-яким іншим).

Для формування децентралізованої ІВК необхідно досягнути стану консенсусу в мережі. Під консенсусом у ІВК мається на увазі стан мережі, в якому кожен вузол впевнений у легітимності всіх інших учасників. Це можливо після процедури «авторизації мережі». Суть якої полягає у ініціації взаємодії кожного користувача з усіма іншими згідно із законами ланцюжка сертифікації в ієрархічній структурі та згідно із законами blockchain в розподіленій [34].

У цьому розділі наведені результати моделювання, проведеного за допомогою розробленого програмного забезпечення (лістинг знаходиться у Додатку Д). Необхідно звернути увагу на те, що ми не інтегруємо алгоритми електронного підпису безпосередньо. Для процедури порівняння нам достатньо стверджувати, що для всіх топологій прийнятий єдиний алгоритм електронного підпису.

Для виконання моделювання процедури «авторизації мережі» для різних топологій слід вказати наступні початкові умови [34]:

1. Мережа задається графом.
2. Вузли зберігають поле «opinion» (логічне значення: «1» - користувач легітимний, «0» - зловмисник).

3. Учасники заздалегідь не знають, які з вузлів контролюють зловмисники. Вони можуть це зрозуміти лише в процесі попарної взаємодії. Це означає
— (а) проходження шляху сертифікації в ієрархічній архітектурі структурі або
— (б) шляхом взаємодії один з одним у розподіленій.
4. На початковому етапі 50 % вузлів контролюються зловмисниками.
5. Якщо виявлено зловмисника, його (і вузли, що залежать від нього в ієрархічній структурі) слід виключити з мережі, а формування консенсусу слід завершити без нього. Таким чином буде сформована мережа легітимних учасників, і вони зможуть взаємодіяти безперешкодно та безпечно.
6. Вузли, які були виключені з мережі, повинні бути перегенеровані (знову із ймовірністю 50%) та включені в мережу.
7. Під часом консенсусу розуміється час, витрачений на повну «авторизацію мережі» (включаючи час на регенерацію та повторне підключення вузлів).

Для опису процедури «авторизації мережі» необхідні наступні припущення:
— розглянуті топології перебувають у закритому / захищеному просторі (таким чином, ми розглядаємо приватну ІВК або приватний blockchain);
— час взаємної / перехресної перевірки (перевірки сертифіката відкритого ключа) займає одну ітерацію;
— час регенерації вузла займає дві ітерації (одна ітерація на генерацію ключової пари, друга – виготовлення сертифікату відкритого ключа).

Протоколи формування децентралізованої ІВК.

Для коректної роботи протоколу обов'язковою умовою є дотримання вимог, закріплених у X.509. Розглядається протокол суворої ієрархічної структури, що означає необхідність побудови шляху сертифікації до кореневого вузла при ініціалізації взаємодії будь-яких двох користувачів.

Процедура «авторизації мережі» для ієрархічної топології мережі повинна складатися з наступного.

1. Взаємодія починається з листя дерева і має напрямок до кореня.

2. Маршрут визначається правилами шляху сертифікації відповідно до X.509
3. Коли виявляється вузол зловмисника, його та всі його дочірні вузли повинні бути виключені та піддані процедурі регенерації.
4. Процедура взаємодії повинна продовжуватися для всіх легітимних вузлів.
5. Після взаємодії всіх легітимних вузлів; слід розпочати процедуру регенерації виключених вузлів.

Більше того,

- якщо у вузла-зловмисника не було «дітей» (діяв як кінцевий користувач), під час процедури його регенерації існує ймовірність (ми встановимо її рівною 50 відсоткам), що він знову виявиться зловмисником.
- якщо ні (діяв як орган сертифікації), то його безпосередньо слід перегенерувати зі значенням поля «opinion» = 1, а всі його дочірні вузли, з ймовірністю 50 %, можуть знову стати зловмисниками.

Процедура «авторизації мережі» для децентралізованої топології мережі повинна складатися з наступного.

1. Взаємодія може бути запущена з будь-якого вузла мережі.
2. Потрібно виконати попарну сертифікацію (обмін сертифікатами ключів) між кожними парами вузлів.
3. Коли виявлено вузол зловмисника, його потрібно виключити та піддати процедурі регенерації.
4. Процедура взаємодії повинна продовжуватися для всіх законних користувачів.
5. Після взаємодії всіх законних вузлів необхідно запустити процедуру регенерації виключених вузлів (враховуючи ймовірність регенерації, рівну 50 відсоткам).
6. Протокол продовжує свою роботу до тих пір, поки всі вузли не стануть легітимними і взаємопов’язаними між собою.

Відповідне моделювання проводилося для двох типів ієрархічної топології: для дерева, із ступенем 3 для кожного вузла (рисунок 3.9), та «дерева з п’ятьма хабами» (рисунок 3.10).

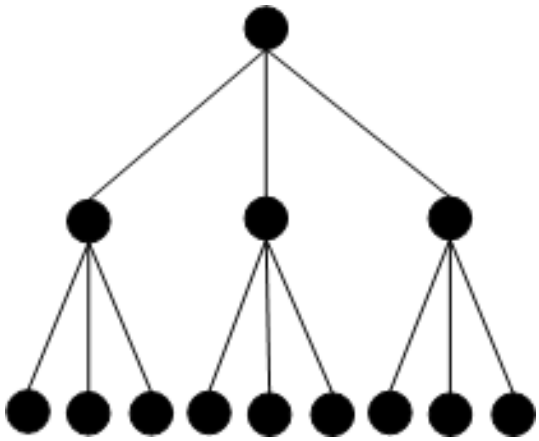


Рис. 3.9 Дерево із ступенем 3 для кожного вузла

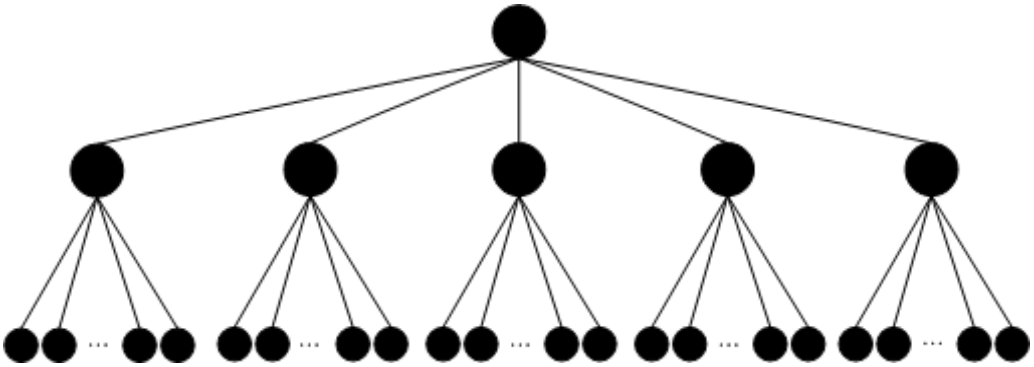


Рис. 3.10 «Дерево з п’ятьма хабами»

Дерево , із ступенем 3 для кожного вузла - це класичний приклад симетричної PKI, який добре підходить для структурування поглибленої організаційної структури. Обмежена кількість дочірніх вузлів не дозволяє системі швидко розширюватися в горизонтальному напрямку. Прикладом використання такої PKI може бути об'єднання невеликих, але чітко структурованих одиниць.

З протилежного боку варто зазначити, що «дерево з п’ятьма хабами» виглядає типово для “широкої” PKI. При цьому ми маємо кілька (у даному випадку п’ять) великих піддерев (підрозділів), у яких може взаємодіяти велика кількість рівних користувачів.

Результати моделювання для протоколу строгої ієрархічної структури наведені на рисунку 3.11.

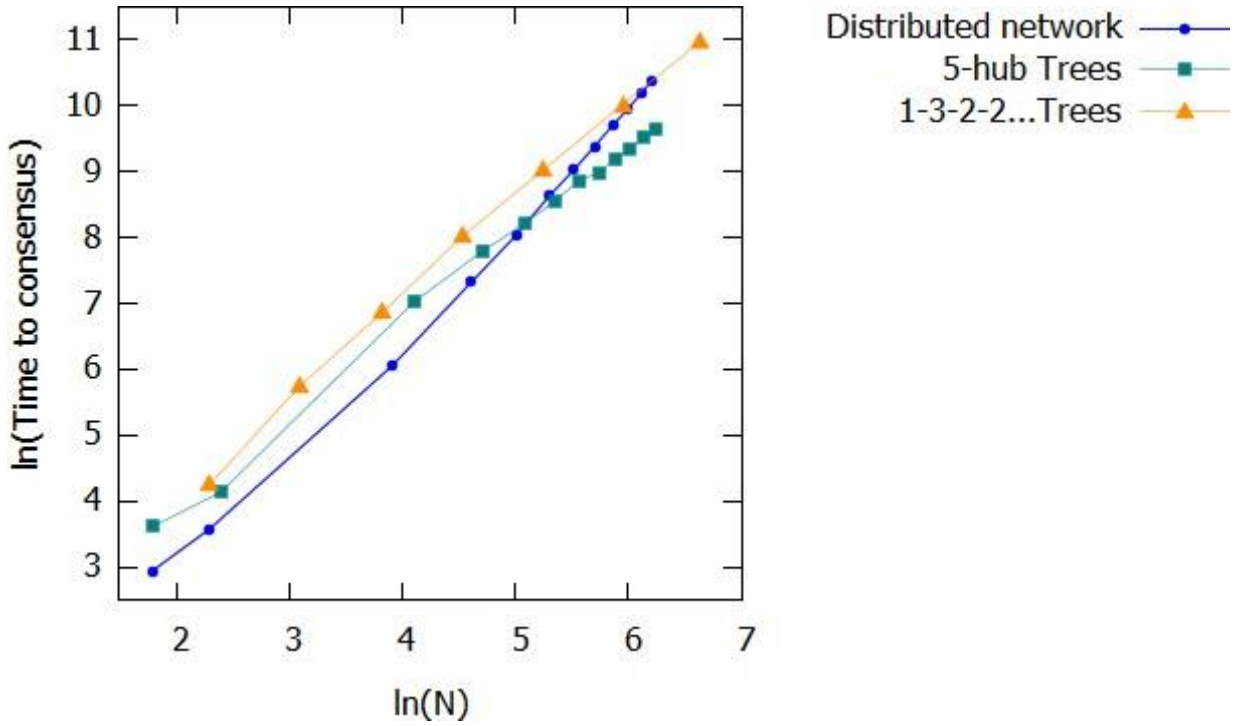


Рис. 3.11 Результати моделювання для різних типів топології. Розподіл законних користувачів / зловмисників на початковій стадії становить 50/50. Ймовірність регенерації для вузла дорівнює 0,5. Результати усереднюються за 100 експериментів.

Таким чином, ми бачимо, що для мереж менших розмірів децентралізований підхід дає більш швидкий результат, а з ростом числа користувачів – погіршується. Однак слід врахувати і інший параметр. Кількість законних користувачів, яких було виключено з мережі. Очевидно, що така ситуація можлива лише у ієрархічних структурах (рисунок 3.12), і для розподіленої мережі це значення буде дорівнює нулю для будь-якого розміру мережі [34].

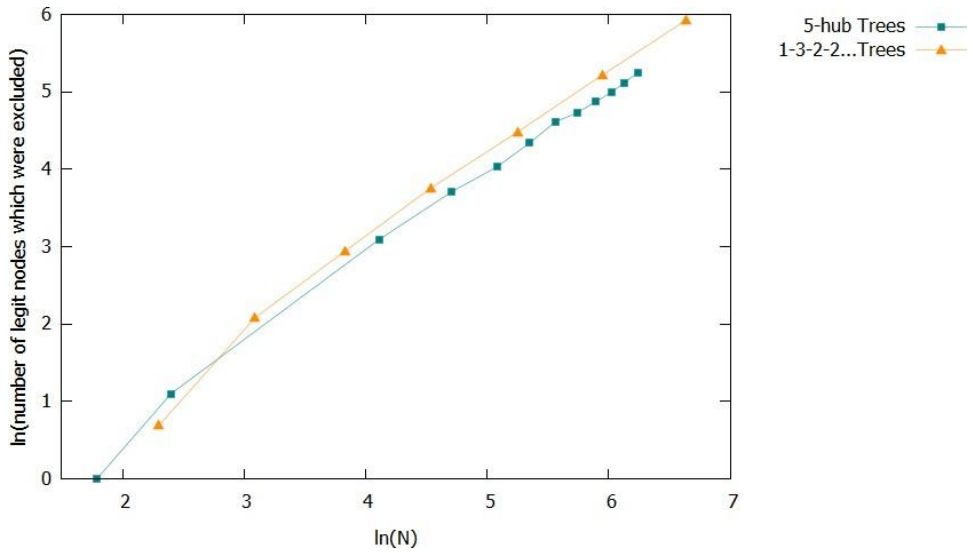


Рис. 3.12 Результати моделювання для топологій дерева. Залежність кількості законних вузлів, які були виключені з розміру мережі. Розподіл законних користувачів / зловмисників на початковій стадії становить 50/50. Ймовірність регенерації для вузла дорівнює 0,5.

Висновки до розділу 3

1. У даному розділі наведена *удосконалена* модель децентралізованої інфраструктури відкритих ключів із використанням технології blockchain, яка відрізняється від існуючих тим, що дозволяє надійно реалізувати модель довіри, сконцентрованої навколо користувача, що дозволяє використовувати її для побудови системи електронного голосування.

Переваги запропонованої децентралізованої ІВК полягають у наступному [33]:

- значне зниження витрат на утримання ієрархічної структури уповноважених на сертифікацію;
- користувачі самостійно контролюють свої ідентифікаційні дані і здатні негайно повідомити про необхідність їх коригування (наприклад, у випадку компрометації);
- нівелювання загрози «man in the middle»;
- зникнення «цілі» для спрямованої атаки. На відміну від ієрархічної структури, коли головними мішенями для зловмисників були центри

сертифікації ключів, в даному випадку відсутня явна ціль для атаки, оскільки записи зберігаються розподілено і, по суті, зловмисник змушений атакувати всю мережу, а не конкретний вузол;

- запропонована система може бути використана не тільки безпосередньо для послуги електронного підпису, але також для забезпечення електронної ідентифікації громадян та для системи електронного голосування;
- вихід з ладу одного або декількох вузлів не призведе до зупинки системи;
- відсутність необхідності робити і зберігати резервні копії. Надійне збереження резервних копій виступає однією із головних вимог для ієрархічної структури PKI;
- інтероперабельність системи полягає в тому, що сертифікати, випущені різними уповноваженими на сертифікацію можуть легко використовуватися в одній системі;
- легка масштабованість, пояснюється тим, що додавання нового користувача (нового вузла) відбувається без змін основних принципів функціонування архітектури;
- резильєнтність системи ІВК на базі технології blockchain буде перевищувати аналогічний показник для централізованої системи.

2. Енергетичні витрати, необхідні для реалізації атаки на децентралізовану систему становитимуть 50% від обчислювальної потужності такої системи. Порушнику необхідно буде атакувати всю систему. Відповідно для того, що б мати 50% шанс на успіх у вирішенні одного блоку, йому необхідно буде мати у своєму розпорядженні обчислювальною потужністю рівної обчислювальної потужності всієї іншої системі. Крім того рекомендація 3-5 ступеневої підтвердження різко і значно знижує його шанси, адже для успішної реалізації атаки йому буде необхідна обчислювальна потужність, яка істотно превишаюшает обчислювальну потужність всієї системи. Таким чином, можна зробити висновок, стійкість системи підвищується з ростом числа вузлів (користувачів).

3. Застосування викладеного підходу дозволить полегшити перехід на нові алгоритми підписів, зокрема на постквантові, в яких стійкість залежить не від криптоперіода ключа (3 роки, 5 років), а від кількості накладених підписів (наприклад, в hash-based підписах). Виходячи з цього, технологія blockchain дозволить більш раціонально управляти сертифікатами відкритих ключів.

4. Наведені результати часових оцінок для формування децентралізованої PKI. Оцінки були отримані для двох ієрархічних топологій мереж, таких як дерево із ступенем 3 для кожного вузла та «дерево з п’ятьма хабами». Також були отримані оцінки для однієї розподіленої мережі, представленої повнозв’язним графом. За результатами оцінок зроблені висновки, що незважаючи на те, що для мереж менших розмірів децентралізований підхід дає більш швидкий результат, а з ростом числа користувачів – погіршується, децентралізовані мережі виступають перспективними з тієї точки зору, що в них виключається можливість відкидання легітимних користувачів.

5. Основні положення даного розділу викладені у публікаціях автора [33-37].

РОЗДІЛ 4

ЕЛЕКТРОННА СИСТЕМА ТАЄМНОГО ГОЛОСУВАННЯ З ВИКОРИСТАННЯМ ПРИНЦИПІВ РОЗВИТКУ ДЕЦЕНТРАЛІЗОВАНИХ ТЕХНОЛОГІЙ

4.1 Принципи функціонування електронних систем голосування

Система електронного голосування може бити побудована за умови надійної реалізації таких базових послуг, як електронний підпис та електронна ідентифікація.

Електронне голосування більш зручне для кінцевих користувачів, оскільки існує можливість голосувати, не виходячи з дому, що підвищує активність потенційних виборців. Забезпечення електронного голосування є більш економічно вигідним, оскільки замість того, щоб постійно друкувати бюлетені, достатньо один раз розробити систему. Крім того, за умови, що ніхто не може втручатися в програму на пристрої для голосування, знижується вірогідність корупційної складової, адміністративного тиску та людських факторів. Важливою перевагою електронного голосування є також наявність можливостей для виборців перевірити правильність врахування їхнього голосу. Однак, з іншого боку дистанційне волевиявлення викликає низку специфічних проблем, які перешкоджають цілісності виборів. Наприклад, віддалено, набагато складніше провести процедуру автентифікації виборця або переконатися, що ніхто не вплинув на процес голосування [50-53]. Наразі електронне голосування є повністю законним або частково застосованим у багатьох країнах світу [38].

Виборчий процес – це здійснення суб’єктами, виборчих процедур, передбачених Конституцією України [43], Законом України “Про вибори депутатів Верховної Ради Автономної Республіки Крим, місцевих рад та сільських, селищних, міських голів” [44], Законом України “Про вибори президента України” [45] а також прийнятими відповідно до них іншими

актами законодавства.

Виборчий процес здійснюється на засадах [50-53]:

1. законності та заборони незаконного втручання будь-кого у цей процес;
2. політичного плюралізму;
3. публічності і відкритості;
4. рівності суб'єктів виборчого процесу перед законом;
5. рівності прав усіх кандидатів;
6. свободи передвиборної агітації, рівних можливостей доступу до засобів масової інформації незалежно від форми власності;
7. неупередженості органів державної влади, органів місцевого самоврядування, їх посадових і службових осіб, керівників підприємств, установ і організацій до місцевих організацій партій, кандидатів у депутати та кандидатів на посаду сільського, селищного, міського голови.

Виборчий процес включає такі етапи [50-53]:

1. утворення виборчих округів;
2. утворення виборчих дільниць;
3. формування складу територіальних виборчих комісій, утворення дільничних виборчих комісій;
4. складання списків виборців, їх перевірка та уточнення;
5. висування та реєстрація кандидатів у депутати та кандидатів на посаду сільського, селищного, міського голови;
6. проведення передвиборної агітації;
7. голосування у день виборів;
8. підрахунок голосів виборців, встановлення підсумків голосування і результатів виборів.

У випадках, передбачених Законами, виборчий процес включає також такі етапи [50-53]:

— повторне голосування;

— підрахунок голосів виборців, установлення підсумків повторного голосування і результатів.

Виборчий процес завершується офіційним оприлюдненням результатів.

Суб’єктами виборчого процесу є:

— виборці;

— Центральна виборча комісія, виборчі комісії, сформовані (утворені) відповідно до нормативних документів;

— кандидати;

— місцеві організації партій, які висунули кандидатів;

офіційні спостерігачі від місцевих організацій партій, які висунули кандидатів.

4.2 Обґрунтування вимог до системи електронного голосування

Система електронного голосування – це сукупність взаємопов'язаних правил, методів, процесів, засобів і технологій, а також правових норм, що в сукупності забезпечують і регулюють дистанційне легітимне волевиявлення авторизованих користувачів(виборців) [50].

Коректна реалізація всіх вищезазначених вимог не можлива лише технічними засобами або лише нормативним регулюванням. Система електронного голосування не залежно від її архітектури повинна складатися із взаємопов’язаних частин.

На рисунку 4.1 наведені складові частини (підсистеми/рівні) системи електронного голосування:

— нормативно-правовий рівень (Закони та інші нормативно-правові документи);
— організаційний рівень (архітектура системи електронного голосування);
— рівень процесів (порядок та процедури взаємодії всіх сторін);
— технологічний рівень (методи, засоби, протоколи, технології).

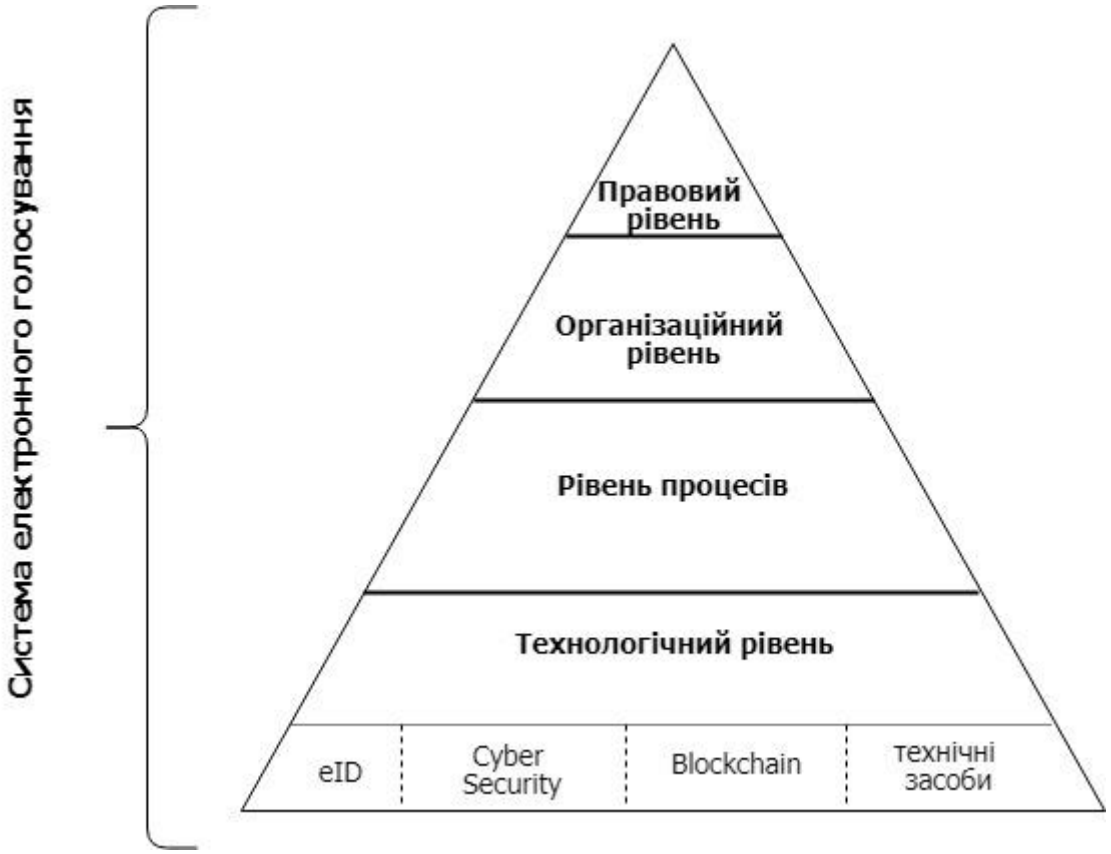


Рис. 4.1 Рівні / підсистеми електронного голосування

Можна виділити такі обов'язкові вимоги безпеки систем електронного голосування [50-53]:

— ніхто, крім виборця, не повинен знати його вибору;
— лише легітимні виборці можуть голосувати, крім того, вони повинні мати можливість проголосувати лише один раз;
— рішення виборця не може бути явно або таємно змінено будь-ким (крім, можливо, самого виборця).

Додатково до них, висуваються бажані вимоги [52]:

— кожен легітимний виборець може мати можливість перевірити, чи правильно врахований його голос;
— кожен легітимний виборець може мати можливість змінити свою думку і вибір протягом визначеного періоду часу;
— система повинна бути захищена від продажу голосів виборцями;

— у разі неправильного підрахунку голосів кожен легітимний виборець повинен мати можливість повідомити про це систему, не виявляючи своєї особистості;
— повинна бути забезпечена неможливість відстежити, звідки віддалено проголосував виборець;
— повинна бути забезпечена автентифікація оператора;
— підтримка системи не повинна вимагати великих ресурсів;
— система повинна бути відмовостійкою у разі технічних несправностей (втрата електроживлення), ненавмисних (втрата виборцем ключа) і зловмисних (навмисного маскування себе як іншого виборця, DoS / DDoS) атак.

Основні загрози для систем такого типу:

— легітимний виборець не може проголосувати;
— втрата анонімності виборців;
— реєстрація неіснуючих виборців;
— використання пустих бюлетенів виборців, які зареєструвалися, але не взяли участі у виборах.

4.3 Аналіз існуючих протоколів електронного голосування

Таємні протоколи голосування – протоколи обміну даними для реалізації безпечного, таємного електронного голосування через Інтернет з використанням комп'ютерів, телефонів або інших спеціальних пристроїв.

Простий алгоритм електронного голосування (рисунок 4.2) [39], по суті, являється процесом обміном повідомленнями підписаними електронними підписам між виборчим комітетом і виборцями.

Тут і далі введемо наступні позначення:

A – агентство електронного голосування;

E – виборець;

B – цифровий виборчій бюлетень.

Алгоритм складається із шести основних етапів.

Eman 1. *A* розміщує списки можливих виборців.

Eman 2. Користувачі, включаючи *E*, оголошують про своє бажання голосувати.

Eman 3. *A* розміщує списки легітимних виборців.

Етапи 1-3 є необхідними. За результатами цих етапів визначається та оприлюднюється кількість легітимних учасників. При цьому існує вірогідність, що деякі з учасників можуть не взяти участь. В подальшому ці етапи будуть розглядатися за один – "затвердження списків".

Eman 4. *A* генерує власний відкритий ключ (*a_public*) і особистий ключ (*a_private*). Особистий ключ надійно зберігається *A*, відкритий публікується для широкого доступу. Таким чином, кожен може зашифрувати повідомлення, використовуючи опублікований відкритий ключ, але тільки *A* може розшифрувати отримане повідомлення.

Eman 5 включає наступне:

1. *E* генерує свої власні відкритий (*PK*) і особистий (*SK*) ключі та публікує відкритий ключ. Таким чином, кожен може перевірити документ *E*, але підписати його може тільки сам *E*. Цей крок може бути пропущений, якщо *A* вже знає електронні підписи виборців (наприклад, вони були створені під час реєстрації в системі);
2. *E* формує цифровий виборчій бюлетень *B*, в якому висловлює свою волю;
3. підписує повідомлення власним особистим ключем (*SK*);
4. шифрує повідомлення за допомогою відкритого ключа *A* (*a_public*);
5. надсилає зашифроване повідомлення *A*.

Eman 6 включає наступне:

1. *A* приймає повідомлення;
2. розшифровує їх за допомогою загальнодоступних *PK* виборців;
3. підраховує голоси та публікує результати.

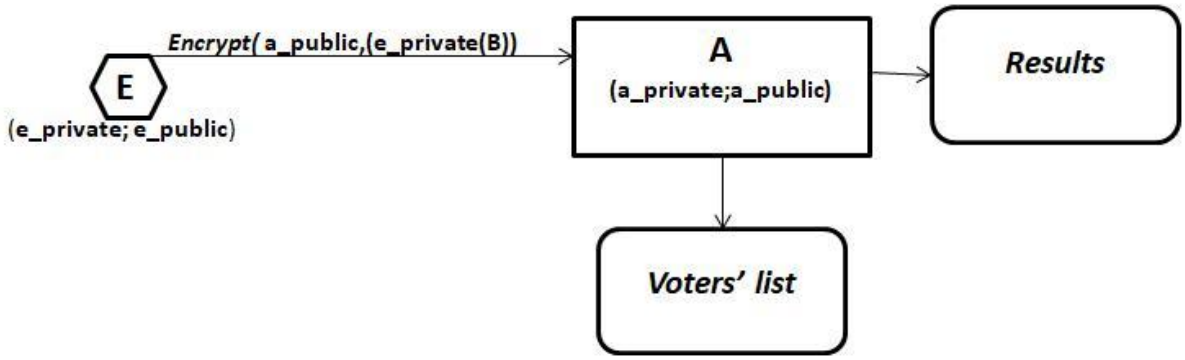


Рис. 4.2 Простий протокол електронного голосування

Надійної реалізації такого простого протоколу достатньо для забезпечення захисту системи від зовнішнього втручання, шахрайства з голосуванням і дискредитації легітимних виборців. Недоліком його є необхідність повної довіри до *A* з боку виборців, оскільки робота Агентства не контролюється ніким. Виборець може надати доказ голосування, але він не може переконатися, що *A* правильно врахував або навіть отримав його бюлетень. Таким чином, описаний тривіальний метод може застосуватися тільки в спільнотах, де кожен довіряє один одному і Агентству, відповідальному за підрахунок голосів.

Існує декілька відомих модифікацій згаданого протоколу. Перший - Протокол двох агентств, що називається також протоколом Нурмі-Салома-Сантіна (Nurmi-Saloma-Santina) [40, 50-51]. Основна ідея якого полягає у тому, щоб замінити одну виборчу установу на дві, для забезпечення взаємного контролю між ними. Таким чином, в системі з'являється додаткова сторона *V*, яка є валідатором, чиї обов'язки включають підготовку списків, а також прийняття або недопущення учасника до голосування. Крім того, згідно з цим протоколом *A* має опублікувати список прийнятих цифрових бюлетенів. В результаті *A* не може згодом відмовити в отриманні повідомлення від *E* і кожен виборець може перевірити, чи правильно його голос був врахований, що виключає проблему відсутності контролю над *A*. З іншого боку, існує можливість змови між *A* та *V*, що призведе до можливих маніпуляцій з результатами. Крім того, існує проблема "мертвих душ". Якщо *V* внесе до

списку завідомо неіснуючих виборців, то *A* зможе фальсифікувати бюлетені від «мертвих душ».

У 1992 році була розроблена схема Fujioka-Okamoto-Ohta [41], яка базується на протоколі двох агентств і сліпого криптографічного підпису. Протокол вимагає попередньо обраного методу маскуючого шифрування, згідно з яким виборець відправляє бюлетень валідатору. Маскуюче шифрування – це особливий тип шифрування, який дозволяє переконатися, що документ є автентичним і підписаний уповноваженим користувачем, але не дозволяє виявити дані, що містяться в ньому. Ця схема частково вирішує проблему змови двох установ. Однак це ускладнює протокол.

Однією з найпопулярніших версій вищезгаданого протоколу є протокол Sensus [47]. При його коректній реалізації, навіть якщо агентствам вдасться дійти до змови, *A* не зможе ідентифікувати виборців. Незважаючи на те, що *A* все ще має можливість «не отримувати» повідомлення, він більше не може ігнорувати повідомлення спеціально від «небажаних» виборців. Залишається тільки проблема голосування виборців, які не вийшли на вибори.

Щоб уникнути недоліків Fujiok-Okamoto-Ohta, у тому числі його модифікацій, необхідне подальше ускладнення алгоритму, що призводить до труднощів практичної реалізації (наприклад, протокол He-Su [42]).

На даний момент протокол Fujiok-Okamoto-Ohta (а також його модифікації, включаючи Sensus) є одним з найбільш перевірених протоколів дистанційного електронного голосування. Саме його варіація застосовувалася на електронних виборах в Естонії [48, 49].

4.4 Принципи побудови децентралізованої системи голосування із використанням технології blockchain

Процес голосування складається з наступних етапів:

1. Формування списків виборців.
2. Голосування.
3. Підрахунок голосів.

Тут і далі *CA* - центр сертифікації (або довірені вузли у децентралізованій PKI).

Архітектура (рисунок 4.3) складається із двох рівнів та базується на раніше запропонованій децентралізованій PKI. Користувачі використовують існуючі ключові пари. Центри сертифікації (довірені вузли) об'єднуються в мережу Blockchain (CAs' Blockchain Ledger) – нижній рівень. На верхньому рівні знаходиться децентралізована інфраструктура для електронного голосування (Decentralized e-voting Infrastructure). Представництва Агентства електронного голосування аналогічно до центрів сертифікації ключів об'єднуються в окрему мережу blockchain (Ais' Blockchain Ledger) Необхідно зазначити, що для таких мереж немає необхідності застосовувати складні та енергоємні протоколи консенсусу, оскільки обидві мережі поєднує довірені («чесні») вузли [50].

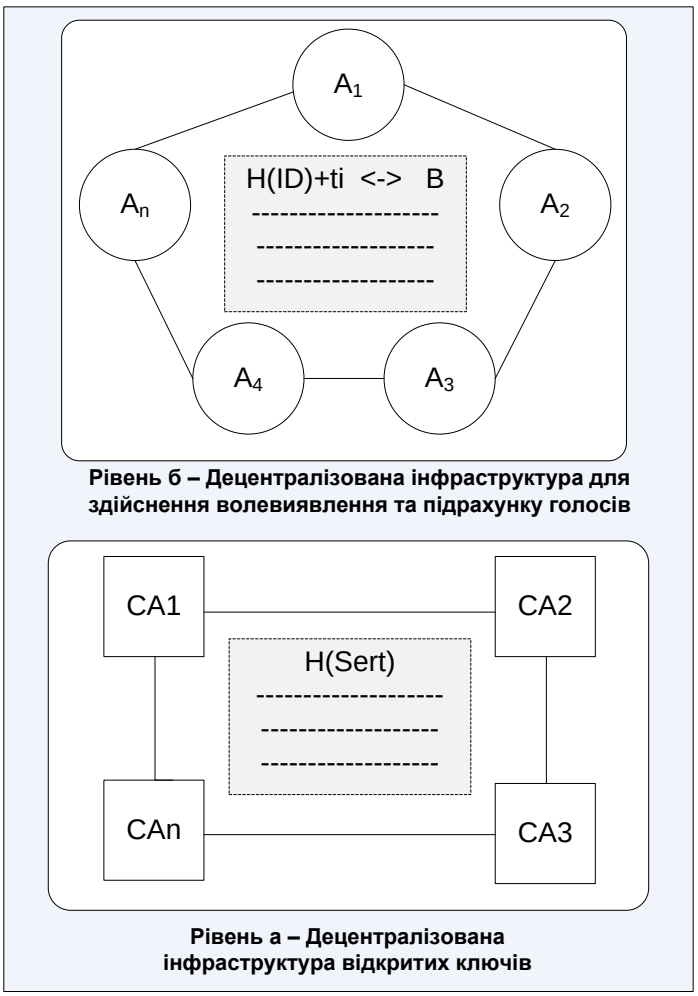


Рис. 4.3 Дворівнева архітектура системи електронного голосування

Перший етап: формування списків виборців.

Алгоритм формування списків виборців наведений на рисунку 4.4.

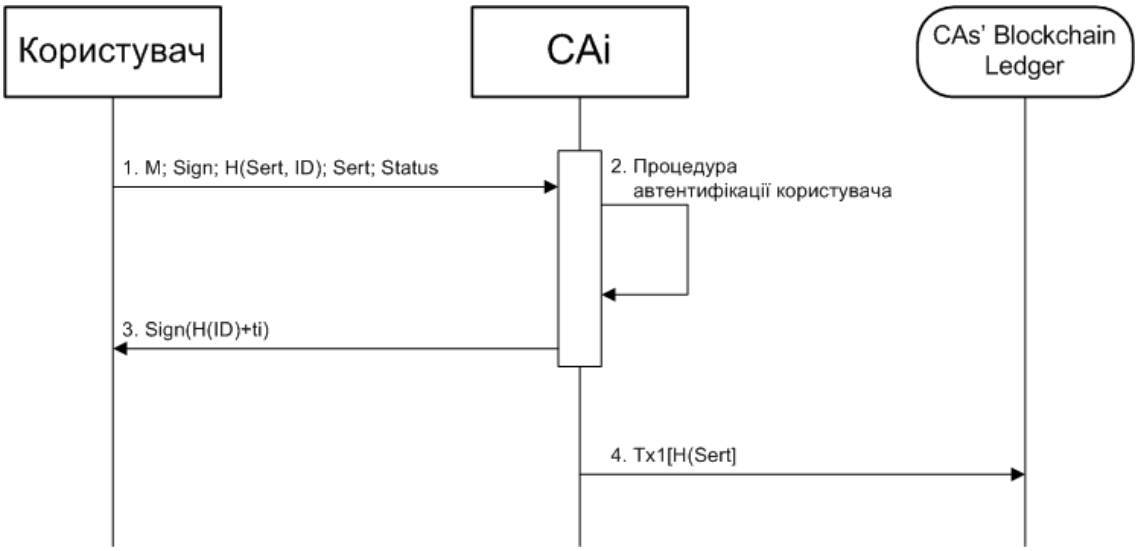


Рис. 4.4 Алгоритм формування списків виборців

Алгоритм формування списків виборців складається із наступних кроків [50].

1. Користувач надсилає запит до довіреного вузла на включення його до списку виборців. Запит формується у вигляді транзакції, яка може бути в цілому використана в децентралізованій PKI:

$$M; Sign; H(Sert, ID); Sert; Status,$$

де $M = H(ID)$

2. Орган з сертифікації (CAi), який є представництвом Агентства, на підставі даних, отриманих під час первинної ідентифікації, перевіряє легітимність виборця (фактично проходить процедура автентифікації виборця). Під час перевірки орган з сертифікації також перевіряє чи не був даний користувач раніше включений до списку легітимних виборців. Таку перевірку можливо здійснити на основі даних із розподіленого реєстру мережі Blockchain (CAs' Blockchain Ledger).

3. Якщо процедура автентифікації пройдена успішно, орган з сертифікації у відповідь на запит, надсилає виборцю його мітку, підписану власним особистим ключем

$$Sign(H(ID)+t_i \ ,$$

де – t_i є ідентифікаційною позначкою (міткою).

4. Орган із сертифікації формує транзакцію Tx1, в яку включає геш-значення від сертифікату виборця (H(Sert)). Учасники мережі blockchain (CAs' Blockchain Ledger) досягають консенсусу щодо включення такої транзакції до розподіленого реєстру. Таким чином, коли вичерпався час, виділений на формування списків легітимних виборців, у цьому блокчейні створено деперсоналізований список потенційних легітимних виборців. Після закінчення періоду, призначеного для формування списків законних виборців, всі довірені вузли передають Агентству дані про мітки, які вони видали виборцям (без відомостей про відповідність між міткою та користувачем):

$$H(ID)+t \ .$$

Таким чином, Агентство отримує список всіх зареєстрованих легітимних виборців, але виборці зберігають свою анонімність.

Другий етап: голосування:

Алгоритм голосування наведений на рисунку 4.5.

Алгоритм голосування складається із наступних кроків [50].

1. Виборець, який отримав підтвердження від довіреного вузла, формує повідомлення зі своїм рішенням/вибором і надсилає Агентству наступний набір даних:

$$H(ID)+ti;\ encrypt\ (M^*)$$

де – $M^*= a\_pub, H(ID)+t, B$

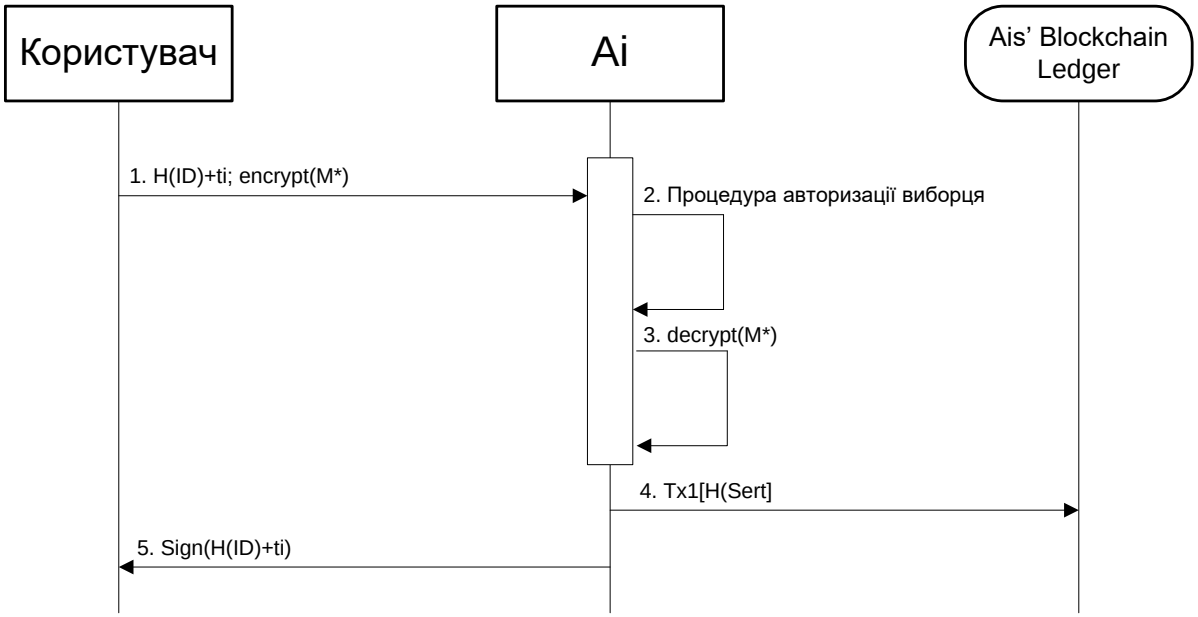


Рис. 4.5 Алгоритм голосування

2. По зовнішній мітці *H (ID) + ti Ai* може ідентифікувати, що голос прийшов саме від легітимного виборця (процедура авторизації виборця).
3. Якщо процедура авторизації пройшла успішно, то використовуючи власний e_private, Ai розшифровує повідомлення та проводить перевірку того, чи зовнішня позначка відповідає тій, яка була зашифрована.
4. Якщо вони збігаються, Ai формує транзакцію Tx2, в яку включає відповідність між *H(ID)+t і B*. Учасники мережі blockchain (Ais' Blockchain Ledger) досягають консенсусу щодо включення такої транзакції до розподіленого реєстру.

При цьому, Агентство, як і будь-який зовнішній спостерігач, досі не знає, хто саме серед легітимних виборців робить цей вибір, таким чином виборці є анонімними без використання сліпих підписів.

5. Якщо перевірки 2 і 3 пройшли успішно, *Ai* в якості підтвердження прийняття його голосу надсилає виборцю його мітку підписану власним особистим ключем.

Перед підрахунком голосів, необхідно виконати наступні перевірки:

$$N(H(Sert))=N(H(ID)+t)$$

Це означає, що кількість геш-значень сертифікатів (N (H(Sert))) в мережі CAs' Blockchain Ledger, організованому між довіреними вузлами, повинна відповідати кількості H (ID) + t, що були надіслані в Агентство довірчими вузлами. Таким чином, виключається можливість A не враховувати голоси легітимних виборців:

$$N(H(ID)+t) \geq N(B)$$

Це означає, що кількість поданих бюлетенів не повинна перевищувати кількість зареєстрованих виборців. Дана перевірка виключає можливість використання «мертвих душ». Якщо всі перевірки є успішними, проводиться підрахунок голосів.

Третій етап: підрахунок голосів.

У Ais' Blockchain Ledger – мережі blockchain, організованій між представництвами Агентства, формується остаточний список відповідності між мітками виборців та їхнім вибором. Потім кожен користувач перевіряє, чи правильно враховано його голос. У разі помилки виборці повідомляють про це. Підрахунок голосів здійснюється автоматично.

4.5 Комплекс для проведення досліджень криптографічних властивостей технології blockchain

З точки зору впровадження децентралізованої системи електронного голосування в Україні важливо забезпечити її інтероперабельність із існуючими системами електронної ідентифікації, зокрема BankID, MobileID, ідентифікація на основі електронного підпису.

4.5.1 Архітектура децентралізованої системи голосування

Архітектура децентралізованої системи електронного голосування є дворівневою і складається із двох неперетинаючихся мереж Blockchain, нижня мережа представляє собою децентралізовану інфраструктуру ідентифікації, верхня мережа – децентралізована інфраструктура для здійснення волевиявлення (рисунок 4.6).

Децентралізована інфраструктура ідентифікації виборців (ДІ eID) має

забезпечувати процедуру надійної ідентифікації користувачів та формування списків легітимних виборців. Вона складається із провайдерів послуг ідентифікації громадян (далі - *IdP*, провайдери). Необхідно забезпечити реалізацію процедури ідентифікації за допомогою:

1. засобів BankID
2. засобів MobileID
3. електронного паспорта громадянина
4. електронного підпису

— програмний носій електронного підпису

— апаратний носій електронного підпису

Відповідно, в ролі *IdP* можуть виступати:

1. банківські установи
2. мобільні оператори
3. центри міграційної служби (центри надання адміністративних послуг – ЦНАП)
4. центри сертифікації ключів національної системи ЕЦП.

Мережа провайдерів ідентифікації формується поза межами децентралізованої системи електронного голосування. Кожен *IdP* має попередньо сформовану локальну базу даних своїх користувачів, яка містить їхні ідентифікаційні дані та, можливо, локальні ідентифікатори. Відповідальність за надійне збереження та коректне викоРисуноктання локальних баз даних покладається на *IdP* [50, 51].

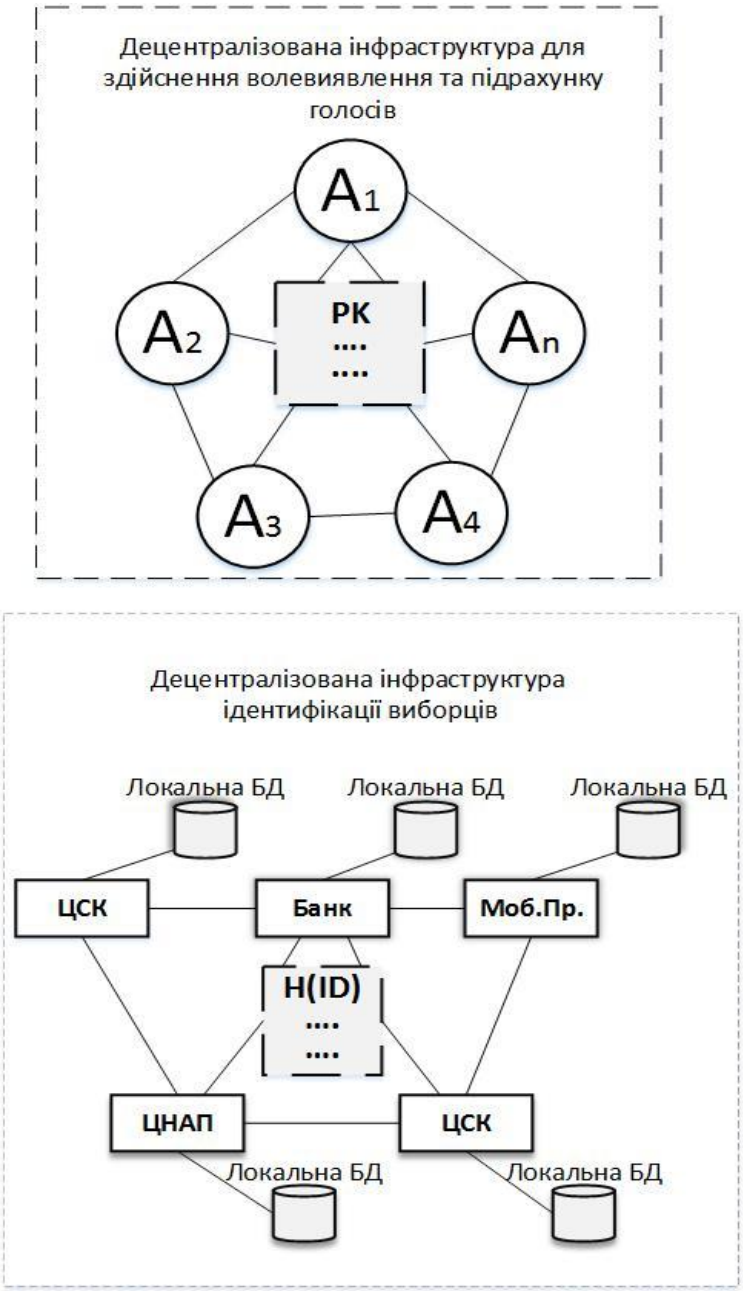


Рис. 4.6 Архітектура децентралізованої системи електронного голосування

Для організації інфраструктури ідентифікації в рамках децентралізованої системи електронного голосування, *IdP* об'єднуються в окрему приватну мережу blockchain (private permissioned blockchain). В даній мережі кожен із *IdP* виступає вузлом-валідатором. Необхідно зазначити, що для такої мережі немає необхідності застосовувати складні та енергоємні протоколи консенсусу, оскільки мережа поєднує довірені («чесні») вузли [50, 51].

Децентралізована інфраструктура для здійснення дистанційного волевиявлення та підрахунку голосів має забезпечувати процес дистанційного волевиявлення зареєстрованих (авторизованих) легітимних виборців та процес підрахунку голосів. Додатково в даній інфраструктурі повинні бути організовані процеси генерації гаманців для зареєстрованих виборців, а також процеси реєстрації (генерації гаманців) кандидатів. Для організації інфраструктури дистанційного волевиявлення в рамках децентралізованої системи електронного голосування представництва відповідальних за проведення виборчого процесу (A1, A2,...,An), подібно до провайдерів ідентифікації, об'єднуються в окрему приватну мережу blockchain (private permissioned blockchain), в якій кожен із Ai виступає вузлом-валідатором - в сукупності вони являють собою децентралізоване Агентство (A). Аналогічно до верхньої мережі blockchain, у нижній також немає необхідності застосовувати складні та енергоємні протоколи консенсусу, оскільки мережа поєднує довірені («чесні») вузли. Вузли-валідатори формують гаманці для легітимних виборців та проводять процедуру автентифікації виборців. Також вони відповідають за процес формування гаманців для альтернатив (кандидатів) [51].

4.5.2 Протокол голосування у децентралізованій системі електронного голосування

Протокол голосування у децентралізованій системі електронного голосування складається з наступних етапів [51]:

I. Формування списків легітимних виборців у децентралізованій інфраструктурі ідентифікації виборців

II. Генерація гаманців легітимних виборців у децентралізованій інфраструктурі для здійснення дистанційного волевиявлення та підрахунку голосів

III. Реєстрація кандидатів у децентралізованій інфраструктурі для здійснення дистанційного волевиявлення та підрахунку голосів

IV. Автентифікація виборців у децентралізованій інфраструктурі для здійснення дистанційного волевиявлення та підрахунку голосів

V. Голосування у децентралізованій інфраструктурі для здійснення дистанційного волевиявлення та підрахунку голосів

VI. Підрахунок голосів у децентралізованій інфраструктурі для здійснення дистанційного волевиявлення та підрахунку голосів

Реалізація даного протоколу із використанням технології blockchain дає можливість в залежності від потреб цільової системи змінювати порядок деяких етапів, а саме четвертого та п'ятого без втрати надійності. Пряма послідовність (четвертий-п'ятий) передбачає допуск до безпосередньо процесу голосування лише автентифікованих користувачів (легітимних виборців). Зворотна послідовність (п'ятий-четвертий) допускає участь у процесі голосування потенційних порушників (нелегітимних виборців), проте завдяки особливостям реалізації механізму консенсусу транзакції, а відповідно і голоси нелегітимних користувачів, враховані не будуть. Це базується на тому твердженні, що в будь-якій мережі blockchain транзакція вважається підтвердженою тільки якщо виконані обидві умови, а саме:

— формат та підписи транзакції перевірені;

— вузли-валідатори досягли консенсусу щодо включення даної транзакції до ланцюжку блоків [51].

Принципи побудови децентралізованої інфраструктури для здійснення дистанційного волевиявлення та підрахунку голосів не дозволяють вузлам-валідаторам включити в ланцюжок блоків транзакцію від нелегітимного виборця, оскільки не буде виконана перша умова (підпис транзакції не буде валідним).

Перший етап: формування списків легітимних виборців у децентралізованій інфраструктурі ідентифікації виборців.

Формування списків легітимних виборців відбувається у нижній мережі blockchain (у децентралізованій інфраструктурі ідентифікації виборців, ДІ eID).

Перед початком формування списків виборців, кожен потенційний виборець самостійно генерує собі ключову пару (*SK; PK*). Після цього він надсилає запит на включення його до списку виборців до одного із доступних

йому *IdP*, в якому у відкритому вигляді надає йому свої ідентифікаційні дані та свій відкритий ключ [51].

Формат запиту залежить від наявних каналів зв'язку між виборцем та *IdP*. Він може бути зроблений дистанційно через мережу Інтернет за умови існування надійного каналу зв'язку (рисунок 4.8) або такий ідентифікаційний запит може бути зроблений особисто потенційним виборцем в межах контрольованої зони *IdP*. Якщо запит здійснюється дистанційно, то відповідальність за дотриманням правил генерації ключової пари покладається на користувача. У випадку, коли запит робиться особисто в межах контрольованої зони, на *IdP* покладається відповідальність за дотримання умов генерації ключової пари користувача [51].

Якщо у потенційного виборця вже є згенерована ключова пара відповідно до вимог одного із провайдерів ідентифікації, він може використовувати її. В такому випадку у запит до провайдера має бути включений сертифікат відкритого ключа (рисунок 4.7) [51].

Якщо у потенційного виборця немає локального ідентифікатора у жодного із *IdP*, то він повинен пройти процедуру первинної ідентифікації у одного із *IdP* та тільки після цього бути включеним до списку легітимних виборців (рисунок 4.9). Процедура первинної ідентифікації має проводитися відповідно до правил конкретного *IdP* [51].

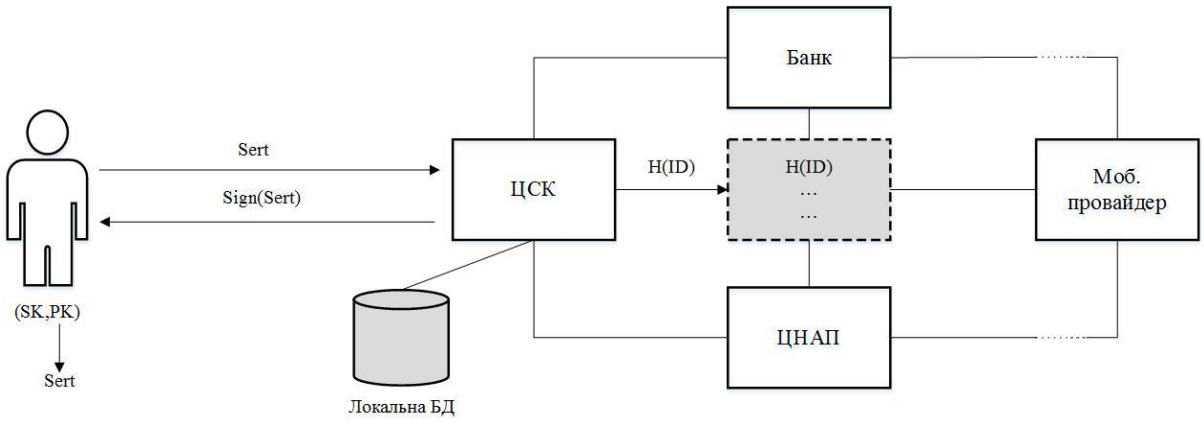


Рис. 4.7 Процедура ідентифікації на основі сертифікату

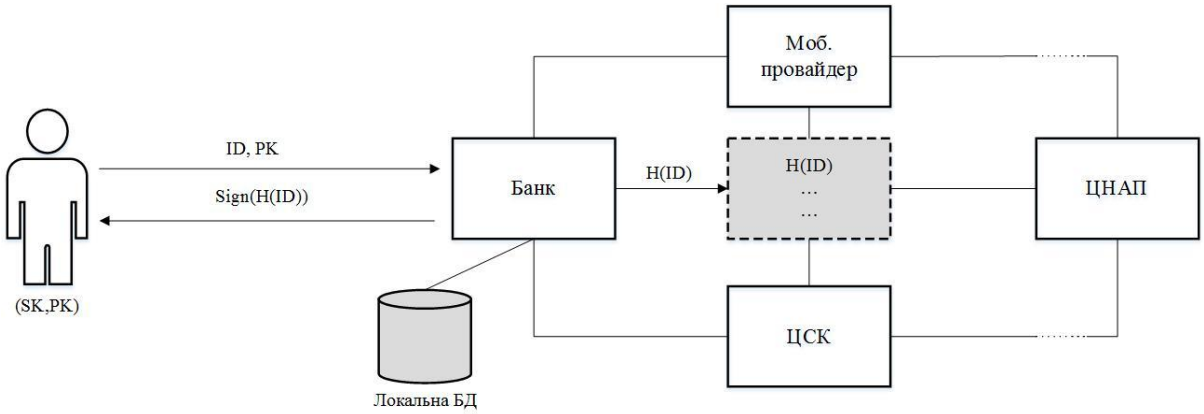


Рис. 4.8 Процедура ідентифікації на основі відкритого ключа (локального ідентифікатора)

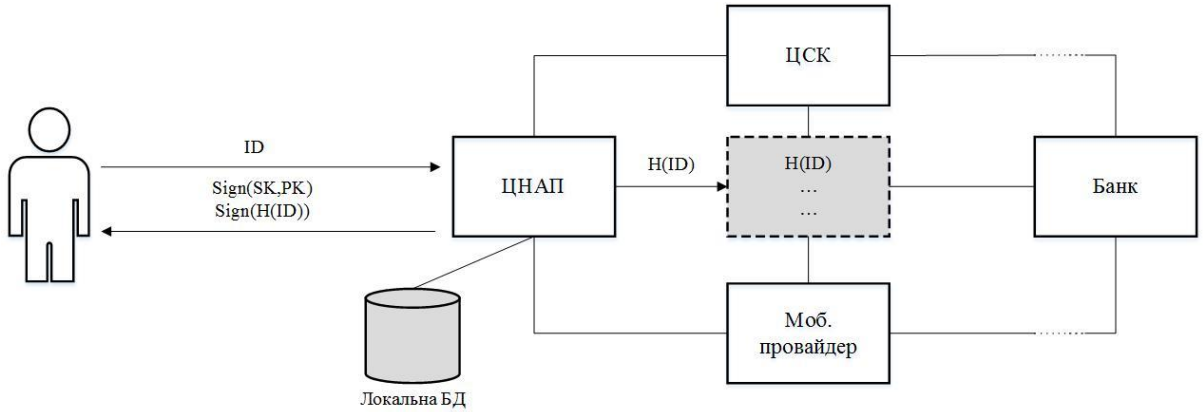


Рис. 4.9 Процедура ідентифікації на основі персональних даних

Алгоритм ідентифікації виборця в децентралізованій системі електронного голосування.

Алгоритм ідентифікації виборця залежить від початкових умов та наявних технічних засобів у виборця. Відповідно до таких умов можна виділити три типи виборців, процеси для яких розглянуті далі.

Перший тип – виборець, який на момент проведення процедури електронного голосування має дійсний сертифікат відкритого ключа (*Sert*), виданий довіреним центром сертифікації ключів (ЦСК). За умови, якщо такий ЦСК включений до ДІ eID він (ЦСК) може провести процедуру ідентифікації виборця в системі електронного голосування [51].

Для такого типу виборців алгоритм ідентифікації в системі електронного голосування виглядає наступним чином (рисунок 4.10).

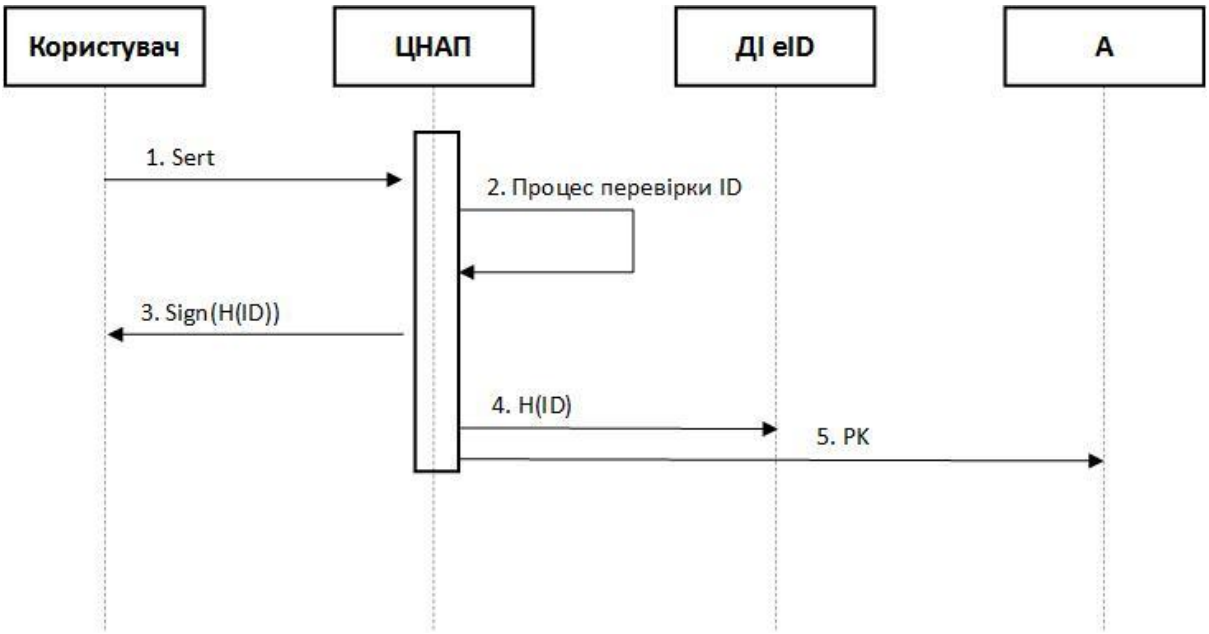


Рис. 4.10 Алгоритм ідентифікації на основі сертифікату відкритого ключа

1. Користувач формує запит на внесення його до списку легітимних виборців, в який включає свій сертифікат відкритого ключа (*Sert*) та направляє такий запит до ЦСК, який видавав йому сертифікат. Необхідно зазначити, що такий запит може бути зроблений дистанційно без використання надійного каналу зв'язку.

2. ЦСК на основі отриманого сертифікату відкритого ключа та ідентифікаційних даних із власної локальної БД проводить процес перевірки користувача, в разі якщо наявних ідентифікаційних даних в локальній БД провайдера ідентифікації недостатньо, він має змогу запросити додаткову інформацію у користувача. Під час перевірки ЦСК також перевіряє чи не був даний користувач раніше включений до списку легітимних виборців. Таку перевірку можливо здійснити на основі даних із розподіленого реєстру мережі blockchain (Blockchain ledger).

3. Якщо сукупність перевірок успішна, тобто користувач має право приймати участь у волевиявленні і він раніше не був внесений до списку

виборців іншим провайдером ідентифікації, то ЦСК в якості підтвердження включення користувача до списків легітимних виборців надсилає йому його деперсоналізовані ідентифікаційні дані, сформовані відповідно до заданого формату (*Sign(H(ID))*). Таке підтвердження також може бути передане через відкритий канал зв'язку.

4. ЦСК відправляє в нижню мережу blockchain деперсоналізовані дані такого користувача (*H(ID)*), які сформовані відповідно до заданого формату.

5. ЦСК по надійному каналу зв'язку надсилає відкритий ключ виборця (*PK*) у верхню мережу blockchain.

Другий тип виборця – виборець, який на момент проведення процедури електронного голосування має локальний ідентифікатор (*local ID*) у локальній базі даних одного із провайдерів ідентифікації, але не має згенерованої ключової пари (алгоритм ідентифікації на основі local ID наведений на рисунку 4.11). Наприклад користувач є клієнтом банку, який входить до списку провайдерів ідентифікації в децентралізованій системі електронного голосування (т.т. входить до нижньої мережі blockchain) [51].

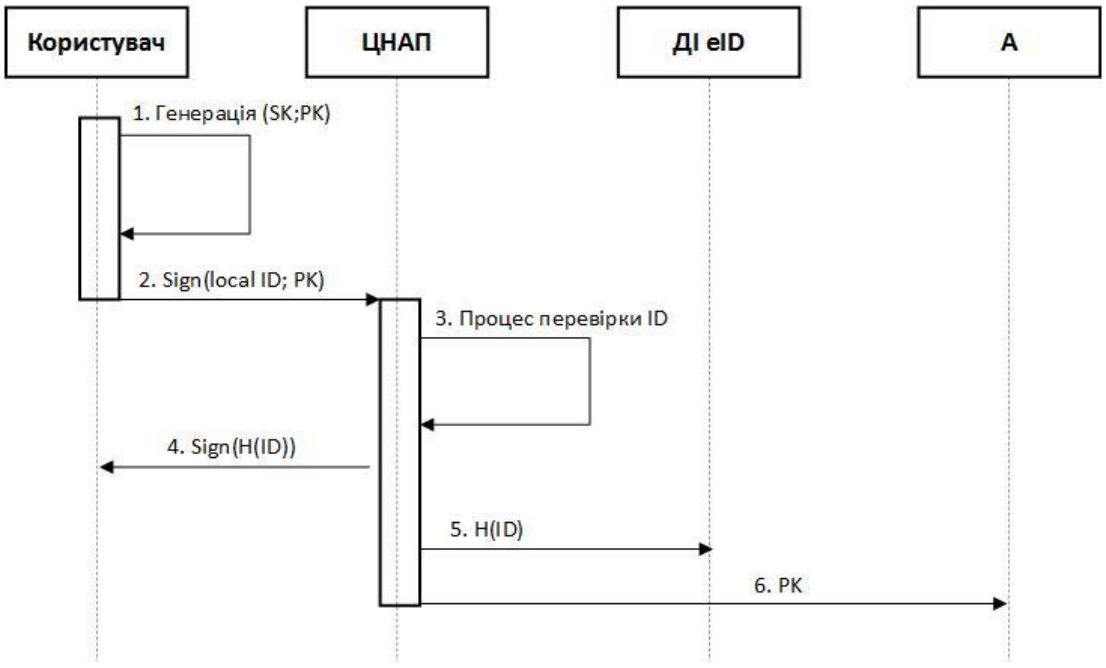


Рис. 4.11 Алгоритм ідентифікації на основі *local ID*

1. Користувач самостійно генерує власну ключову пару *(SK; PK)*. В даному випадку користувач самостійно несе відповідальність за дотримання всіх умов генерації ключової пари, а також за надійне збереження особистого ключа.

2. Користувач через захищений канал зв'язку надсилає банку (або іншому провайдеру ідентифікації) підписаний власним особистим ключем набір даних, який складається із його локального ідентифікатора в БД обраного провайдера (*local ID*) та свого відкритого ключа (*PK*).

3. Банк (або інший провайдер ідентифікації) на основі ідентифікаційних даних із власної локальної бази даних (БД) проводить процес перевірки користувача, в разі якщо наявних ідентифікаційних даних в локальній БД провайдера ідентифікації недостатньо, він має змогу запросити додаткову інформацію у користувача. Під час перевірки банк також перевіряє чи не був даний користувач раніше включений до списку легітимних виборців. Таку перевірку можливо здійснити на основі даних із розподіленого реєстру мережі blockchain (Blockchain ledger).

4. Якщо сукупність перевірок успішна, тобто користувач має право приймати участь у волевиявленні і він раніше не був внесений до списку виборців іншим провайдером ідентифікації, то банк в якості підтвердження включення користувача до списків легітимних виборців надсилає йому підписаний власним особистим ключем його деперсоналізовані ідентифікаційні дані, сформовані відповідно до заданого формату (*Sign(H(ID))*). Таке підтвердження також бути передане через відкритий канал зв'язку.

5. Банк відправляє в нижню мережу blockchain деперсоналізовані дані такого користувача (*H(ID)*), які сформовані відповідно до заданого формату.

6. ЦСК по надійному каналу зв'язку надсилає відкритий ключ виборця (*PK*) у верхню мережу blockchain.

Третій тип виборця – виборець, який на момент проведення процедури електронного голосування немає локального ідентифікатора (*local ID*) у

локальній базі даних жодного із провайдерів ідентифікації або виборець, який на момент проведення процедури електронного голосування має локальний ідентифікатор, проте немає можливості для самостійної генерації ключової пари (алгоритм ідентифікації на основі *ID* наведений на рисунку 4.12).

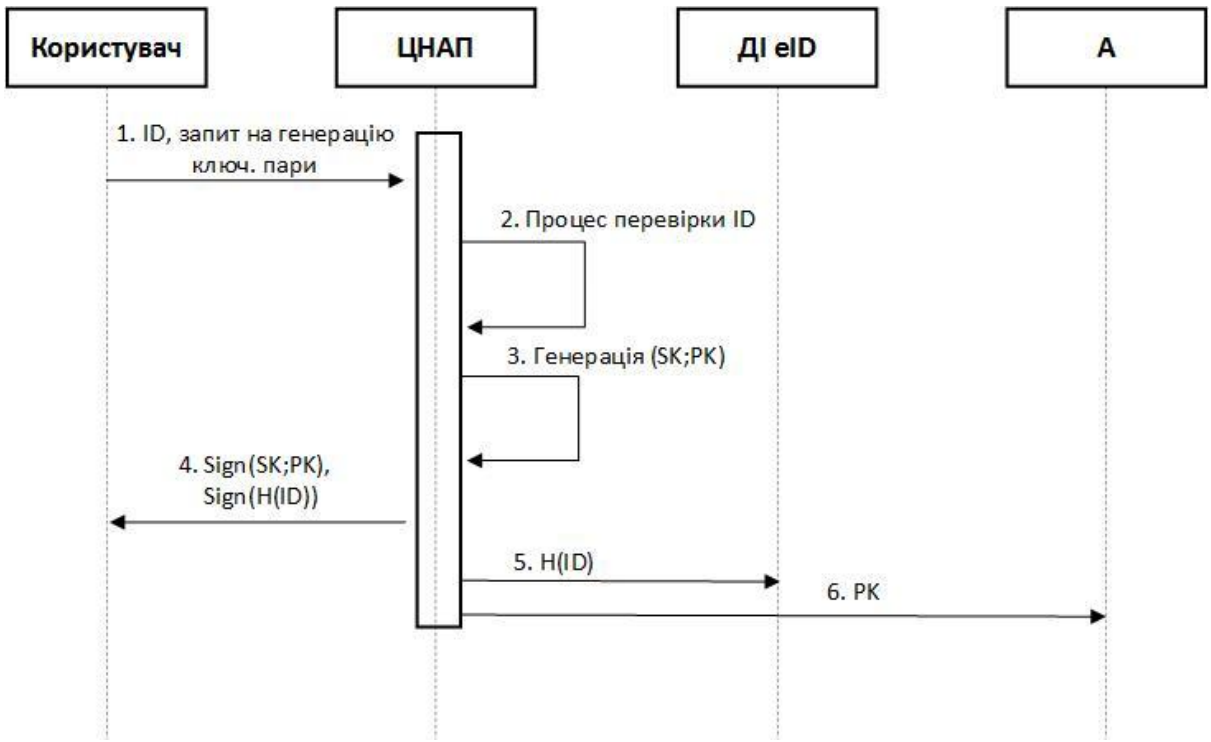


Рис. 4.12 Алгоритм ідентифікації на основі *ID*

1. Користувач робить запит на генерацію ключової пари у одного із провайдерів ідентифікації. При запиті користувач надає свої ідентифікаційні дані особисто.

2. ЦНАП (або інший провайдер ідентифікації) на основі отриманих ідентифікаційних даних проводить процес перевірки користувача, в разі якщо наданих (або наявних в локальній БД провайдера) ідентифікаційних даних недостатньо, він має змогу запросити додаткову інформацію у користувача. Під час перевірки банк також перевіряє чи не був даний користувач раніше включений до списку легітимних виборців. Таку перевірку можливо здійснити на основі даних із розподіленого реєстру мережі blockchain (Blockchain ledger).

3. ЦНАП (або інший провайдер) проводить процедуру генерації ключової пари. Генерація ключової пари відбувається безпосередньо в контрольованій зоні провайдера ідентифікації (наприклад ЦНАП). В даному випадку відповідальність за дотримання вимог генерації покладається на провайдера. Особистий ключ користувача передається безпосередньо йому на апаратному носії (оптичний диск/захищений носій ключової інформації).

4. Якщо сукупність перевірок успішна, тобто користувач має право приймати участь у волевиявленні і він раніше не був внесений до списку виборців іншим провайдером ідентифікації, то банк в якості підтвердження включення користувача до списків легітимних виборців надсилає йому підписаний власним особистим ключем його деперсоналізовані ідентифікаційні дані, сформовані відповідно до заданого формату (*Sign(H(ID))*). Таке підтвердження також бути передане через відкритий канал зв'язку.

5. ЦНАП відправляє в нижню мережу blockchain деперсоналізовані дані такого користувача (*H(ID)*), які сформовані відповідно до заданого формату.

6. ЦНАП по надійному каналу зв'язку надсилає відкритий ключ виборця (*PK*) у верхню мережу blockchain.

Таким чином, коли вичерпався час, виділений на формування легітимних списків виборців, у нижньому блокчейні створено анонімний (деперсоналізований) список потенційних легітимних виборців, а Агентство отримує список всіх зареєстрованих легітимних виборців, але виборці зберігають свою анонімність.

Формат деперсоналізованих ідентифікаційних даних:

$$H(ID),$$

де *ID* - ідентифікаційні дані користувача у наступній послідовності: (серія та номер паспорту громадянина); *H* - криптографічна геш-функція

Формат деперсоналізованих ідентифікаційних даних має бути єдиним для всіх *IdP*. Ця умова унеможливить спроби виборців повторно зареєструватися у

різних *IdP* [51].

Другий етап: генерація гаманців легітимних виборців у децентралізованій інфраструктурі для здійснення дистанційного волевиявлення та підрахунку голосів.

Алгоритм генерації гаманця виборця (рисунок 4.13) ініціюється вузлом-валідатором верхньої мережі blockchain в момент отримання ним відкритого ключа від будь-якого із провайдерів ідентифікації у формі транзакції. Початковий баланс гаманця виборця 0 [51].

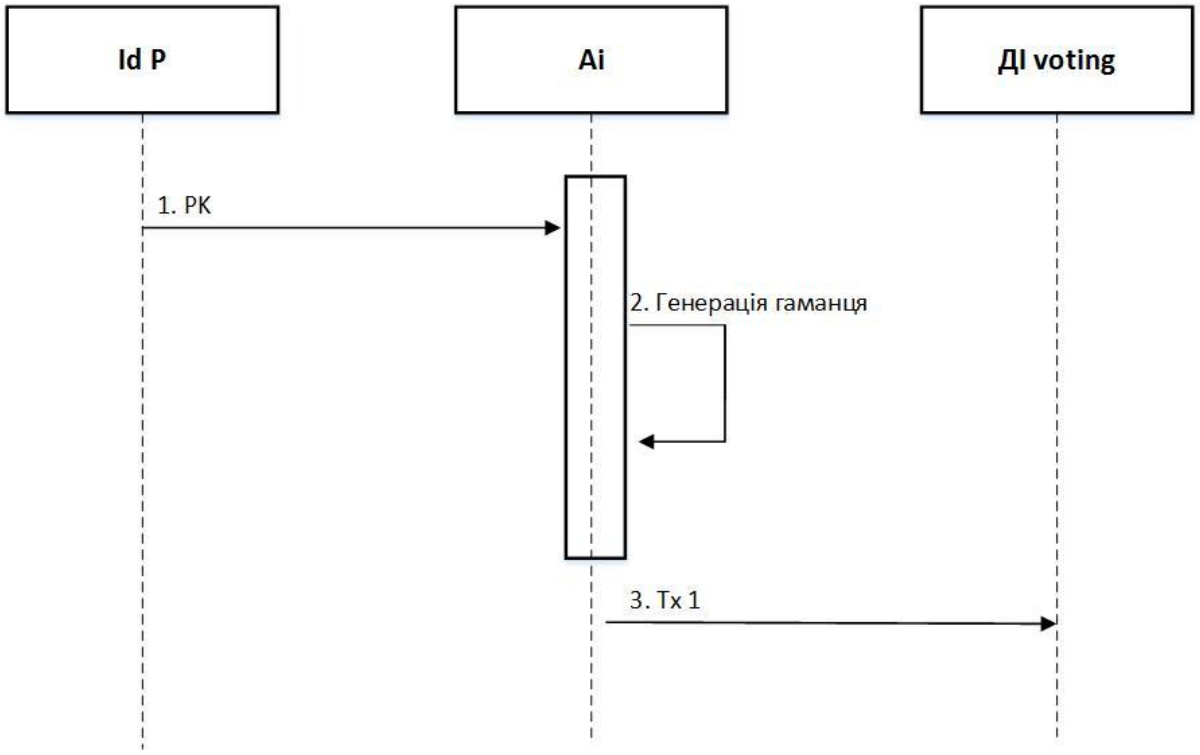


Рис. 4.13 Алгоритм генерації гаманця виборця

1. *IdP* по надійному каналу зв'язку надсилає відкритий ключ виборця (*PK*) вузлу-валідатору верхньої мережі blockchain.

2. Вузол-валідатор верхньої мережі blockchain проводить процедуру генерації гаманця для даного виборця. Відкритий ключ (*PK*) виборця, який був наданий вузлу-валідатору стає адресою гаманця данного виборця.

3. Вузол-валідатор формує транзакцію Tx1, яку підписує власним особистим ключем та надсилає її у верхню мережу blockchain (ДІ voting). Вузли-валідатори цієї мережі досягають консенсусу щодо даної транзакції.

Третій етап: реєстрація кандидатів у децентралізованій інфраструктурі для здійснення дистанційного волевиявлення та підрахунку голосів.

Реєстрація кандидатів відбувається у верхній мережі blockchain (децентралізованій інфраструктурі для здійснення дистанційного волевиявлення та підрахунку голосів, ДІ voting). Тут і далі під Агентством будемо розуміти сукупність територіальних виборчих дільниць, об'єднаних в окремий приватний blockchain [51].

Відповідальність за процедуру реєстрації (рисунок 4.14) кандидатів покладено на валідаторів верхньої мережі blockchain.

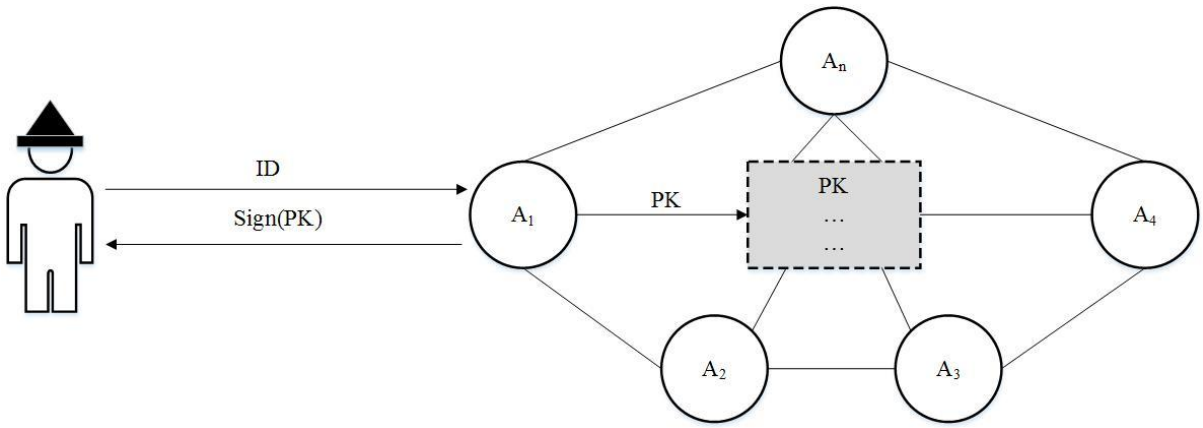


Рис. 4.14 Процедура реєстрації кандидатів

Представники відповідальних за проведення процедури волевиявлення які виступають в ролі вузлів-валідаторів у верхній мережі blockchain проводять первинну ідентифікацію кандидатів та ініціюють транзакцію на включення даного кандидата (генерацію гаманця кандидата із нульовим стартовим балансом) [51].

На рисунку 4.15 зображений алгоритм реєстрації кандидата.

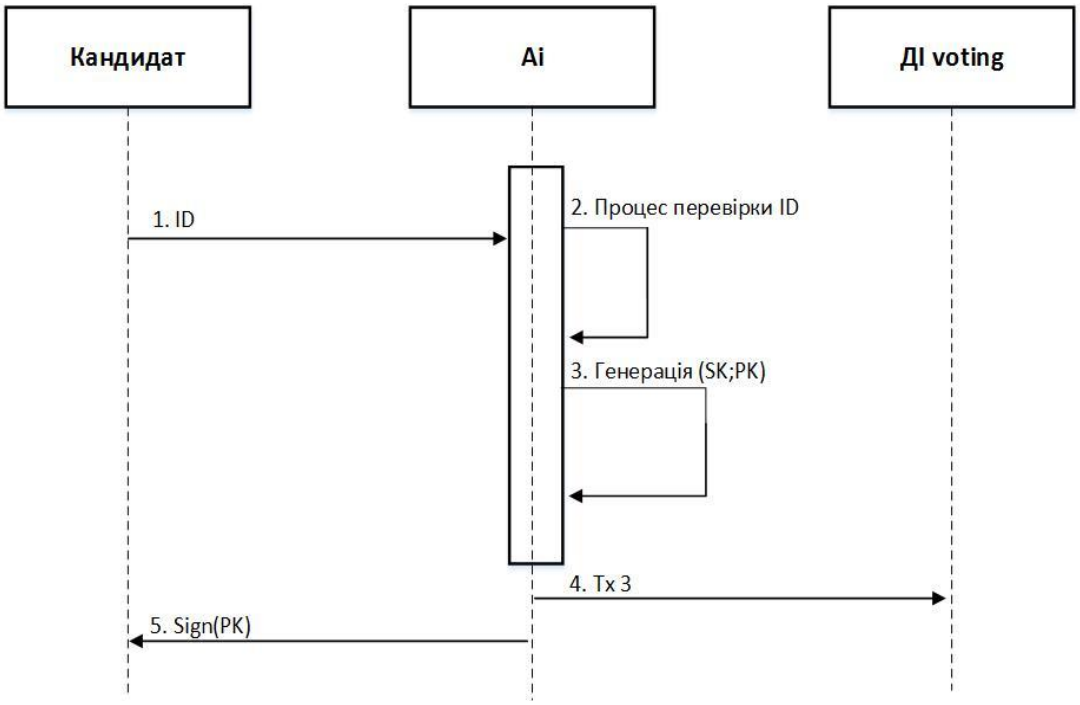


Рис. 4.15 Алгоритм реєстрації кандидата

1. Кандидат надає свої ідентифікаційні дані (*ID*) представнику Агентства

2. Представник Агентства проводить процедуру перевірки наданих ідентифікаційних даних.

3. Якщо даний кандидат має право бути включений до списку (тобто він відповідає всім вимогам), представник Агентства генерує гаманець (фактично ключову пару (*SK, PK*)).

4. Представник Агентства формує транзакцію щодо включення даного кандидата до списку, яку підписує власним особистим ключем.

5. Представник Агентства в якості підтвердження включення кандидатури до списку надсилає йому підписаний власним особистим ключем його відкритий ключ (*Sign(PK)*).

Четвертий етап: автентифікація виборців у децентралізованій інфраструктурі для здійснення дистанційного волевиявлення та підрахунку голосів.

Виборець, який отримав підтвердження від *IdP*, для допуску до процесу голосування та хоче прийняти участь у волевиявленні, звертається до одного із

вузлів Агентства для процедури автентифікації (рисунок 4.16). Автентифікуватися користувач може лише за допомогою особистого ключа (*SK*), за умови, що в мережі blockchain Агентства існує відповідний відкритий ключ (*PK*).

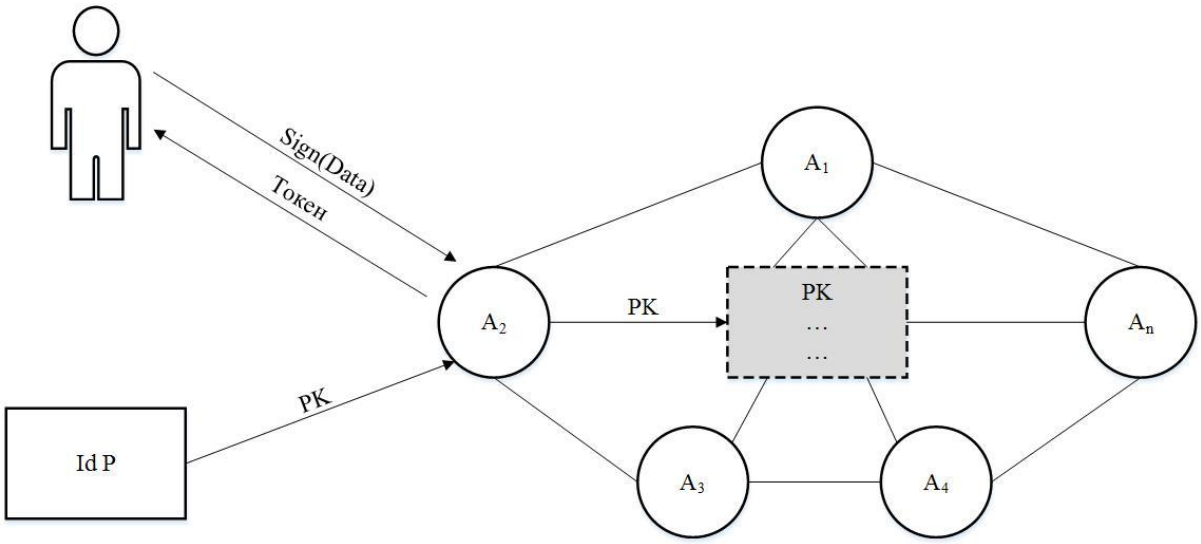


Рис. 4.16 Процедура автентифікації виборця

Якщо алгоритм автентифікації (рисунок 4.17) пройшов успішно, то баланс гаманця виборця збільшується на 1 токен.

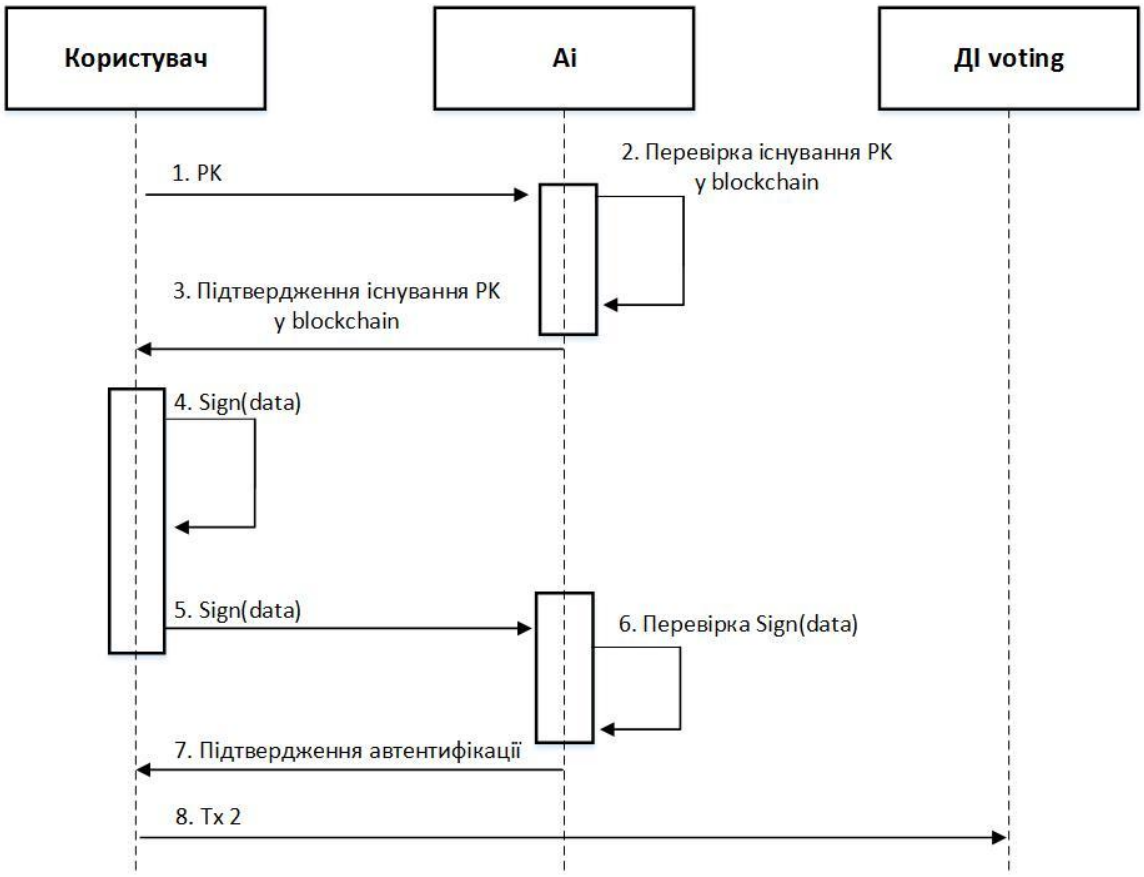


Рис. 4.17 Алгоритм автентифікації виборця

1. Користувач надає свій відкритий ключ до одного із вузлів-валідаторів

2. Вузол-валідатор проводить перевірку чи легітимний даний користувач (якщо користувач легітимний, то в ланцюжку блоків існує транзакція, яка ініціювала створення гаманця із такою адресою (*PK*)).

3. Якщо відповідний гаманець існує, вузол-валідатор надсилає підтвердження користувачу.

4. Користувач використовуючи власний особистий ключ (*SK*) підписує заздалегідь визначений набір тестових даних.

5. Та надсилає його вузлу-валідатору

6. Вузол-валідатор перевіряє підпис користувача використовуючи відкритий ключ, який міститься в системі.

7. Якщо перевірка пройшла успішно, вузол-валідатор надсилає користувачу підтвердження автентифікації.

8. Формується транзакція, підписана особистим ключем користувача (*SK*), яка ініціює збільшення балансу гаманця користувача на 1 токен.

П'ятий етап: голосування у децентралізованій інфраструктурі для здійснення дистанційного волевиявлення та підрахунку голосів

Виборці, які пройшли процедуру автентифікації здійснюють волевиявлення шляхом пересилки токена на одну із адрес гаманців, які відповідають зареєстрованим кандидатам, формуючи відповідну транзакцію, яку вони підписують власним особистим ключем.

Зворотній порядок четвертого та п'ятого етапів фактично відбувається наступне (рисунок. 4.18). Такий порядок полегшує реалізацію алгоритму на мало ресурсних пристроях [51, 66].

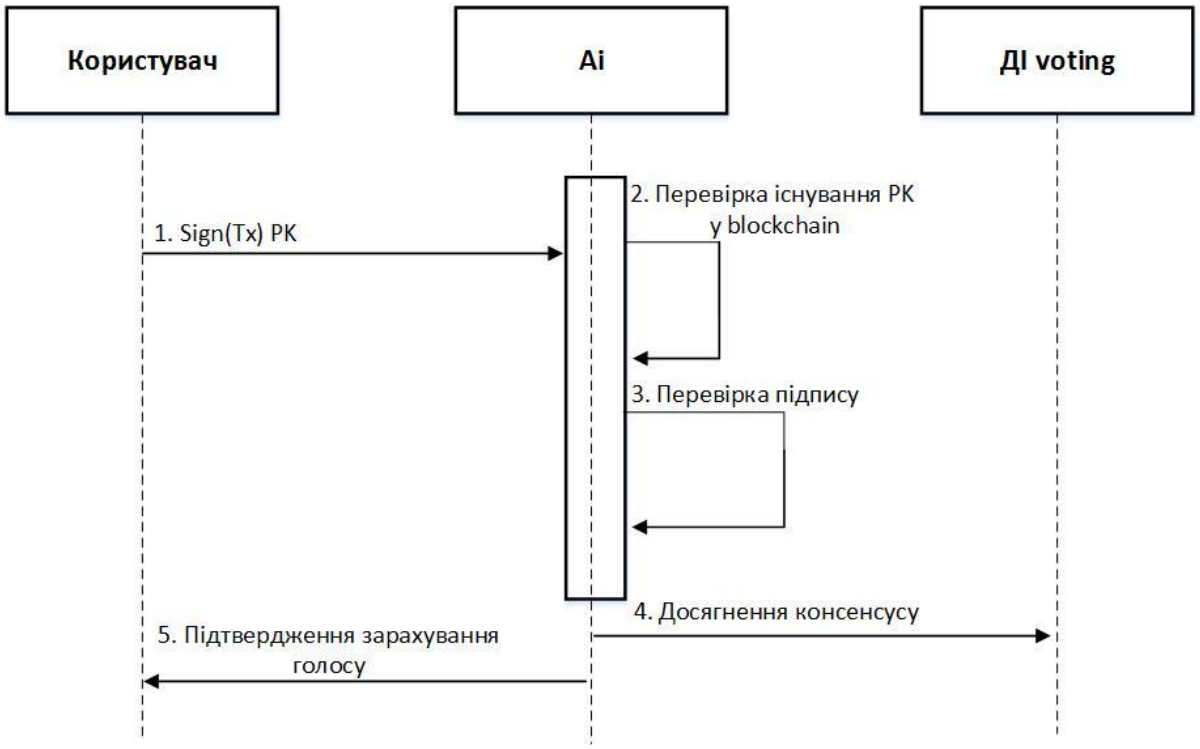


Рис. 4.18 Зворотній порядок п’ятого та четвертого етапів

1. Користувач формує транзакцію голосування, тобто транзакцію, яка ініціює пересилку токену на адресу обраного кандидата. Дана транзакція підписується із викоРисуноктання особистого ключа користувача.

2. Вузол-валідатор отримуючи транзакцію спочатку проводить перевірку легітимності користувача (наявності відповідного гаманця). Для цього валідатору необхідно впевнитися, що у ланцюжку блоків існує транзакція, яка ініціювала генерацію гаманця даного користувача.

3. Якщо попередня перевірка виконана успішно, вузол-валідатор проводить перевірку валідності електронного підпису, тобто перевірку факту володіння даним користувачем відповідним особистим ключем. Якщо обидві перевірки виконані успішно, вузли-валідатори досягають консенсусу щодо включення транзакції Tx у ланцюжок блоків.

4. Вузол-валідатор надсилає користувачу підтвердження зарахування його голосу.

Шостий етап: підрахунок голосів у децентралізованій інфраструктурі для здійснення дистанційного волевиявлення та підрахунку голосів

Підрахунок голосів здійснюється автоматично. Результати стають доступними всіх після завершення часу, відведеного для голосування [51].

Висновки до розділу 4

1. У даному розділі встановлено, що класичні системи голосування не відповідають усім необхідним вимогам для систем голосування. Зокрема, виборець не може перевірити, чи правильно його голос враховано і, якщо необхідно, повідомити про це уповноважені органи.

2. Обґрунтовано, що система електронного голосування охоплює процеси на чотирьох рівнях: нормативний, організаційний, рівень процесів, технологічний. У четвертому розділі сформульовані процеси, які відбуваються на кожному із чотирьох рівнях, а також показаний взаємозв’язок між ними.

3. *Удосконалена* модель системи електронного голосування, яка відрізняється від існуючих тим, що забезпечує формування деперсоналізованого списку виборців без використання сліпих підписів, що дозволяє спростити алгоритми взаємодії між сторонами.

4. Показано, що запропонований підхід зберігає переваги існуючих систем електронного голосування, таких як Fujiok-Okamoto-Ohta, Sensus, а також протоколу He-Su без реалізації сліпих підписів. Це допомагає зменшити складність впровадження.

5. *Розроблена* дворівнева архітектура системи електронного голосування, яка дозволяє забезпечити процеси електронної ідентифікації за допомогою вже існуючих засобів, таких як BankID, MobileID, електронний підпис. Це забезпечить інтероперабельність системи електронного голосування із розгорнутими системами електронної ідентифікації в Україні.

6. *Розроблені* алгоритми та протоколи для децентралізованої системи електронного голосування, які впроваджені у комплексі для проведення досліджень криптографічних властивостей технології blockchain.

7. Показано, що запропонована система може бути реалізована із використанням мало ресурсних пристроїв (мобільних телефонів).

8. Основні положення даного розділу викладені у публікаціях автора [50-53, 66].

РОЗДІЛ 5

МЕТОДИ ТА МЕХАНІЗМИ ЕЛЕКТРОННОГО ПІДПИСУ НА ГЕШ-ФУНКЦІЯХ ДЛЯ ПОСТКВАНТОВОГО ПЕРІОДУ

5.1 Порівняльний аналіз алгоритмів квантово-захищенних електронних підписів на основі геш-функцій та особливості їхньої реалізації

Криптографія заснована на використанні геш-функцій використовує схеми одноразового підпису такі як, наприклад, схема Lamport-Diffie або Winternitz. Стійкість таких схем ґрунтується виключно на стійкості геш-функції, що використовується.

Для реалізації таких схем використовуються бінарні дерева. Основна ідея використання полягає в тому, що кожна позиція на дереві розраховується як значення геш-функції від конкатенації дочірніх вузлів дерева. Вузол, який знаходиться на вершині дерева є відкритим ключем та обраховується послідовно як показано на рисунку 5.1. Листя дерева зберігають значення одноразових ключів.

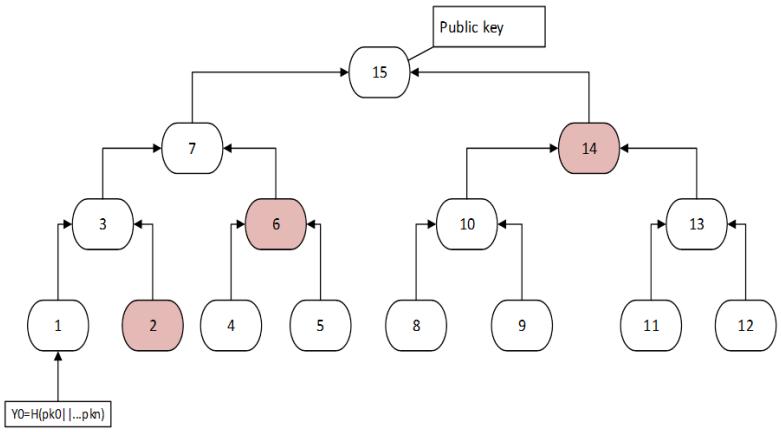


Рис. 5.1 – Генерація відкритого ключа

Ідея використання дерева була запропонована у 1979 році Merkle [75]. Проте вона має ряд недоліків, такі як великий розмір ключів та час генерації

підпису. На сьогоднішній день відомі модифікації алгоритму Merkle, а саме [57, 78]:

– алгоритм Leighton-Micali;
– алгоритм XMSS;
– алгоритм SPHINCS.

Реалізація схем електронного підпису проводиться у два етапи: реалізація схеми одноразового підпису та реалізації загальної схеми дерева сигнатур.

В якості схеми одноразового підпису можуть бути використані, наприклад, такі: LMTOS [54], WOTS, WOTS+ [55] тощо в залежності від модифікації.

Для реалізації загальної схеми сигнатур необхідними для всіх алгоритмів є наступні функції [65, 68]:

– генератор випадкової послідовності;
– дерево Мерклі;
– геш-функція;
– алгоритм одноразового підпису;
– обраний алгоритм обходу дерева.

При реалізації XMSS алгоритму та алгоритму SPHINCS вимагається додаткове L-tree для проведення процедури згортання відкритого ключа [56].

Використання алгоритму BDS дозволяє зменшити часові затрати на процедуру обходу дерева. Процедура обходу дерева використовує BDS алгоритм з мінімальними часовими витратами.

На основі проведеного аналізу [59-61, 82-83] можна побудувати зведену таблицю порівняння алгоритмів електронного підпису на основі геш-функцій, які є перспективними для використання в постквантовий період [65, 68] (Табл. 5.1).

Таблиця 5.1

Порівняння алгоритмів електронного підпису на основі геш-функцій

<table>
<tr><td rowspan="2">Критерій</td><td colspan="4">Алгоритм</td></tr>
<tr><td>Merkle</td><td>Leighton-Micali</td><td>XMSS</td><td>SPHINCS</td></tr>
<tr><td>Стійкість</td><td>128</td><td>128</td><td>256</td><td>256</td></tr>
<tr><td>Модель загроз</td><td>EUF-CMA</td><td>EUF-CMA</td><td>EUF-CMA</td><td>EUF-CMA</td></tr>
<tr><td>Довжина відкритого ключа</td><td>32 байта</td><td>20 байт</td><td>64 байт</td><td>1 056 байт</td></tr>
<tr><td>Довжина підпису</td><td>1 731 байт</td><td>668 байт</td><td>8 392 байт</td><td>41 000 байт</td></tr>
<tr><td>Можливі одноразові підписи</td><td colspan="4">В якості одноразового підпису в даних схемах можуть виступати: LMOTS, WOTS, WOTS+ и др.</td></tr>
<tr><td>Можливі геш-функції</td><td colspan="4">Однонаправлена криптографічно стійка геш-функція</td></tr>
<tr><td>Гнучкість вибору одноразового підпису/геш-функції</td><td>+</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td>Час генерації підпису</td><td>217 мс</td><td>43 мс</td><td>2,87 мс</td><td>153,39 с</td></tr>
<tr><td>Час перевірки підпису</td><td>1,53 мс</td><td>33 мс</td><td>0,22 мс</td><td>1,71 с</td></tr>
<tr><td rowspan="3">Необхідні функції для реалізації</td><td colspan="2" rowspan="3">Генератор випадкової послідовності
Дерево Мерклі
Геш-функція
Одноразовий підпис
Алгоритм обходу дерева</td><td colspan="2">Генератор випадкової послідовності
Дерево Мерклі
Геш-функція
Одноразовий підпис</td></tr>
<tr><td colspan="2">L-tree</td></tr>
<tr><td>Алгоритм обходу дерева</td><td>HORST</td></tr>
<tr><td>Заповнення нижнього рівня дерева Мерклі</td><td colspan="2">Заненесення значеня відкритого ключа одноразового підпису</td><td colspan="2">Використання додаткового L – дерева для стискання відкритого ключа</td></tr>
<tr><td>Кросплатформеність</td><td>+</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td>Можливість розпаралелювання</td><td>-</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>Можливість програмної/апаратної реалізації</td><td>+</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td>Наявність в криптографічних бібліотеках</td><td>-</td><td>-</td><td>Open SSL</td><td>-</td></tr>
<tr><td>Версії</td><td>-</td><td>-</td><td>XMSS+, XMSS^MT</td><td>-</td></tr>
<tr><td>Стан стандартизації</td><td>-</td><td>Hash-Based Signatures draft-mcgrew-hash-sigs-06</td><td>XMSS: Extended Hash-Based Signatures draft-irtf-cfrg-xmss-hash-based-signatures-09</td><td>-</td></tr>
</table>

5.1.1 Результати порівняльного аналізу алгоритмів квантово-захищенних електронних підписів на основі геш-функцій

Для проведення процедури порівняння були обрані критерії стійкості, гнучкості та швидкодії, які наведені в таблиці 5.2 [65, 68].

Таблиця 5.2

Критерії порівняння алгоритмів

Критерій	Алгоритм			
	Merkle	Leighton-Micali	XMSS	SPHINCS
Стійкість	128	128	256	256
Актуальність моделі загроз	+	+	+	+
Довжина відкритого ключа	32 байта	20 байт	64 байт	1 056 байт
Довжина підпису	1 731 байт	668 байт	8 392 байт	41 000 байт
Можливі одноразові підписи	В якості одноразового підпису в даних алгоритмах можуть виступати: LMOTS, WOTS, WOTS+ и др.			
Можливі геш-функції	Однонаправлена криптографічно стійка геш- функція			
Час генерації підпису	217 мс	43 мс	2,87 мс	153,39 с
Час перевірки підпису	1,53 мс	33 мс	0,22 мс	1,71 с

Порівняння проводилось методом ієрархій. В даному випадку маємо 3 рівні ієрархій (рисунок 5.2).

– Рівень 1: мета аналізу – вибір найкращого алгоритму – найвищий рівень ієрархії;

– Рівень 2: вісім критеріїв порівняння;
– Рівень 3: чотири альтернативи – чотири алгоритми електронного підпису.

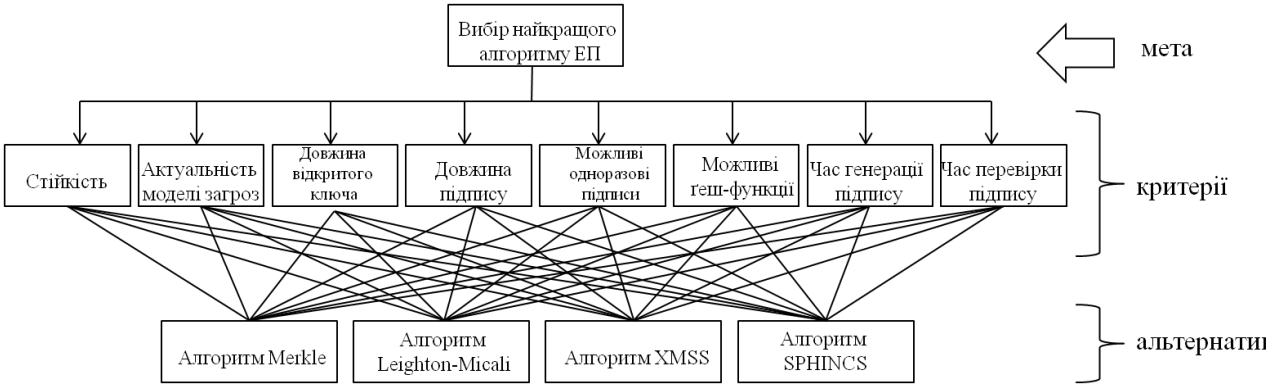


Рис. 5.2 Рівні ієрархій

Критерії порівнюються попарно по відношенню до мети, альтернативи - попарно по відношенню до кожного з критеріїв. Відповідно заповнюються матриці парних порівнянь (одна- для критеріїв, n матриць для альтернатив, де n- кількість критеріїв) (Табл. 5.3).

Таблиця 5.3

Матриця попарних порівнянь

	К1	К2	…	К8	Пріоритет
К1	1	8	…	3	
К2	1/8	1	…	1/5	
…	…	…	1	…	
К8	1/3	5	…	1	

Два об'єкти, що знаходяться на одному рівні порівнюються по своїй відносній вагомості для одного об'єкта вищого рівня. Порівняння проводиться з використанням спеціальної «шкали відносної важливості» - шкали Саатті [70] (таблиця 5.4).

Таблиця 5.4

Шкала Саатті

Ступінь переваги	Визначення	Пояснення
1	Рівна значимість	Дві альтернативи однакові з точки зору мети
2	Слабкий ступінь переваги	Проміжна градація між рівною значимістю та середньою перевагою
3	Середній ступінь переваги	Одна із альтернатив є трохи кращою за іншу
4	Перевага вище середнього	Проміжна градація між середньою та помірно сильною перевагою
5	Помірно сильна перевага	Одна із альтернатив явно краща за іншу
6	Сильна перевага	Проміжна градація між сильною та дуже сильною перевагою
7	Сильніша перевага	Одна із альтернатив набагато краще іншої. Домінування підтверджується практикою.
8	Дуже сильна перевага	Проміжна градація між сильнішою перевагою та абсолютною перевагою.
9	Абсолютна перевага	Очевидна перевага однієї альтернативи над іншою.

За результатами обробки матриць отримуємо один вектор локальних пріоритетів критеріїв розмірності m (де m- кількість критеріїв) та m векторів локальних пріоритетів розмірності n (де n- кількість альтернатив). Вектор локальних пріоритетів показує їхню відносну значущість.

Пошук вектора локальних пріоритетів зводиться до задачі пошуку власного вектора матриці попарних порівнянь

$$A * X = \lambda * X$$

де A – матриця попарних порівнянь; X- вектор із шуканих пріоритетів; λ- власне значення матриці попарних порівнянь

з наступним його нормуванням

$$\sum X_i = 1$$

У таблиці 5.5 наведена зведена матриця пріоритетів критеріїв.

Таблиця 5.5

Матриця пріоритетів критеріїв

	Пріоритет критерію	Merkle	Leighton-Micali	XMSS	SPHINCS
Стійкість	0.413	0.083	0.083	0.417	0.417
Актуальність моделі загроз	0.257	0.250	0.250	0.250	0.250
Відкритий ключ	0.064	0.299	0.185	0.209	0.307
Підпис	0.064	0.299	0.185	0.209	0.307
Гнучкість у виборі одноразового підпису	0.033	0.250	0.250	0.250	0.250
Гнучкість у виборі одноразового геш-функції	0.033	0.250	0.250	0.250	0.250
Час генерації підпису	0.068	0.120	0.315	0.511	0.054
Час верифікації підпису	0.068	0.120	0.315	0.511	0.054

Вектор глобальних пріоритетів по відношенню до мети розраховується наступним чином: кожен компонент цього m-вектора – скалярне множення вектора локальних пріоритетів критеріїв на m- вектор, який складається із шуканих пріоритетів альтернативи по даному критерію.

Базуючись на вхідних даних отримані наступні глобальні пріоритети [65, 68] (Табл. 5.6).

Таблиця 5.6

Глобальні пріоритети

I	XMSS	0.349
II	SPHINCS	0.300
III	Leighton-Micali	0.182
IV	Merkle	0.170

На рисунку 5.3 результати наведені у графічному вигляді.

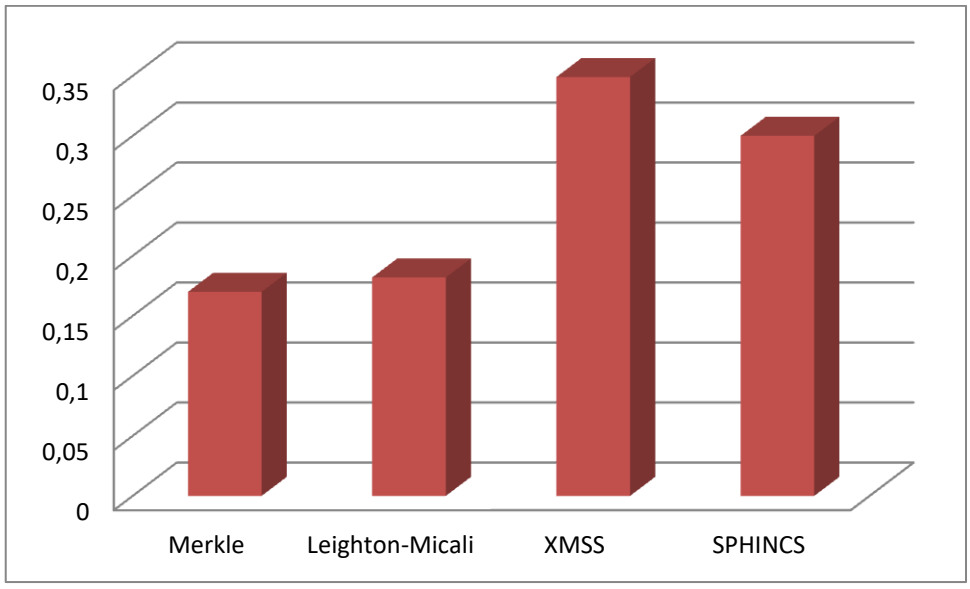


Рис. 5.3 Глобальні пріоритети

Таким чином, за результатами проведеного порівняльного аналізу на основі обраних критеріїв стійкості, швидкодії та гнучкості, можемо зробити висновок про перевагу XMSS алгоритму. Необхідно зауважити, також що існує

модифікація даного алгоритму XMSS+, яка орієнтована на реалізацію у пристроях з обмеженими ресурсами, що виступає додатковою перевагою алгоритму над іншими, зважаючи на постійну тенденцію зростання числа мобільних пристроїв [79].

Алгоритм XMSS був реалізований із використанням національного стандарту гешування ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування» для двох рівнів стійкості. Результати експериментів наведені в таблиці 5.7.

Таблиця 5.7

Результати використання національного стандарту хешування для алгоритму XMSS [58]

	Стійкість 128	Стійкість 256
	Відкритий ключ: 64 байта	Відкритий ключ: 128 байт
	Особистий ключ: 132 байта	Особистий ключ: 260 байт
Час генерації ключа, мс	111697	61030
Час генерації підпису, мс	110168	601727
Час перевірки підпису, мс	219	1232

Результати експерименту отримані із використанням процесора Intel(R) Pentium(R) CPU G850 @2.90 GHz.

5.2 Аналіз механізмів одноразових електронних підписів на основі геш-функцій

5.2.1 Сутність одноразового механізму електронного підпису Lamport

Загальні параметри одноразового механізму Lamport (ЕП Lamport). Підписуюча сторона *А* та перевіряюча сторона *Б* узгоджують наступні загальні параметри [54, 58]:

— стандартизовану геш-функцію з параметрами;

— довжину геш-значення;

— допустимі генератори випадкових / псевдовипадкових послідовностей.

Генерація ключових пар [58, 63]. Підписуюча сторона *A* генерує *n* секретних ключових пар (X,Y) використовуючи узгоджені генератори випадкових чи псевдо випадкових послідовностей (5.1).

$$X = (x_1, ..., x_i, ..., x_n)$$
$$Y = (y_1, ..., y_i, ..., y_n) \quad (5.1)$$

з довжиною кожного із секретних ключів l_h , де l_h довжина геш-значення обраної геш-функції. Таким чином, кожна пара (x_i, y_i) є *i*-тою частиною секретного (особистого) ключа.

Відкритий ключ обчислюється шляхом гешування секретних ключів (5.1), тобто, отримуємо *n* пар відкритих ключів:

$$H(X) = (H(x_1), ..., H(x_i), ..., H(x_n))$$
$$H(Y) = (H(y_1), ..., H(y_i), ..., H(y_n)) \quad (5.2)$$

з довжиною геш-значення l_h.

Секретні ключі (5.1) повинні бути доступними та відомими тільки підписувачу *A*. Відкриті ключі (5.2) мають бути доступними усім користувачам, які можуть отримувати від *A* підписані повідомлення.

Підпис повідомлення. Для підпису повідомлення *M* підписуюча сторона *A* виконує гешування повідомлення *M* з використанням узгодженої (криптографічної) геш-функції з параметрами Pr. В результаті чого отримує геш-значення

$$h_M = H(M, Pr)) \quad (5.3)$$

Значення h_M , по суті, зашифровується засобом заміни бітів геш-значення h_M секретними одноразовими ключами (5.1), при чому кожен h_{Mi} біт, що приймає значення «0», заміняється послідовно секретним ключем із множини (5.1) *X*, а h_{Mi}

біт, що приймає значення «1» послідовно заміняється секретним ключем із множини (5.1) Y. Так відбувається для усіх бітів геш-значення h_{Mi}.

Вказана послідовність l_h секретних ключів і є Z – електронним підписом повідомлення M. Він разом з вибраними x_i чи y_i стає відкритим та доступним як користувачам (потенційним контрагентам) відповідного домену так і порушнику (крипто аналітику). Надалі такий ЕП у відповідному форматі передається та зберігається разом з повідомленням.

Підписане повідомлення має наступний вигляд (5.4)

$$\{M; Z = (\{x_1 \mid y_1\}), \{x_2 \mid y_2\}, ..., \{x_i \mid y_i\}, ..., \{x_n \mid y_n\}) = \\ = \{M, Z = (z_1, z_2, ..., z_i, ..., z_n)\} \quad (5.4)$$

В (5.4) символ «|» означає, що при зашифруванні в ЕП появляється один із використаних секретних сигналів - x_i чи y_i, що визначається i– тим бітом геш-значення h_{Mi}. Таким чином, випадкові послідовності $(z_1, z_2, ..., z_i, ..., z_n)$ із секретного ключа стають ЕП повідомлення M.

Після процесу зашифрування використані ключі x_i чи y_i, що були секретними, стають відкритими. Далі будемо вважати, що відкритими із множини (5.1) стають лише i ключів, а n залишились секретними. Такі ключі в механізмі Lamport після вироблення ЕП більше не можуть використовуватися.

Перевірка повідомлення [58, 64]. Перевіряюча сторона отримує підписане повідомлення $M*$ виду

$$\{M^*; Z^* = (\{x_1 \mid y_1\}), \{x_2 \mid y_2\}, ..., \{x_i \mid y_i\}, ..., \{x_n \mid y_n\}) = \\ = Z* = (z^*_1, z^*_2, ..., z^*_i, ..., z^*_n) \quad (5.5)$$

де символ «*» означає, що як повідомлення M, так і підпис Z можуть бути зміненими чи підробленими.

Перевірка ЕП повідомлення (5.5) відбувається наступним чином:

1. Перевіряюча сторона здійснює гешування повідомлення M^*, в результаті чого отримує геш-значення

$$h_{Mi*} = H(M^*, \Pr) \quad (5.6)$$

2. У відповідності зі значеннями h_{Mi^*} із ЕП Z^* у відповідності з усіма значеннями бітів h_{Mi^*} із відкритого ключа (5.2) вибираються геш-значення $H(x_i)$ чи $H(y_i)$.

Причому, якщо обчислене значення h_{Mi^*} приймає значення «0», то із відкритого ключа (5.2) вибирається відповідне значення $H(x_i)$, а якщо «1», то із відкритого ключа (5.2) вибирається відповідне значення $H(y_i)$. Так виконується для усіх значень блоків бітів геш-значення (5.6). В результаті перевіряюча сторона отримує

$$Z^{'} = (\{H(x_1) \mid H(y_1)\}), \{H(x_2) \mid H(y_2)\}, ..., \{H(x_i) \mid H(y_i)\}, ..., \{H(x_n) \mid H(y_n)\}) = \\ = (z_1^{'}, z_2^{'}, ..., z_i^{'}, ..., z_n^{'}) \quad (5.7)$$

3. Далі, перевіряюча сторона послідовно гешує усі ключі ЕП (5.4) та порівнює отримані значення зі значеннями (5.7) $(z_1^{'}, z_2^{'}, ..., z_i^{'}, ..., z_n^{'})$. Якщо усі *n* значень співпали, то ЕП вважається справжнім, в іншому випадку – викривленим.

Формально відбувається перевірка того, що для кожного *i* виконується вимога

$$z_i^{'} = H\left(z_i\right) \quad (5.8)$$

5.2.2 Особливості одноразового механізму ЕП Lamport-Diffie

Одною із перших модифікацій механізму ЕП Lamport був механізм Lamport-Diffie (LD-OTS) [71] в частині уточнення вимог до геш-функцій. Відповідно до даної модифікації, геш-функція (5.2) має бути одно направленою, а геш-функція, яка використовується для гешування повідомлення *M* при виробленні ЕП, повинна бути криптографічною [58].

Загальні параметри одноразового механізму Lamport-Diffie. Припустимо, що *l* – додатне ціле число, довжина геш-значення, яке є параметром безпеки механізму. При цьому використовується однонаправлена геш-функція

$$f : \{0,1\}l \to \{0,1\}l \quad (5.9)$$

та криптографічна геш-функція

$$g : \{0,1\}^* \to \{0,1\}l \quad (5.10)$$

Генерація ключових пар [58, 62]. Секретний ключ X складається з 2n випадкових бітових строчок довжиною l_h, причому можливий випадок, коли $l_h = n$

.

$$X = (x_{n-1}[0], x_{n-1}[1], ..., x_1[0], x_1[1], x_0[0], x_0[1]) \in R\{0,1\}^{(n,2n)} \quad (5.11)$$

Відкритий ключ Y – це послідовність строчок – результат гешування (5.11).

$$Y = (y_{n-1}[0], y_{n-1}[1], ..., y_1[0], y_1[1], y_0[0], y_0[1]) \in R\{0,1\}^{(n,2n)} \quad (5.12)$$

Підпис повідомлення. Повідомлення $M = \{0,1\}^*$ підписується з використанням секретного ключа X (5.11). За допомогою криптографічної геш-функції g обчислюється геш-значення повідомлення M.

$$g(M) = h = (h_{l-1}, ..., h_0) \quad (5.13)$$

ЕП повідомлення M буде, аналогічним (5.4), n строчок

$$\sigma = (x_{n-1}[h_{n-1}], ..., x_1[h_1], x_0[h_0]) \in R\{0,1\}^{(l,n)} \quad (5.14)$$

Таким чином, ЕП з використанням механізму LD-OTS є послідовність із n бітових рядків, кожен з яких довжиною l. Тобто, ЕП здійснюється аналогічно до механізму Lamport згідно з (5.4), i-тий біт підпису є $x_i[0]$, якщо i-тий біт геш-значення h дорівнює «0», інакше – $x_i[1]$, якщо i-тий біт геш-значення h дорівнює «1». Всього довжина ЕП складає $l \times n$ бітів, а при $l=n$ буде $l^2 = n^2$.

Перевірка підпису [58, 62]. Перевірка здійснюється аналогічно до механізму Lamport (5.6) та (5.8). Після обчислення геш-значення від повідомлення $h(M^*)$, підпис якого перевіряється, у відповідності зі значеннями h_{Mi^*} із ЕП Z^* у відповідності з усіма значеннями бітів h_{Mi^*}(«0» чи «1») із відкритого ключа (5.12) вибираються геш-значення $y_i[0]$ чи $y_i[1]$. Після чого за допомогою одно направленої геш-функції обчислюються геш-значення ЕП (5.14), які порівнюються з отриманими вище з (5.12).

Таким чином, особливістю механізму Lamport-Diffie виступає визначення функцій гешування (5.9) та (5.10), а також формат запису та використання секретного та відкритого ключів – в зворотному порядку.

5.2.3 Одноразовий електронний підпис Winternitz

Ідея механізму Winternitz (WOTS) полягає в тому, щоб підписувати декілька бітів геш-значення, використовуючи один рядок одноразового ключа [55].

Загальні положення механізму Winternitz. У механізмі Winternitz (W-OTS) використовуються одностороння геш-функція (5.9) та криптографічна геш-функція (5.10). Параметр Winternitz $w \geq 2$ обирається як кількість бітів, що повинні бути підписані одночасно з використанням одноразового ключа.

В механізмі Winternitz вводяться наступні параметри t_1, t_2, t [6,8], такі, що

$$t_1 = \lceil l / w \rceil, t_2 = \lceil \log_2 t_1 / w \rceil, t = t_1 + t_2 \tag{5.15}$$

де l довжина геш-значення, $w \geq 2$ – параметр, який визначає кількість бітів, що підписуються одним рядком одноразового ключа. Параметр t_2 визначає число нулів, які мають бути додані на початку геш-значення, для того, щоб отримана в результаті нова довжина t була кратна w [62].

Зазвичай параметр w визначають з обмеженням у вигляді

$$w = 2^{\partial}, \partial = 1, 2, 3, 4, 5, 6, 7, 8... \tag{5.16}$$

Генерація ключових пар [68]. У загальному випадку секретними ключами є $t_1 2^w$ випадкових бітових строчок довжини l

$$X = (x_{t_{l-1}}, ..., x_i, ..., x_1, ..., x_0) \in R\{0,1\}^{(l, t_1, 2^w)} \tag{5.17}$$

Таким чином, секретним ключем (5.17) є $t_1 2^w$ секретних ключів довжини l.

Відкритим ключем Y є послідовність строчок, яка обчислюється шляхом застосування геш-функції f до кожного бітового рядку (5.17)

$$Y = (y_{t_{l-1}}, ..., y_i, ..., y_1, ..., y_0) \in R\{0,1\}^{(l, t_1, 2^w)} \tag{5.18}$$

де

$$y_i = f(x_i), 0 \leq i \leq t_1 2^w - 1 \tag{5.19}$$

Тобто, при генерації відкритого ключа необхідно виконати $t_1 2^w$ викликів однонаправленої геш-функції f. При цьому число секретних та відкритих ключів,

які потрібні для виконання ЕП, залежить від величини *w*. Таким чином, змінюючи параметр *w*, можна змінювати довжини секретного та відкритого ключів [63-65].

Підпис повідомлення [68]. Нехай геш-значення повідомлення M є $g(M) = d = (d_{l-1},...,d_0)$. Для того щоб довжина d ділилась на w, спочатку необхідно встановити мінімальне число нулів таким чином, щоб довжина d геш-значення ділилась на w. За цієї умови розширений рядок d розділяється на tl бітових блоків довжини w, тобто

$$d = b_{t1-1} \| ...b_i ... \| b_0 \tag{5.20}$$

де знак «||» означає конкатенацію.

Далі засобом заміни кожного bi блоку геш-значення, повідомлення M зашифровується з використанням секретного ключа (5.17). Як результат ЕП повідомлення, тобто зашифроване геш-значення $g(M)$, має такий вигляд

$$g(M) = S^* = (f^{b_{t1-1}}(x_{t1-1}),..., f^{bi}(x_i),..., f^{b1}(x_1), f^{b0}(x_0) =$$

$$= (s^*_{t1-1},..., s^*_i,..., s^*_1, s^*_0) \tag{5.21}$$

Необхідно відмітити, що в (5.21) $s^*_{t1-1},..., s^*_i,..., s^*_1, s^*_0$ - це ключі, які до вироблення ЕП були секретними. Але після вироблення ЕП вони стають відкритими.

Перевірка підпису. Для перевірки ЕП отриманого повідомлення M^*, що має вигляд

$$S^* = (s^*_{t1-1},..., s^*_i,..., s^*_1, s^*_0) \tag{5.22}$$

спочатку аналогічно (5.20) обчислюється геш-значення $g(M^*)$, що має такий вигляд

$$d^* = b^*_{t1-1}, b^*_i, b^*_0 \tag{5.23}$$

Наявність символу (*) у M^* та у всіх b^*_i елементах означає, що вони могли бути викривленими штучно чи в результаті помилок при обробленні, передаванні та прийманні.

Далі, для всіх b^*_i (5.23), із відкритого ключа (5.18) у відповідності з їх значеннями, вибираються певним чином геш-значення, що є складовими відкритого ключа. В результаті отримуємо

$$Y = (y_{t1-1},...,y_i,...,y_1,y_0) \in \{0,1\}^{(l,t1)} \quad (5.24)$$

Після чого здійснюється гешування значень $s^*_{t1-1},...,s^*_i,...,s^*_1,s^*_0$, тобто ключів безпосередньо ЕП (5.22), в результаті отримуємо

$$Y^* = (y^*_{t1-1},...,y^*_i,...,y^*_1,y^*_0) \in \{0,1\}^{(l,t1)} \quad (5.25)$$

На останок порівнюємо значення (5.24) y_i та (5.25) y^*_i для $j = 0,1,...,i,...,tl-1$

Якщо $y_i = y^*_i$ для усіх $j = 0,1,...,i,...,tl-1$, то ЕП правильний, що підтверджує цілісність та справжність підписаного з його допомогою повідомлення *M*, а також дозволяє встановити авторство повідомлення *M*.

5.2.4 Удосконалена математична модель постквантового електронного підпису POTS

Загальні параметри. В розробленому удосконаленому механізмі POTS [62-64] використовується одностороння/криптографічна геш–функція *f* та криптографічна геш-функція *g*

$$\mathrm{f}: \{0, 1\}\mathrm{l} \rightarrow \{0, 1\}^{\mathrm{l}} \quad (5.25)$$

$$\mathrm{g}: \{0, 1\}* \rightarrow \{0, 1\}^{\mathrm{l}.}$$

Для вироблення ЕП повідомлення *M* спочатку виконується гешування повідомлення *M* з використанням узгодженої (як правило криптографічної) геш-функції з параметрами *Pr*, а потім обчислюється геш-значення

$$h_M = H(M, Pr)) \quad (5.26)$$

Далі значення h_M, по суті, зашифровується засобом заміни *w* блоків бітів геш-значення h_M секретними одноразовими ключами. Процес такого зашифрування продовжується для усіх блоків бітів геш-значення.

Таким чином, l_h бітів геш-значення h_{Mi} заміняються (зашифровуються) одноразовими ключами, тобто, по суті безумовно стійким шифром, оскільки послідовність бітів h_{Mi} заміняється одноразовими секретними випадковими послідовностями. Послідовність l_k і є електронним підписом повідомлення *M*. Такий ЕП разом з вибраними x_i чи y_i стає відкритим та доступним як

користувачам (потенційним контрагентам) відповідного домену так і порушнику (криптоаналітику). В подальшому такий ЕП у відповідному форматі передається та зберігається разом з повідомленням і є його одноразовим ЕП. Для механізму POTS підпис складається з *k* випадкових послідовностей, таких, що $k \le l_h$ [63,64].

Генерація ключових пар для механізму POTS [63]. Приймемо, що параметр $w \ge 1$ визначає кількість бітів геш-значення, що повинна бути підписана одночасно, тобто замінена одним секретним ключем.

При w=1 отримуємо частковий випадок – механізм Lamport з OTS ключами.

При w ≥ 2 отримуємо загальний випадок механізму Winternitz, із модифікованими функціями зашифрування та перевірки [63].

В механізмі POTS ЕП (зашифрування) здійснюється (не обов'язково) на основі застосування до усіх w_b блоків перетворення виду

$$z = Z(w_b), \tag{5.27}$$

внаслідок чого *w* біт блоку відображаються в *w** біт нового блоку. Причому L_{bi} довжина b_i блоку може бути як більше так і менше довжини L_{bi^*} блоку b_i^*, отриманого внаслідок перетворення (5.27).

Необхідно відмітити, що головною відмінністю механізму POTS є те, що в ньому застосовується перетворення кожного b_i блоку у такому вигляді. Якщо

$$0 \le b_i \le (2^w / 2) - 1 \tag{5.28}$$

то кожен b_i блок зашифровується (заміняється) послідовно секретним ключем із множини *X*, інакше зашифровується (заміняється) послідовно секретним ключем із множини *Y*.

Також, по аналогії з узагальненням Winternitz визначені параметри t_1, t_2, t у вигляді

$$t_1 = \left\lceil l / \log_2 w^* \right\rceil, t_2 = \left\lceil \log_2 t_1((w^* - 1)) / \log_2 w^* \right\rceil + 1, t = t_1 + t_2. \tag{5.29}$$

Будемо вважати, що для геш-значення повідомлення, що подається у вигляді блоків b_i (b_i^*) виду

$$d = bt1\text{-}1 \,||\, .bi\, .\, .\, ||\, b0\,, \tag{5.30}$$

можна визначити контрольну суму у вигляді

$$c^* = \sum_{i=1}^{t_1} (w^* - 1 - b_i^*) \tag{5.31}$$

або

$$c^* = \sum_{i=1}^{t_1 1} (2^{w^*} - b_i^*)\,, \tag{5.32}$$

В моделі POTS не виключається, що параметри t_1, t_2, t можуть бути визначеними іншим чином. В механізмах POTS дані геш-значення d (5.30) та контрольних сум C (5.31) та (5.32) можуть зашифровуватись з різною збитковістю [62-64].

Разом з тим, попередній аналіз показав, що вид функцій перетворення блоків (5.27) та (5.28) може суттєво вплинути на криптографічну стійкість проти існуючих та можливих атак. Тому, однією із важливих задач є визначення функцій перетворення, які будуть дозволяти забезпечити зменшення довжин секретних та відкритих ключів, а також зменшувати довжину підпису, забезпечуючи допустиму криптографічну стійкість проти існуючих та потенційних атак із використанням класичних та квантових комп'ютерів [63].

Після виконаного перетворення (5.31) чи (5.32) значення контрольної суми C^* у вигляді блоків бітів w^* конкатенується з геш-значенням (5.30) d і потім виконується одночасне ідентичне зашифруваннння та верифікація. Контрольні суми можуть обчислюватись довільним чином в залежності від необхідності. Крім того, значення d та контрольних сум C (5.31) та (5.32) можуть зашифровуватись згідно із необхідною схемою OTS [63].

Уточнення параметрів для POTS. Для здійснення ЕП необхідно уточнення параметрів підпису – *t1*, *t2* та *t*. Якщо довжини L_s випадкових чи псевдовипадкових послідовностей кратні w^*, то *t1* визначає кількість блоків бітів геш-значення, що будуть підписуватись (зашифровуватись) одним секретним ключем. В цьому випадку

$$t = t1 = n / w^* \tag{5.33}$$

Якщо *n* не кратне w^*, то в останньому блоці буде менше чим w^* бітів, тому число бітів, які потрібно підписати необхідно збільшити так, щоби *t1* було цілим. В (5.32) *t2* визначає число блоків, за допомогою яких подається контрольна сума. У загальному випадку

$$t^* = t1 + t2 \tag{5.34}$$

Без втрати як теоретичного так і практичного подання та дослідження WOTS можна (але не обов'язково) вважати, що довжина блока *w= 1,2,3,3.,4.6….*, за цієї умови для однозначного зашифрування кожного із w_i блоків потрібно у загальному випадку [63]

$$N_w = 2^w, \; w = 2,3,4,5,6... \tag{5.35}$$

випадкових послідовностей кожного секретного ключа.

У випадку (5.28) для зашифрування кожного w_i блоку необхідно

$$N_w = 2 \tag{5.36}$$

випадкових послідовностей кожного секретного ключа. Тому, у залежності від значення *w*, виграш *U* у зменшенні довжини секретного ключа у загальному випадку для POST стосовно WOST складає

$$U = 2^{w-1} \tag{5.37}$$

Секретним ключем механізму POTS $X_d\ (w^*), Y_d\ (w^*)$ є послідовність t множин секретних ключів

$$X_d(w^*) = (x_{t-1}, \ldots, x_i, \ \ldots, \ x_0)$$

$$Y_d(w^*) = (y_{t-1}, \ldots, yi, \ \ldots, \ y_0) \tag{5.38}$$

з довжиною кожної із секретних послідовностей $l(w^*)$.

Кожна множина секретних ключів $X_d\ (w^*), Y_d\ (w^*)$ є частиною секретного (особистого) ключа.

Відкритий ключ механізму POTS обчислюється засобом гешування секретних ключів (5.38) з застосуванням одно направленої чи криптографічної геш-функції f (g). Внаслідок отримуємо t множин по 2 відкритих ключа в кожній:

$$H_d(X) = H(x_{t-1}),\ldots, \mathrm{H}(x_i),\ \ldots,\ \mathrm{H}(x_0)$$
$$H_d(Y) = H(y_{t-1}),\ldots, \mathrm{H}(y_i),\ \ldots,\ \mathrm{H}(y_0) \qquad (5.39)$$

з довжиною геш-значення l_h кожної послідовності секретного ключа.

Підпис повідомлення для механізму POTS. Нехай повідомлення *M* має геш-значення

$$g(M) = h = (h_l, ..., h_i, ..., h_0), \qquad (5.40)$$

яке потрібно підписати з використанням криптографічної геш-функції g.

У загальному випадку, якщо l_h не кратне w^*, то до l_h додається необхідне число нулів, так щоб довжина l_h була кратна w^*. Рядок l_h бітів розділяється на *t* блоків $b_{t-1},...,b_i,...,b_0$ з довжиною *w* бітів кожен. Далі будемо розглядати випадок (5.33) [63].

Для вироблення підпису та його перевірки будемо застосовувати правила, коли довжина блока буде змінюватись. В результаті такого перетворення *w* біт b_i блоку відображаються в *w** біт b_i^* нового блоку, а довжина L_{hi^*} нового блоку b_i^* може бути як більше, так і менше довжини L_{hi} блоку b_i, отриманого внаслідок перетворення (5.31).

Таким чином в механізмі POTS здійснюються такі попередні перетворення:

— рядок l_h бітів геш-значення розділяється на *t* блоків $b_{t-1},...,b_i,...,b_0$ з довжиною *w* бітів кожного блоку;

— w біт b_i блоків відображаються в w^* біт нових b_i^* блоків (причому врахований випадок, коли $b_i^* = b_i$);

— w^* біт нових блоків (5.27) b_i^* зашифровуються з використанням секретного ключа ($X_d(b_i^*), Y_d(b_i^*)$) згідно (5.36)-(5.38) з довжиною кожної із секретних послідовностей $l(w^*)$.

Таким чином, на відміну від механізму Winternitz, в механізмі POTS w біт b_i блоків відображаються в w^* біт b_i^* блоків, які можуть мати як меншу довжину так і більшу по відношенню до w.

В результаті ЕП має такий вигляд [63]

$$\{M; Z^* = (\{x_{t^*-1} \mid y_{t^*-1}\}), \{x_{t^*-2} \mid y_{t^*-2}\}, ..., \{x_i \mid y_i\}, ..., \{x_0 \mid y_0\}) =$$

$$\{M, Z^* = (z_{t^*}, z_{t^*-1}, ..., z_i, ..., z_0)\} \quad (5.41)$$

В (5.41) символ «|» означає, що при зашифрування в ЕП з'являється одна із використаних секретних послідовностей x_i чи y_i, яка визначається і-тим блоком довжини w* бітів. В подальшому параметр t* означає число блоків, яке може бути як більше так і менше t, а також дорівнювати t.

Перевірка підпису для механізму POTS. Перевірка ЕП здійснюється у такій послідовності [62-64].

1). Із використанням криптографічної геш-функції g здійснюється гешування повідомлення M^*, підпис якого перевіряється, в результаті отримується геш-значення

$$h_{Mi^*} = g(M^*, \Pr). \quad (5.42)$$

Якщо довжина h_{Mi^*} не кратна w, то до рядка бітів h_{Mi^*} у відповідності з домовленістю добавляється деяке число нулів, так щоб довжина h_{Mi^*} була кратна w. Рядок h_{Mi^*} бітів розділяється на t* блоків $b_{t^*-1}, ..., b_i, ..., b$ довжини w* бітів кожен.

2). У відповідності зі значеннями b_i блоків h_{Mi^*} із відкритого ключа (5.38) вибираються геш-значення $H(x_i)$ чи $H(y_i)$, внаслідок отримуємо

$$Z^* = (\{H(x_1) \mid H(y_1)\}), \{H(x_2) \mid H(y_2)\}, ..., \{H(x_i) \mid H(y_i)\}, ..., \{H(x_n) \mid H(y_n)\}) =$$

$$(z^*_{t-1}, z^*_{t-2}, ..., z^*_i, ..., z^*_0) \quad (5.43)$$

3). Користувач, який отримав підписане повідомлення, гешує усі послідовності ЕП (5.40), отримує їх геш-значення

$$(H(z_{t^*}), H(z_{t^*-1}), ..., H(z_i), ..., H(z_0)) \quad (5.44)$$

та порівнює отримані значення зі значеннями (5.41), тобто $(z_{t^*}, z_{t^*-1}, ..., z_i, ..., z_0)$. Якщо усі t^* значень при порівнянні співпали, то ЕП вважається справжнім, в іншому випадку – викривленим [63,64].

5.3. Аналіз властивостей ЕП з одноразовими ключами на основі геш-функцій

В даному розділі наведені оцінки та результати порівняння розмірів одноразових ключів та ЕП.

В якості вихідних даних приймемо наступні.

В механізмі Lamport та Lamport-Diffie будемо використовувати значення $n = l_h, w = 1, l_h = 256, 512$. При цьому, довжина секретного та відкритого ключів визначається як $2 \times l_h \times n$, довжина ЕП – як $l_h \times n$.

В механізмі Winternitz будемо використовувати значення $n = l_h, w = 2, 4, 6, 8, 16, l_h = 256, 512$. При цьому, довжина секретного та відкритого ключів визначається як $2 \times w^2 \times n_i \times l_h$, довжина ЕП обчислюється як $l_h \times n_i$.

В удосконаленому механізмі POTS відповідно будемо використовувати значення $l_h = \mu \times n, \mu = 2, 4, 8, 16, 32, 128, 256$. При цьому, довжина секретного та відкритого ключів визначається як $2 \times \mu_i \times l_h$, довжина ЕП обчислюється як $l_h \times \mu_i$.

В таблицях 5.8 – 5.10 наведені результати оцінки розмірів секретних та відкритих одноразових ключів та розмірів ЕП для вказаних механізмів.

Таблиця 5.8

Результати оцінки розмірів секретних та відкритих одноразових ключів та розмірів ЕП для механізмів Lamport та Lamport-Diffie

Розміри даних lh, n		Розмір секретного ключа	Розмір відкритого ключа	Розмір ЕП
256	256	2^{17}	2^{17}	2^{16}
512	512	2^{19}	2^{19}	2^{18}

Таблиця 5.9

Результати оцінки розмірів секретних та відкритих одноразових ключів та розмірів ЕП для механізму Вінтерніц

Розміри даних lh,	n_i	w_i	Розмір секретного ключа	Розмір відкритого ключа	Розмір ЕП
256	128	2	2^{18}	2^{18}	2^{15}
	64	4	2^{19}	2^{19}	2^{14}
	32	8	2^{23}	2^{23}	2^{16}
512	256	2	2^{20}	2^{20}	2^{17}
	128	4	2^{21}	2^{21}	2^{16}
	64	8	2^{25}	2^{25}	2^{17}

Таблиця 5.10

Результати оцінки розмірів секретних та відкритих одноразових ключів та розмірів ЕП для удосконаленого механізму

Розміри даних lh,		w_i	Розмір секретного ключа	Розмір відкритого ключа	Розмір ЕП
256	μ_i	2	2^{10}	2^{10}	2^{9}
		4	2^{11}	2^{11}	2^{10}
		8	2^{12}	2^{12}	2^{11}
		16	2^{13}	2^{13}	2^{12}
		32	2^{14}	2^{14}	2^{13}
		128	2^{16}	2^{16}	2^{14}
		256	2^{17}	2^{17}	2^{16}
512	μ_i	2	2^{11}	2^{11}	2^{10}
		4	2^{12}	2^{12}	2^{11}
		8	2^{13}	2^{13}	2^{12}
		16	2^{14}	2^{14}	2^{13}
		32	2^{15}	2^{15}	2^{14}
		128	2^{17}	2^{17}	2^{16}
		256	2^{18}	2^{18}	2^{17}
		512	2^{19}	2^{19}	2^{18}

Висновки до розділу 5

1. У даному розділі наведені результати порівняльного аналізу алгоритмів квантово-захищених електронних підписів на основі геш-функцій, які показали, що криптографічні схеми, засновані не геш-функціях виглядають перспективними для використання у постквановому періоді за рахунок доказової стійкості геш-функцій проти атак з використанням як класичних, так і квантових комп'ютерів. Іншою перевагою таких схем є їхня гнучкість реалізації, оскільки для одного алгоритму може бути обрана будь-яка геш-функція.

2 Отримані експериментальні результати використання національного стандарту гешування ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування» в алгоритмі XMSS.

3 Розкриті особливості одноразового механізму ЕП Lamport, особливості одноразового механізму ЕП Lamport-Diffie, а також ЕП Winternitz.

4. Наведений *удосконалений* метод одноразових ключів Winternitz для постквантового періоду на основі геш-функцій, який відрізняється від існуючого модифікованими функціями зашифрування та перевірки, що дозволяє зменшити розміри особистого та відкритого ключів у 100 разів.

У цілому результати порівняння досліджених та запропонованого механізму дозволяють зробити такі висновки:

- розміри секретних та відкритих одноразових ключів та розмірів ЕП для механізму Winternitz у порівнянні з механізму Lamport вимагають збільшення розмірів секретних та відкритих одноразових ключів від 2 до 64 разів, але розміри ЕП зменшуються в 2 рази;
- розміри секретних та відкритих одноразових ключів та розмірів ЕП для удосконаленого механізму у порівнянні з механізмом Lamport можуть бути зменшені для довжини ЕП 256 від 2 до 128 разів, а для довжини ЕП 512 від 2 до 512 разів;

— розміри секретних та відкритих одноразових ключів та розмірів ЕП для удосконаленого механізму у порівнянні з механізмом Winternitz для довжини 256 можуть бути зменшені для довжини ЕП 256 від 64 до 256 разів, а для довжини ЕП 512 від 64 до 512 разів. При цьому довжини ЕП зменшуються від 8 до 32разів (для довжини геш-значення 256) , а для довжини512 від 2 до 128 разів [63-64].

5. У п’ятому розділі наведені оцінки та порівняння розмірів одноразових ключів та електронних підписів для розглянутих алгоритмів.

6. Основні положення даного розділу викладені у публікаціях автора [62-66, 68]

ВИСНОВКИ

В дисертаційній роботі розв’язана актуальна задача розробка моделей і методів забезпечення стійкості та резильєнтності систем електронних довірчих послуг у постквантовий період та досягнення мета – розробка методів забезпечення надійної і безпечної роботи систем електронних довірчих за рахунок використання технології blockchain та постквантової криптографії. В цілому можна зробити наступні висновки.

1. Проведений в рамках дисертаційних досліджень аналіз [6, 7] показав, що в найближчий час довіра до інформаційних систем, які обробляють критичну інформацію, без засобів квантово-захищеної криптографії буде неможлива через різкий та стрімкий розвиток квантових обчислень. Відповідно до теореми Mosco [4] встановлено, що в разі якщо квантовий комп’ютер буде побудований до того, як існуюча інфраструктура стане стійкою до квантового криптоаналізу, а необхідний час забезпечення таємниці ще не минув, виникає ситуація, що критичні дані стають незахищеними.

2. Проведений аналіз міжнародних вимог до алгоритмів у постквантовий період [8, 9, 14-17] показав, що такі вимоги формуються виходячи із цільового призначення, а саме: вимоги стійкості, техніко-економічні та техніко-експлуатаційні вимоги. В роботі висвітлені існуючі основні напрямки розробки нових квантово-захищених алгоритмів, а саме: криптографічні перетворення на основі завадостійких кодів, перетворення на основі геш-функцій, криптографічні перетворення на решітках, мультіваріативно-квадратичні криптографічні перетворення, а також використання ізогеніїв еліптичних кривих. Розкриті сутності актуальних моделей загроз для постквантового періоду для примітивів типу шифрування (IND-CCA2) та електронного підпису (EUF-CMA).

3. В роботі встановлено, що безпека систем, які можуть протистояти атакам із використанням квантових комп’ютерів, може забезпечуватися не лише за допомогою використання стійких постквантових алгоритмів, а також за

допомогою організаційних, організаційно-технічних рішень та методів. Розкрито поняття резильєнтності систем та показано, що резильєнтність систем надання електронних довірчих послуг може забезпечуватися за допомогою переходу на децентралізовані архітектурні рішення, а також за рахунок використання технології blockchain. Більше того, можливість системи продовжувати функціонувати в умовах кібератак, а також швидко відновлювати роботу після виступає ще однією характеристикою резильєнтності, яка не може бути забезпечена виключно за рахунок параметрів стійкості криптопримітивів.

4. Дисертаційні дослідження показали, що децентралізовані системи здатні краще забезпечити функціонування електронних систем в умовах збільшення спектру електронних послуг та зростання кількості користувачів, оскільки вони позбавлені недоліку «традиційних» систем, які зазвичай мають порогове навантаження після перевищення якого ефективність функціонування системи знижується. Обґрунтовано, що для надійного функціонування децентралізованих систем (в тому числі у критичних інфраструктурах) можливе використання технології blockchain із децентралізованими протоколами консенсусу. Зроблений висновок, що вона здатна забезпечувати довіру між користувачами системи в умовах взаємної недовіри без залучення сторонніх гарантів, тим самим значно зменшуючи ймовірність загрози підкупу або зловмисної змови між можливими внутрішніми порушниками. Проведений аналіз [18-30] дозволив сформулювати рекомендації щодо використання децентралізованих протоколів консенсусу, які зазначають, що вибір протоколу консенсусу має базуватися насамперед на умовах, в яких передбачається функціонування системи.

5. Успішне впровадження сучасних технологій електронного урядування, а також електронних довірчих послуг не можливо без створення відповідної інфраструктури на національному рівні. Відповідною інфраструктурою реалізації є інфраструктура відкритих ключів (ІВК), яка спирається на довіру між користувачами в умовах функціонування системи а

рамках моделі взаємної недовіри. Для того, щоб система ІВК могла бути реалізована, одна із семи запропонованих у [31] моделей довіри має бути надійно реалізована. Проведений аналіз розгорнутої національно ІВК показав, що її ієрархічна структура має ряд недоліків, таких як: залежність безпеки всієї системи від кореневого сертифікату, неможливість користувачів самостійно в повній мірі розпоряджатися власними ідентифікаційними даними, відсутність інфтероперабельності системи ІВК, накопичення дублікатів цифрових ідентичностей для однієї фізичної особи тощо. В дисертаційній роботі *удосконалена* модель децентралізованої інфраструктури відкритих ключів на основі технології blockchain, яка відрізняється від існуючих тим, що дозволяє надійно реалізувати модель довіри, сконцентрованої навколо користувача, що дозволяє використовувати її для побудови системи електронного голосування. Запропонована модель децентралізованої ІВК передбачає значне зниження витрат на її утримання, можливість для користувачів самостійно розпоряджатися власними даними, легку масштабованість та інтеоперабельність. Відмічається, що резильєнтність децентралізованої ІВК на основі технології blockchain буде вищою ніж у існуючої ієрархічної структури, оскільки при запровадженні децентралізованого підходу до побудови зникає ціль для направленої зловмисної атаки, а також децентралізована система здатна продовжувати нормально функціонувати в умовах кібератак або випадкових збоїв. Застосування викладеного підходу дозволить полегшити перехід на нові алгоритми підписів, зокрема на постквантові, в яких стійкість залежить не від криптоперіода ключа (3 роки, 5 років), а від кількості накладених підписів (наприклад, в hash-based підписах). Виходячи з цього, технологія blockchain дозволить більш раціонально управляти сертифікатами відкритих ключів. Архітектура удосконаленої моделі децентралізованої інфраструктури відкритих ключів на основі технології blockchain побудована таким чином, що вона може бути використана для розгортання системи електронного голосування без функціональних змін.

6. В дисертаційній роботі за допомогою розробленого програмного забезпечення отримані результати часових оцінок для формування децентралізованої ІВК для різних топологій мереж та виходячи із різних початкових умов. Аналіз отриманих оцінок підтвердив перевагу децентралізованих систем з огляду на нульову кількість легітимних користувачів, які можуть позбавитися можливості використання системи в умовах зловмисних чи випадкових збоїв, кібератак.

7. В ході проведеного аналізу [38-42] в рамках дисертаційних досліджень було встановлено, що електронне віддалене голосування виглядає перспективним з точки зору зручності для як для виборців, так і для відповідальних за проведення процедури волевиявлення. Проте встановлено, що реалізація існуючих системи електронного голосування є достатньо трудоємким, оскільки передбачає імплементацію складних алгоритмів взаємодії із використанням сліпих електронних підписів. В роботі *удосконалена* модель системи електронного голосування, яка відрізняється від існуючих тим, що забезпечує формування деперсоналізованого списку виборців без використання сліпих підписів, що дозволяє спростити алгоритми взаємодії між сторонами. Запропонована модель зберігає переваги існуючих систем електронного голосування, таких як Fujiok-Okamoto-Ohta, Sensus, а також протоколу He-Su без реалізації сліпих підписів, що дозволить знизити складність впровадження. Система електронного голосування охоплює процеси на чотирьох рівнях: нормативний, організаційний, рівень процесів, технологічний; сформульовані процеси, які відбуваються на кожному із чотирьох рівнях, а також показаний взаємозв’язок між ними.

8. Для легшого розгортання системи на національному рівні, а також забезпечення інтероперабельності, розроблена дворівнева архітектура системи електронного голосування, яка дозволяє забезпечити процеси електронної ідентифікації за допомогою вже існуючих засобів, таких як BankID, MobileID, електронний підпис. Також в роботі розроблені алгоритми та протоколи для децентралізованої системи електронного голосування, які впроваджені у

комплексі для проведення досліджень криптографічних властивостей технології blockchain.

9. Проведений аналіз показав, що електронні підписи на основі геш-функцій виглядають перспективними для використання у постквантовий період за рахунок доказової стійкості геш-функцій, а також за рахунок гнучкості вибору механізму одноразових підписів та геш-функцій. В рамках роботи було проведено порівняльний аналіз методом ієрархій чотирьох схем електронного підпису для постквантового періоду: Leighton-Micali, XMSS, SPHINCS. Для порівняння використовувалися три рівні ієрархій та вісім критеріїв, серед яких: стійкість, актуальність моделі загроз, довжина відкритого ключа та довжина підпису. Для алгоритму XMSS були отримані експериментальні результати використання національного стандарту гешування ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування».

10. За результатами аналізу таких схем одноразового підпису, як: ЕП Lamport-Diffie, а також ЕП Winternitz видно, що розміри ключів та підпису є досить високими, що в подальшому ускладнить процес використання таких алгоритмів. Було показано, що розміри секретних та відкритих одноразових ключів та розмірів ЕП для механізму Winternitz у порівнянні з механізму Lamport вимагають збільшення розмірів секретних та відкритих одноразових ключів від 2 до 64 разів, але розміри ЕП зменшуються в 2 рази. В дисертаційній роботі *удосконалено* метод одноразових ключів Winternitz для постквантового періоду на основі геш-функцій, який відрізняється від існуючого модифікованими функціями зашифрування та перевірки, що дозволяє зменшити розміри особистого та відкритого ключів у 100 разів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

2. Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market – COM/2012/0238 Final - 2012/0146 (COD).

3. Регламент (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та скасування Директиви 1999/93 / ЄС

4. Mosca M. Setting the Scene for the ETSI Quantum-safe Cryptography Workshop // E-proceedings of «1st Quantum-Safe-Crypto Workshop», Sophia Antipolis, Sep 26-27.

5. Lily Chen. Report on Post-Quatum Cryptography. NISTIR 8105 (DRAFT) // NIST. URL: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.

6. ETSI GR QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework.

7. Neal Koblitz, Menezes Alfred J.. A riddle wrapped in an enigma // Eprint.iacr. 2018. URL: https://eprint.iacr.org/2015/1018.pdf

8. Горбенко І. Д.,, Кузнєцов О. О., Потій О. В., Горбенко Ю. І., Ганзя Р. С., Пономар В. А.. Постквантова криптографія та механізми її реалізації // Радиотехника. 2016. Вип. 186. С. 32–52.

9. Merkle Ralph. A certified digital signature. In Gilles Brassard, editor, Advances inCryptology // 1990. CRYPTO ’89. Vol. 3.35 of LNCS, P. 218–238.

10. Потій О. В., Ісірова К. В. Аналіз вимог та моделей безпеки для постквантової криптографії // Математичне та комп'ютерне моделювання. Серія: Технічні науки. 2017. Вип. 15. С. 192-197. DOI:

https://doi.org/10.32626/2308-5916.2017-15 URL: http://mcm-tech.kpnu.edu.ua/article/view/112043/106880

11. Isirova K., Potii O. Requirements and Security Models for Post-Quantum Cryptography Analysis. *ICTERI PhD Symposium*: Proccedings of ICTERI PhD Symposium, Kyiv, 16-17 May 2017, Kyiv: IEEE, 2017. P. 36-41. (SCOPS).URL: http://ceur-ws.org/Vol-1851/paper-6.pdf

12. Потій О. В., Горбенко І. Д., Ісірова К. В. Міжнародні вимоги до криптоалгоритмів у постквантовий період. *XII Міжнародна науково-практична конференція «Теоретичні та прикладні аспекти побудови програмних систем»:* Збірник матеріалів XII Міжнародної науково-практичної конференції «Теоретичні та прикладні аспекти побудови програмних систем», 5-9 грудня 2016, Київ: Київський Національний університет імені Тараса Шевченка, 2016. С. 215.

13. Потій О. В., Ісірова К. В. Аналіз вимог та моделей безпеки для постквантової криптографії. *II Науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем»* : Збірник матеріалів II Науково-практичної конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем», 23-24 березня, Київ: Київський національний університет імені Тараса Шевченка, 2017. С. 163.

14. Post-Quantum Cryptography. URL: https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

15. Canetti Ran, Krawczyk Hugo. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. URL: http://iacr.org/archive/eurocrypt2001/20450451.pdf.

16. Shoup V. On Formal Models for Secure Key Exchange, Theory of Cryptography Library, 1999. URL: http://philby.ucsd. edu/cryptolib/1999/9912.html.

17. Yoshida Y., Morozov K., Tanaka K.CCA2 Key-Privacy for Code-Based Encryption in the Standard Model. Post-Quantum Cryptography. PQCrypto 2017. Lecture Notes in Computer Science, Vol. 10346. Springer, Cham.

18. . Aniello L., Baldoni R., Gaetani E., Lombardi F., Margheri A., Sassone V. A prototype eval-uation of a tamper-resistant high performance blockchain-based transaction log for a distributed database // EDCC. IEEE, 2017.

19. Cachin C., Guerraoui R., Rodrigues L. Introduction to reliable and secure distributed programming // Springer, 2011.

20. Ісірова К. В., Потій О. В. Децентралізовані протоколи консенсусу: можливості та рекомендації щодо використання // Радіотехніка. 2018 Вип. 195. С. 203-208. DOI: https://doi.org/10.30837/rt.2018.4.195.20 URL: http://rt.nure.ua/article/view/175202

21. Garay J. A., Kiayias A., Leonardos N. The Bitcoin Backbone Protocol // Analysis and Applications, volume 9057 of LNCS, pages 281{310. Springer, 2015.

22. Kiayias Aggelos Panagiotakos Giorgos. On Trees, Chains and Fast Transactions in the Blockchain Yonatan Sompolinsky and Aviv Zohar. PHANTOM: A Scalable BlockDAG protocol

23. Bernardo Machado David, Gazi Peter, Kiayias Aggelos, Russell Alexander. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake protocol. IACR Cryptology ePrint Archive, 2017:573, 2017.

24. Danezis George, Meiklejohn Sarah. Centrally banked cryptocurrencies // 23nd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016. The Internet Society, 2016.

25. Http-based seeding specification URL: http://www.bittornado.com/docs/webseed-spec.txt (дата звернення 10.10.2020)

26. Castro M., Liskov B. Practical byzantine fault tolerance and proactive recovery // ACM Trans. Comput. Syst., 20(4):398-461, 2002.

27. Algorand Whitepaper: https://www.algorand.com/docs/whitepapers/

28. Baird Leemon. The swirlds hashgraph consensus algorithm: fair, fast, byzantine fault tolerance.

29. Mingxiao D., Xiaofeng M., Zhe Z., Xiangwei W., Qijun C. A review on consensus algorithm of blockchain

30. Tromp J. Cuckoo Cycle; a memory bound graph-theoretic proof-of-work // Financial Cryptography and Data Security: BITCOIN 2015 : journal. — Springer, 2015. — P. 49—62.

31. ISO / IEC 9594-8 and ITU-T X.509. (2017). Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and aribute certificate frameworks.

32. Потий А. В., Леншин А. В., Сорока Л. С., Есин В. И., Мороз Б. И. Инфраструктура открытых ключей: технологии, архитектура, построение и внедрение: учебное пособие // Днепропетровск: Академия пограничной службы Украины 2011.- 202 с.

33. Исирова Е. В., Потий А. В., Семенец В. В. Принципы построения децентрализованной инфраструктуры открытых ключей // Радиотехника. 2018. Вып. 193. С. 82-93. URL: http://rt.nure.ua/article/view/175717

34. Isirova K., Potii O., Claussen J. C. Establishing trust protocols in mutual distrust network by consensus formation // Radiotekhnika. Is. 198. P. 96-104 DOI: https://doi.org/10.30837/rt.2019.3.198.07 URL: http://rt.nure.ua/article/view/184662

35. Isirova K. Blockchain Technology as the Prospective Instrument for Ensuring Electronic Trust Services in Conditions of Cyberthreats // European Cybersecurity Journal. 2018. Vol. 5. Is. 1. P 34-43 URL: https://cybersecforum.eu/wp-content/uploads/2020/08/ECJ-VOLUME-5-2019-ISSUE-1.pdf

36. Isirova K., Potii O. Decentralized public key infrastructure development principles. *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)* : Proccedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), 24-27 May, 2018, Kyiv: IEE, 2018. P. 305-310 (SCOPUS).

37. Ісірова К. В., Потій О. В. Принципи побудови децентралізованої інфраструктури відкритих ключів. *XX Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах»* : Збірник матеріалів XX міжнародної науково-практичної

конференції «Безпека інформації в інформаційно-телекомунікаційних системах», 22 травня, Київ: Державна служба спеціального зв'язку та захисту інформації України, 2018. С. 110-112.

38. E-voting world map URL: https://www.e-voting.cc/en/it-elections/world-map/ (дата звернення 11.11.2020).

39. Nurmi Hannu, Salomaa Arto. Conducting secret ballot elections in computer networks: Problems and solutions // Annals of Operations Research 51 (1994) 185-194. — University of Turku.

40. Nurmi, H., Salomaa, A., an Santean, L. Secret ballot elections in computer networks. Computers and Security, 36, 10 (1991), pp. 553-560.

41. Fujioka, A., Okamoto, T., Ohta, K.: A Practical Secret Voting Scheme for Large Scale Elections. In: ASIACRYPT '92. LNCS, Springer (1993) 244–251

42. Qi He, Zhongmin Su. A New Practical Secure e-Voting Scheme (1998)

43. Конституція України : офіц. текст. Київ : КМ, 2013. 96 с.

44. Про вибори депутатів Верховної Ради Автономної Республіки Крим, місцевих рад та сільських, селищних, міських голів : Закон України від 10.07.2010 р. № 2487-VI. Дата оновлення: 08.08.2015. URL: https://zakon.rada.gov.ua/laws/show/2487-17#Text (дата звернення: 15.11.2020).

45. Про вибори президента України : Закон України від 05.03.199 р. № 474-XIV. Дата оновлення 01.01.2020. URL: https://zakon.rada.gov.ua/laws/main/474-14#Text (дата звернення: 15.11.2020).

46. Про електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. Дата оновлення: 13.02.2020. URL: https://zakon.rada.gov.ua/laws/main/2155-19#Text (дата звернення: 15.11.2020).

47. Julien P. Stern. A New and Efficient All-Or-Nothing Disclosure of Secrets Protocol

48. Brassard G., Crepeau C., Robert J.-M. All-or-nothing disclosure of secrets // Springer Lecture Notes in Computer Science 263(1987)

49. Kohno T., Stubblefield A., Rubin A. D., Wallach D. S. Analysis of an electronic voting system // IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004, Berkeley, CA, USA, 2004, pp. 27-40.

50. Ісірова К. В., Потій О. В. Принципи побудови електронної системи таємного голосування з використанням децентралізованих технологій // Радіотехніка. 2019. Вип. 199. С. 121-129. DOI: https://doi.org/10.30837/rt.2019.4.199.15 URL: http://rt.nure.ua/article/view/194028

51. Горбенко І.Д., Онопрієнко В.В., Горбенко Ю.І., Кузнецов О.О., Ісірова К.В., Родінко М.Ю. Проблеми, принципи побудови та перспективи розвитку національної системи електронного голосування в Україні // Радіотехніка. 2020. Вип. 200, С. 85-97 DOI: https://doi.org/10.30837/rt.2020.1.200.08 URL: http://rt.nure.ua/article/view/210067

52. Isirova K., Potii O. Development Principles for Electronic Voting System Using Distributed Ledger Technology. *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*: Proccedings of *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT),* 14-18 May, 2020, Kyiv: IEEE, 2020. P. 446-450 (SCOPUS).

53. Isirova K., Kiian A., Rodinko M., Kuznetsov A.. Decentralized electronic voting system based on blockchain technology developing principals. *2020 Third International Workshop on Computer Modeling and Intelligent Systems (CMIS)*. Proccedings of 2020 Third International Workshop on Computer Modeling and Intelligent Systems (CMIS), 27 April – 1 May, Zaporizhzhia 2020. P. 211-223 (SCOPUS).

54. Leslie Lamport. Constructing digital signatures from a one way function. Technical // Report SRI-CSL-98, SRI International Computer Science Laboratory, 1979.

55. Andreas Hülsing. W-OTS+ – shorter signatures for hash-based signature schemes // Progress. in Cryptology – AFRICACRYPT 2013. Vol. 7918 of LNCS. P. 173–188.

56. Daniel J. Bernstein; Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, Zooko Wilcox-O'Hearn. SPHINCS: practical stateless hash-based Signatures // Lecture Notes in Computer Science. 2015. Vol. 9056

57. I. Gorbenko, V. Ponomar. Examining a possibility to use and the benefits of post-quantum algorithms dependent on the conditions of their application // EasternEuropean Journal of Enterprise Technologies. 2017. Vol. 2, Issue 9-86. P. 21-32. URL: http://journals.uran.ua/eejet/article/view/96321/93.881.

58. Ю. І.Горбенко, Т. В.Мельник, І. Д.Горбенко. Аналіз потенційних постквантових електронних підписів на основі геш – функцій // Радиотехніка. 2017. – Вип. 189. С. 115131.

59. Н. В. Ковалёва, И. Д. Горбенко. Анализ постквантовых механизмов цифровой подписи на основе хеш-функций // Прикладная радиоэлектроника. 2016. Том 15. №3. – С. 103-113.

60. Ю. І. Горбенко Під заг. Ред. Горбенко І. Д. Методи побудування та аналізу, стандартизація та застосування КРСМ. Монографія. Форт. Харків, 2015. 958с.

61. Ю. І. Горбенко, Р. С. Ганзя. Аналіз стійкості популярних криптоситем проти квантового криптоаналізу на основі алгоритму Гровера. Захист інформації. 2014. С. 22-28

62. Gorbenko Yu. I., Isirova K. V. Improved Mechanism of One-Time Keys for Post-Quantum Period Based on the Hashing Functions // Telecommunications and Radio Engineering. 2018. Vol. 77. Is. 14. P. 1277-1296. (SCOPUS). DOI: 10.1615/TelecomRadEng.v77.i14.50
URL:http://www.dl.begellhouse.com/journals/0632a9d54950b268,65ffeeb16fd38695,40df0aea4f078f90.html

63. Горбенко Ю.І., Ісірова К.В. Удосконалений механізм одноразових ключів для постквантового періоду на основі геш-функцій // Радіотехніка. 2017. Вип. 191, С. 24-39. URL: https://nure.ua/wp-content/uploads/2017/Scientific_editions/191/5.pdf

64. Gorbenko Yu., Isirova K. Improved mathematical model of the post-quantum eletronic signature mechanism // COMPUTER SCIENCE AND CYBERSECURITY. 2018. Is. 4(12). P. 22-28. URL: https://periodicals.karazin.ua/cscs/article/view/12249/11723

65. Isirova K., Potii O., Gorbenko Yu. Post Quantum Hash Based Digital Signatures Comparative Analysis. Features of their Implementation and Using in Public Key Infrastructure. *2017 4th International scientific-practical conference problems of infocommunications-science and technology (PIC S&T)*: Proccedings of 2017 4th International scientific-practical conference problems of infocommunications-science and technology (PIC S&T), 10-13 October, 2017. Kharkiv, 2017. P. 105-109. (SCOPUS).

66. Горбенко Ю. І., Ісірова К. В. Сценарії створення та перевірки вдосконалених електронних підписів в мобільному середовищі. *XI Міжнародна науково-практична конференція «Теоретичні та прикладні аспекти побудови програмних систем»* : Збірник матеріалів XI Міжнародної науково-практичної конференції «Теоретичні та прикладні аспекти побудови програмних систем», 15-17 грудня, 2014, Київ: Київський Національний університет імені Тараса Шевченка, 2014. С. 75.

67. Ю. І. Горбенко, І. Д. Горбенко. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика. – Харків: Форт, 2010. – 593с.

68. Потій О. В., Ісірова К. В., Карпенко А. С. Особливості реалізації квантово-захищених цифрових підписів на основі геш-функцій. *XIX Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах»* : Збірник матеріалів XIX міжнародної науково-практичної конференції «Безпека інформації в

інформаційно-телекомунікаційних системах», 25-26 травня, Київ: Державна служба спеціального зв'язку та захисту інформації України, 2017. С. 84-85.

69. I. Gorbenko, A. Kuznetsov, Yu. Gorbenko, S. Kavun, O. Kachko, M. Yesina. Electronic Signature Mechanisms. The Current State, the Existing Contradictions and Prospects of Practical Use for the Post-Quantum Period: Monograph. – ASC Academic Publishing, USA, 2017. – 165 p.

70. Saaty, Thomas L. Relative Measurement and its Generalization in Decision Making: Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors - The Analytic Hierarchy/Network Process (англ.) // RACSAM (Review of the Royal Spanish Academy of Sciences, Series A, Mathematics) : journal. — 2008. — June (vol. 102, no. 2). — P. 251—318.

71. W. Diffie, M. Hellman New Directions in Cryptography // IEEE Trans on Information Theory IT-22 (November 1976), 644-654

72. L. Aniello, R. Baldoni, E. Gaetani, F. Lombardi, A. Margheri, and V. Sassone. A prototype evaluation of a tamper-resistant high performance blockchain-based transaction log for a distributed database. In EDCC. IEEE, 2017.

73. C. Cachin, R. Guerraoui, and L. Rodrigues. Introduction to reliable and secure distributed programming. Springer, 2011

74. J. A. Garay, A. Kiayias, and N. Leonardos. The Bitcoin Backbone Protocol: Analysis and Applications, volume 9057 of LNCS, pages 281-310. Springer, 2015.

75. Merkle, Ralph Charles. Secrecy, authentication, and public key systems : Technical Report No. 1979-1. — Citeseer, 1979. — doi:10.1.1.637.3952

76. Stefano De Angelis; Leonardo Aniello1; Roberto Baldoni1,Federico Lombardi;Andrea Margheri and Vladimiro Sassone. PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain

77. Nojima R., Imai H., Kobara K., Morozov K.: Semantic security for the mceliece cryptosystem without random oracles. Des. Codes Cryptography 49(1-3), 289–305 (2008)

78. Dods, Chris and Smart, Nigel P and Stam, Martijn. Hash based digital signature schemes // IMA International Conference on Cryptography and Coding. — Springer Berlin Heidelberg, 2005. — С. 96—115. — doi:10.1007/11586821_8

79. Ісірова К. В. Бизнес модель информационной безопасности. *Науково-технічна конференція «Інформаційна безпека України»* : Збірник матеріалів науково-технічної конференції «Інформаційна безпека України», 12-13 березня 2015, Київ: Київський національний університет імені Тараса Шевченка, 2015. С. 109.

80. Ісірова К. В. Застосування електронних підписів для забезпечення кібернетичної безпеки. *Науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем»* : Збірник матеріалів Науково-практичної конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем», 10-11 березня 2016, Київ: Київський національний університет імені Тараса Шевченка, 2016. С. 42.

81. George Danezis, Sarah Meiklejohn. Centrally banked cryptocurrencies. In 23nd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016. The Internet Society, 2016.

82. Madeline Gonzarlez Muniz, Rainer Steinwandt: Security of signature schemes in the presence of key-dependent messages. In Tatra Mt. Math. Publ. 47 (2010), 15–29

83. Rabin M. Digitalized Signatures. In Foundations of Secure Computing // Academic Press (1978). P. 155-168

Додаток А

Список публікацій здобувача за темою дисертації

Наукова публікація у періодичному науковому виданні держави, яка входить до Організації економічного співробітництва та розвитку, включеному до наукометричної бази Scopus

1. Gorbenko Yu. I., Isirova K. V. Improved Mechanism of One-Time Keys for Post-Quantum Period Based on the Hashing Functions // Telecommunications and Radio Engineering. 2018. Vol. 77, Is. 14. P. 1277–1296. DOI: 10.1615/TelecomRadEng.v77.i14.50 (Scopus, United States of America).
   URL: https://www.scopus.com/record/display.uri?eid=2-s2.0-85053395224&origin=resultslist
   (Особистий внесок здобувача: удосконалена математична модель постквантового електронного підпису POTS).

Наукові публікації у фахових виданнях України

2. Потій О. В., Ісірова К. В. Аналіз вимог та моделей безпеки для постквантової криптографії // Математичне та комп'ютерне моделювання. Серія: Технічні науки. 2017. Вип. 15. С. 192–197.
   DOI: https://doi.org/10.32626/2308-5916.2017-15
   URL: http://mcm-tech.kpnu.edu.ua/article/view/112043/106880
   (Особистий внесок здобувача: обґрунтування моделей безпеки для постквантової криптографії, модель безпеки IND-CCA2, модель безпеки EUF-CMA).
3. Исирова Е. В., Потий А. В., Семенец В. В. Принципы построения децентрализованной инфраструктуры открытых ключей // Радиотехника. 2018. Вып. 193. С. 82–93.
   URL: http://rt.nure.ua/article/view/175717
   (Особистий внесок здобувача: опис існуючої інфраструктури відкритих ключів, проблемні питання побудови, концепція побудови PKI на основі технології blockchain).

4. Ісірова К. В., Потій О. В. Децентралізовані протоколи консенсусу: можливості та рекомендації щодо використання // Радиотехника. 2018. Вып. 195. С. 203–208. DOI: https://doi.org/10.30837/rt.2018.4.195.20 URL: http://rt.nure.ua/article/view/175202 *(Особистий внесок здобувача: призначення протоколів консенсусу, порівняльний аналіз протоколів консенсусу)*.
5. Isirova K., Potii O., Claussen J. C. Establishing trust protocols in mutual distrust network by consensus formation // Радиотехника. Вып. 198. С. 96–104. DOI: https://doi.org/10.30837/rt.2019.3.198.07 URL: http://rt.nure.ua/article/view/184662 *(Особистий внесок здобувача: формування довіри у комп'ютерних мережах, принципи розробки децентралізованої PKI, протокол встановлення консенсусу в ієрархічній структурі, протокол встановлення консенсусу в децентралізованій структурі)*.
6. Ісірова К. В., Потій О. В. Принципи побудови електронної системи таємного голосування з використанням децентралізованих технологій // Радіотехніка. 2019. Вип. 199. С. 121–129. DOI: https://doi.org/10.30837/rt.2019.4.199.15 URL: http://rt.nure.ua/article/view/194028 *(Особистий внесок здобувача: принципи електронних систем голосування, система електронного голосування на основі децентралізованих принципів, принципи побудови децентралізованої системи електронного голосування)*.
7. Горбенко І. Д., Онопрієнко В. В., Горбенко Ю. І., Кузнецов О. О., Ісірова К. В., Родінко М. Ю. Проблеми, принципи побудови та перспективи розвитку національної системи електронного голосування в Україні // Радіотехніка. 2020. Вип. 200. С. 85–97. DOI: https://doi.org/10.30837/rt.2020.1.200.08 URL: http://rt.nure.ua/article/view/210067 *(Особистий внесок здобувача: обґрунтування вимог та умов застосування національної системи електронного голосування в Україні, обґрунтування структури та основних складових національної системи електронного голосування в Україні)*.

Публікації, які додатково відображають наукові результати дисертації

8. Isirova K. Blockchain Technology as the Prospective Instrument for Ensuring Electronic Trust Services in Conditions of Cyberthreats // European Cybersecurity Journal. 2018. Vol. 5. Is. 1. P 34-43
URL: https://cybersecforum.eu/wp-content/uploads/2020/08/ECJ-VOLUME-5-2019-ISSUE-1.pdf
9. Горбенко Ю. І., Ісірова К. В. Удосконалений механізм одноразових ключів для постквантового періоду на основі геш-функцій // Радіотехніка. 2017. Вип. 191, С. 24–39.
URL: https://nure.ua/wp-content/uploads/2017/Scientific_editions/191/5.pdf
(Особистий внесок здобувача: постановка проблеми та можливості її вирішення, дослідження захищеності механізму POTS).
10. Gorbenko Yu., Isirova K. Improved mathematical model of the post-quantum eletronic signature mechanism // COMPUTER SCIENCE AND CYBERSECURITY. 2018. Is. 4(12). P. 22–28.
URL: https://periodicals.karazin.ua/cscs/article/view/12249/11723
(Особистий внесок здобувача: удосконалений механізм одноразових ключів для постквантового періоду POTS).

Наукові праці, які засвідчують апробацію матеріалів дисертації

11. Isirova K., Potii O. Requirements and Security Models for Post-Quantum Cryptography Analysis // ICTERI PhD Symposium : Proccedings of ICTERI PhD Symposium, 16–17 May 2017. Kyiv, 2017. P. 36–41. (SCOPUS).
URL: http://ceur-ws.org/Vol-1851/paper-6.pdf
(Особистий внесок здобувача: обґрунтування моделей безпеки для крипто алгоритмів у постквантовий період, модель безпеки для шифрування, модель безпеки для електронного підпису).
12. Isirova K., Potii O., Gorbenko Yu. Post Quantum Hash Based Digital Signatures Comparative Analysis. Features of their Implementation and Using in Public Key Infrastructure // Problems of infocommunications-science and technology

(PIC S&T): Proccedings of International scientific-practical conference, 10–13 October 2017. Kharkiv, 2017. P. 105–109. (SCOPUS).

(Особистий внесок здобувача: результати порівняння алгоритмів квантово-захищених цифрових підписів на основі геш-функцій).

13. Isirova K., Potii O. Decentralized public key infrastructure development principles // Dependable Systems, Services and Technologies (DESSERT) : Proccedings of International Conference, 24–27 May 2018. Kyiv, 2018. P. 305–310. (SCOPUS).

(Особистий внесок здобувача: принципи побудови децентралізованої інфраструктури відкритих ключів).

14. Isirova K., Potii O. Development Principles for Electronic Voting System Using Distributed Ledger Technology // Dependable Systems, Services and Technologies (DESSERT) : Proccedings of International Conference on Dependable Systems, Services and Technologies (DESSERT), 14–18 May 2020. Kyiv, 2020.
P. 446–450. (SCOPUS).

(Особистий внесок здобувача: принципи побудови децентралізованої системи електронного голосування).

15. Isirova K., Kiian A., Rodinko M., Kuznetsov A. Decentralized electronic voting system based on blockchain technology developing principals // Computer Modeling and Intelligent Systems (CMIS) : Proccedings International Workshop,
27 April – 1 May 2020. Zaporizhzhia, 2020. P. 211–223. (SCOPUS).

(Особистий внесок здобувача: архітектура децентралізованої системи електронного голосування, протокол голосування у децентралізованій системі електронного голосування).

16. Горбенко Ю. І., Ісірова К. В. Сценарії створення та перевірки вдосконалених електронних підписів в мобільному середовищі // Теоретичні та прикладні аспекти побудови програмних систем : Збірник матеріалів XI Міжнародної науково-практичної конференції, 15–17 грудня 2014 р. Київ, 2014. С. 75.

(Особистий внесок здобувача: сценарії створення та перевірки вдосконалених електронних підписів в мобільному середовищі).

17. Ісірова К. В. Бизнес модель информационной безопасности // Інформаційна безпека України : Збірник матеріалів науково-технічної конференції, 12–13 березня 2015 р. Київ, 2015. С. 109.
18. Ісірова К. В. Застосування електронних підписів для забезпечення кібернетичної безпеки // Проблеми кібербезпеки інформаційно-телекомунікаційних систем : Збірник матеріалів Науково-практичної конференції, 10–11 березня 2016 р. Київ, 2016. С. 42.
19. Потій О. В., Горбенко І. Д., Ісірова К. В. Міжнародні вимоги до криптоалгоритмів у постквантовий період // Теоретичні та прикладні аспекти побудови програмних систем : Збірник матеріалів XII Міжнародної науково-практичної конференції, 5–9 грудня 2016 р. Київ, 2016. С. 215.
(Особистий внесок здобувача: аналіз міжнародних вимог до криптоалгоритмів у постквантовий період).
20. Потій О. В., Ісірова К. В. Аналіз вимог та моделей безпеки для постквантової криптографії // Проблеми кібербезпеки інформаційно-телекомунікаційних систем : Збірник матеріалів II Науково-практичної конференції, 23–24 березня 2017 р. Київ, 2017. С. 163.
(Особистий внесок здобувача: аналіз моделей безпеки для постквантової криптографії).
21. Потій О. В., Ісірова К. В., Карпенко А. С. Особливості реалізації квантово-захищених цифрових підписів на основі геш-функцій // Безпека інформації в інформаційно-телекомунікаційних системах : Збірник матеріалів XIX міжнародної науково-практичної конференції, 25–26 травня 2017 р. Київ, 2017. С. 84–85.
(Особистий внесок здобувача: порівняльний аналіз алгоритмів квантово-захищенних цифрових підписів на основі геш-функцій та особливості їхньої реалізації).

22. Ісірова К. В., Потій О. В. Принципи побудови децентралізованої інфраструктури відкритих ключів // Безпека інформації в інформаційно-

телекомунікаційних системах : Збірник матеріалів XX міжнародної науково-практичної конференції, 22 травня 2018 р. Київ, 2018. С. 110–112. *(Особистий внесок здобувача: принципи побудови інфраструктури відкритих ключів із використання технології blockchain).*

Додаток Б

Акт впровадження результатів дисертаційної роботи у наукову роботу кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна

"ЗАТВЕРДЖУЮ"

Проректор з наукової роботи
Харківського національного університету
імені В.Н. Каразіна
проф. _____ В.О. Катрич
« 10 » 04 2020 р.

АКТ
впровадження результатів дисертаційної роботи
на здобуття ступеня доктора філософії
Ісірової Катерини Володимирівни
у наукову роботу кафедри безпеки інформаційних систем і технологій
Харківського національного університету імені В.Н. Каразіна

Комісія у складі голови комісії, доктора технічних наук, професора Кузнецова О.О. та членів комісії, доктора технічних наук, професора Горбенко І.Д., доктора технічних наук, доцента Рассомахіна С.Г., встановила, що у Харківському національному університеті імені В.Н. Каразіна впроваджені результати дисертаційних досліджень, що одержані Ісіровою Катериною Володимирівною при виконанні науково-дослідної роботи № 1-41-18 «Аналіз, дослідження, розробка та стандартизація криптографічних систем для захисту інформації в постквантовому середовищі, в умовах інформаційних і гібридних війн» (№ ДР 0118U002024) в частині розробки архітектури децентралізованої системи електронного голосування.

Голова комісії, д.т.н., професор О.О. Кузнецов

Члени комісії:
д.т.н., професор І.Д. Горбенко

д.т.н., доцент С.Г. Рассомахін

Додаток В

Акт впровадження результатів дисертаційної роботи у навчальний процес Харківського національного університету імені В.Н. Каразіна

"ЗАТВЕРДЖУЮ"
Проректор з науково-педагогічної роботи
Харківського національного університету
імені В.Н. Каразіна
Академік НАН України
проф. _____ М.О. Азаренков
«10» 09 2020 р.

АКТ
впровадження результатів дисертаційної роботи
на здобуття ступеня доктора філософії
Ісірової Катерини Володимирівни
у навчальний процес Харківського національного університету імені В.Н. Каразіна

Комісія у складі голови комісії, доктора технічних наук, доцента Рассомахіна С.Г. та членів комісії, доктора технічних наук, професора Горбенко І.Д., кандидата технічних наук, Полуяненко М.О. встановила, що у Харківському національному університеті імені В.Н. Каразіна впроваджені наступні результати, що одержані Ісіровою Катериною Володимирівною в процесі виконання дисертаційних досліджень.

1. По дисципліні "Технології блокчейн" для спеціальності "Кібербезпека" при підготовці та читанні лекцій за темами 3-розділу «Питання безпеки децентралізованих систем», зокрема використані результати по побудуванню моделі децентралізованої інфраструктури відкритих ключів на основі технології блокчейн та побудуванню моделі децентралізованої системи електронного голосування.

Голова комісії, д.т.н., доцент С.Г. Рассомахін

Члени комісії:
д.т.н., професор І.Д. Горбенко

к.т.н. М.О. Полуяненко

Додаток Г

Акт впровадження результатів дисертаційної роботи у Приватному акціонерному товаристві «Інститут інформаційних технологій»

"ЗАТВЕРДЖУЮ"

Виконавчий директор

АТ «ІІТ»

_____ В.Д. Кравченко

"__" _____ 2020 р.

АКТ
впровадження результатів дисертаційної роботи
на здобуття ступеня доктора філософії
Ісірової Катерини Володимирівни
у Приватному акціонерному товаристві «Інститут інформаційних технологій»

Комісія у складі голови комісії, члена Наглядової ради, першого заступника головного конструктора АТ "ІІТ", кандидата технічних наук Горбенко Ю.І. та членів комісії, начальника відділу АЗЗІ АТ "ІІТ" Бобуха В.А., технічного директора АТ "ІІТ" Шумова О.І. встановила, що у Приватному акціонерному товаристві «Інститут інформаційних технологій» впроваджені наступні результати, що одержані Ісіровою Катериною Володимирівною в процесі виконання дисертаційних досліджень.

1. Удосконалений метод одноразових ключів Вінтерніц для постквантового періоду на основі геш-функцій, який дозволяє зменшити розміри особистого та відкритого ключів у 100 разів.

Голова комісії, член Наглядової ради,
перший заступник головного
конструктора АТ "ІІТ, к.т.н. Ю.І. Горбенко

Члени комісії:
начальник відділу АЗЗІ АТ "ІІТ" В.А. Бобух

технічний директор АТ "ІІТ" О.І. Шумов

Додаток Д

Лістинг програми для проведення симуляцій оцінки часових витрат на формування децентралізованої PKI

```
import networkx as nx
import random

def findParent(vertex):
    neighbours = list(G.adj[vertex])
    for i in range(0, len(neighbours)):
        if (neighbours[i] < vertex):
            return neighbours[i]
    return -1

def findChildren(vertex):
    neighbours = list(G.adj[vertex])
    children = []
    for i in range(0, len(neighbours)):
        if (neighbours[i] > vertex):
            children.append(neighbours[i])
    return children

def findDescendants(vertax):
    descendants = findChildren(vertax)
    for i in range(0, len(descendants)):
        children = findDescendants(descendants[i])
        descendants.extend(children)
    return descendants


def findIntruder(vertex):
    counter = 0
    if (G.node[vertex]['opinion'] == 0):
        return [vertex, 0]
    else:
        counter += 1
    parent = findParent(vertex)
    if (parent != -1):
        if G.node[parent]['opinion'] == 1:
            parent, counterIncrement = findIntruder(parent)
            counter += counterIncrement
    return [parent, counter]
```

```
def checkLegit(graph):
    for node in list(graph.nodes):
        if (graph.node[node]['opinion'] == 0):
            return False
    return True

G = nx.Graph()

numOfNodesOnLev = 1
startOfLevel = 0
currentIndex = 1

numOfChildrenOnLev = [1, 3, 2, 2]

for k in range(1, len(numOfChildrenOnLev)):
    for i in range(startOfLevel, startOfLevel + numOfNodesOnLev):
        for j in range(0, numOfChildrenOnLev[k]):
            G.add_edge(i, currentIndex)
            currentIndex += 1
    startOfLevel = startOfLevel + numOfNodesOnLev
    numOfNodesOnLev *= numOfChildrenOnLev[k]


for i in range(0, len(list(G.nodes))):
    G.add_node(i, opinion=random.randint(0, 1))

numberofNodes = len(list(G.nodes))
nodesQueue = list(G.nodes)

for i in range(0, numberofNodes):
    print(i, G.node[i])

print('список узлов', list(G.nodes))
print('количество узлов', numberofNodes)
print('список ребер', list(G.edges))


listOfIntruders = []
listOfLegit = []

for i in range(0, numberofNodes):
    if G.node[i]['opinion'] == 0:
```

```
        listOfIntruders.append(i)
    else:
        listOfLegit.append(i)

legitDesOfIntr = []

for nod in listOfLegit:
    parentIntr = findIntruder(nod)
    if parentIntr[0] != -1:
        legitDesOfIntr.append(nod)

numberOfAllExcludedNodes = len(listOfIntruders) + len(legitDesOfIntr)
numberOfRealIntruders = len(listOfIntruders)
numberOfLegitBlocked = len(legitDesOfIntr)

print('list of legit', listOfLegit)
print('list of intruders', listOfIntruders)
print('all excluded nodes', listOfIntruders, legitDesOfIntr)
print('number of all excluded nodes', numberOfAllExcludedNodes)
print('number of intruders', numberOfRealIntruders)
print('legit nodes which were excluded', legitDesOfIntr)
print('number of legit nodes which were excluded', numberOfLegitBlocked)


counterOfIteration = 0
counterOfRegeneration = 0

while(not checkLegit(G)):
    while(len(nodesQueue) != 0):
        print('nodes Queue', nodesQueue)
        currentNod = nodesQueue.pop()
        intruder = findIntruder(currentNod)
        print('current Node', currentNod, intruder)
        print('nodes Queue*', nodesQueue)
        counterOfIteration += intruder[1]
        if (intruder[0] != -1):
            if (intruder[1] > 0):
                G.node[intruder[0]]['opinion'] = 1
                print('intruder', intruder[0], G.node[intruder[0]])
                nodesQueue.remove(intruder[0])
                intruderDescendants = findDescendants(intruder[0])
                print('descendants of intruder', intruderDescendants)
```

```
            for child in intruderDescendants:
                if (child in nodesQueue):
                    print(child)
                    G.node[child]['opinion'] = random.randint(0, 1)
                    counterOfRegeneration += 1
                    print('nodes Queue', nodesQueue)
                    nodesQueue.remove(child)
                    print('nodes which stil in list', nodesQueue)
        else:
            print(intruder[0])
            G.node[intruder[0]]['opinion'] = random.randint(0, 1)
            counterOfRegeneration += 1
    nodesQueue = list(G.nodes)

rez = counterOfIteration + 2 * counterOfRegeneration

print('counterOfiteration', counterOfIteration)
print('counter of regeneration', counterOfRegeneration)
print('rez', rez)
print(checkLegit(G))
```