МЕТОДИ ТА МЕХАНІЗМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ БЛОКЧЕЙН

УДК 004.056.5 **DOI:10.30837/rt.2020.1.200.08**

І.Д. ГОРБЕНКО, д-р техн. наук, В.В. ОНОПРІЄНКО, канд. техн. наук,
Ю.І. ГОРБЕНКО, канд. техн. наук, О.О. КУЗНЕЦОВ, д-р техн. наук,
К.В. ІСІРОВА, М.Ю. РОДІНКО

ПРОБЛЕМИ, ПРИНЦИПИ ПОБУДОВИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ НАЦІОНАЛЬНОЇ СИСТЕМИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ В УКРАЇНІ

Вступ

Голосування у демократичних країнах є головним способом прийняття важливих рішень, що стосуються нації, держави, уряду, суспільних чи політичних подій, тощо. Волевиявлення проводиться при призначенні виборних осіб, президентів та парламенту, інколи суддів та шерифів, та є обов'язковою складовою представницької демократії. Зокрема, голосування реалізується і через основну форму прямого народовладдя – референдуми, народні збори, національні опитування, тощо.

Перебіг голосування, як і ступінь довіри до отриманих результатів волевиявлення, безпосередньо залежить від чесності організаторів та прозорості їх дій. Зокрема, в історії людства існує багато прикладів, коли свавілля та беззаконня можновладців спотворювало не тільки результати голосування, але і базові принципи демократії, роблячи народ безмовним покірним стадом, прикриваючись при цьому гаслами боротьби за «світле майбутнє» і добробут народу. Відомий вислів Наполеона III, що перефразовано Йосипом Сталіним: «Неважливо, як проголосують, а важливо те, як порахують», точно передає жахливу перспективу спотворення волевиявлення та узурпації влади. Саме тому забезпечення всіх умов для проведення прозорого та чесного голосування є головним завданням національного уряду, запорукою демократії, народної підтримки, гідності та єдності нації. Важливим кроком у цьому напрямку є впровадження електронних засобів та систем, які зменшують можливості адміністративного втручання та зловживання владою, правового тиску та маніпуляцій.

Під електронним голосуванням розуміється спосіб здійснення волевиявлення, при якому процес голосування, підрахунку та оприлюднення результатів здійснюється за допомогою електронних засобів та систем. Це найбільш широке тлумачення, яке включає різні технології: від електронної обробки фізичних носіїв з результатами волевиявлення (наприклад, паперових бюлетенів) до телеопитувань та сучасних технологій Інтернет-голосування. Кожну з відомих технологій можна характеризувати за як рівнем автоматизації певних процесів, так і за ступенем довіри та забезпечуваної безпеки як від зовнішнього втручання так і можливого зловживання організаторами та/або власниками інформаційних систем. Звісно, що практичне застосування на національному рівні можливе лише за умови вивчення та врахування історичного досвіду та відомих проблем, пошуку раціонального компромісу між наданням зручних у користуванні надійних автоматизованих послуг та певних припущень щодо можливих втрат або зловживань. І цей компроміс повинен влаштовувати переважну більшість як тих, хто голосує, так і тих, хто рахує, бо застосовувані технології повинні користуватися довірою і повагою, отримані результати однозначно сприйматися населенням і міжнародною спільнотою, а відомий вислів стосовно «правильного підрахунку» був повністю виключений навіть як гіпотетичний наслідок впровадження такої системи в Україні.

Останніми роками в світі з'явилося багато нових електронних технологій, які підвищують якість нашого життя, надають нові сервіси та послуги, зменшують ризики негативних подій та пом'якшують можливі наслідки. Одна із таких технологій – блокчейн – здійснила справжню революцію в цифровому світі, зробила блакитні мрії безнадійних романтиків реа-

льністю сьогодення. Насправді, вже зараз існують електроні гроші, непідконтрольні жодному центробанку, уряду чи монарху. Справжня децентралізація в електронному світі породжує нову, досі незнайому інфраструктуру, коли будь-хто і будь-де повністю анонімно та безпечно може створювати надійні активи, інвестувати та передавати власність, позичати та давати в борг, навіть невідомій особі. І все це функціонує повністю прозоро, без зайвої метушні можновладців та казнокрадів, без приводу до правоохоронців та податкового тиску. Це справжня демократія фінансового світу, грошове народовладдя, без контролюючих та підконтрольних, без посередників та узурпаторів, це фінансова воля.

Децентралізація в блокчейні реалізується через складні та пов'язані між собою криптографічні механізми, які гарантують, що події, які вже відбулися та задокументовані, не можуть бути змінені чи скомпрометовані. В таких системах неможливо заднім числом ввести додаткове мито чи змінити звітність, неможливо скасувати борг або обвалити курс національної валюти. Блокчейн-системи – це захищені сховища, в яких забезпечується історично стійке зберігання записів (реєстрів), і ці реєстри можуть містити будь-яку важливу інформацію. У криптовалютах таким чином зберігається інформація про наявні цифрові активи, у блокчейн-кадастрах – відомості щодо власників, в електронних аукціонах – історія торгів, тощо. І вся ця інформація не може бути змінена за примхою можновладця чи депутата, бандита чи олігарха, ця інформація історично захищена, незмінна, неспростовна і це надає можливість для якісно нового стану – незалежності та свободи. Свободи фінансів та власності, купляти та продавати, діяти та інвестувати, свободи вибору – і це найголовніше. Дійсно, історично стійке збереження кожного результату волевиявлення особистості забезпечує свободу та незалежність голосування спільноти. І ця технологія вже існує, і наше завдання – впровадити її в Україні.

Метою статті є аналіз можливих шляхів із розбудови національної децентралізованої системи електронного блокчейн-голосування в Україні, обґрунтування її структури та основних складових, надання конкретних пропозицій стосовно архітектури системи, базової моделі та протоколів взаємодії.

Історичний досвід та проблеми побудови національних систем електронного голосування

Забезпечення чесного та прозорого процесу волевиявлення громадян є одним із основних принципів демократичного суспільства та без перебільшення – питанням національної безпеки держави. Традиційний спосіб голосування з використанням друкованих бюлетенів, підрахунок яких здійснюється членами виборчих комісій, є вразливим до маніпуляцій та ресурсоємним, як з точки зору фінансових, так і часових витрат. На друк десятків мільйонів бюлетенів витрачаються величезні кошти, а підрахунок голосів, зазвичай, розтягується на декілька тижнів.

Перші спроби автоматизації процесу підрахунку голосів були зроблені у 60-х роках минулого століття у США. Виборець, як і раніше, власноруч робив відмітку на паперовому бюлетені, проте підрахунок голосів здійснювався вже не вручну, а за допомогою спеціальної машини, яка зчитувала відмітки з бюлетенів. Трохи пізніше з'явилися машини для голосування з електронними дисплеями та кнопками (або сенсорними дисплеями), що замінили паперові бюлетені. Результати голосування зберігалися у пам'яті такої машини. Подібні системи застосовувалися на виборчих дільницях у США, Індії, Бразилії.

Із розвитком комп'ютерних мереж та Інтернету почали розроблятися системи дистанційного голосування, що застосовуються у таких країнах як США, Великобританія, Швейцарія, Естонія. Так, наприклад, у Швейцарії віддалене голосування застосовується при проведенні місцевих референдумів, а пароль для доступу до електронного бюлетеня отримується виборцями через поштову службу.

Однією з найбільш прогресивних країн з точку зору впровадження систем дистанційного волевиявлення є Естонія, де на місцевих та парламентських виборах громадяни мають змогу віддати свої голоси онлайн через систему електронного голосування. Ідентифікація користу-

вачів здійснюється за допомогою ID карток, тому для голосування окрім комп'ютера необхідно мати пристрій для читання електронних карток. Голосування є таємним і здійснюється із застосуванням асиметричної криптографії. Однією зі сторін протоколу голосування є агентство електронного голосування, що розміщує списки виборців, підраховує голоси та публікує результати голосування.

За ступенем автоматизації системи електронного голосування можна поділити на такі, що:

- застосовують для підрахунку голосів електронні пристрої, що зчитують відмітки з паперових бюлетенів;
- застосовують машини для голосування з електронними дисплеями та кнопками (або сенсорними дисплеями) замість паперових бюлетенів; результати голосування зберігаються у пам'яті машини для голосування;
- реалізують дистанційне (віддалене) голосування через мережу Інтернет із використанням криптографічних протоколів.

Перший та другий типи систем електронного голосування хоч і підвищують ефективність процесу голосування, проте не відкидають необхідності приходу виборців на виборчі дільниці. У свою чергу, віддалене голосування дозволяє виборцю віддати свій голос, не виходячи з дому, що підвищує явку виборців.

Очевидно, що віддалене голосування є складнішим у реалізації, оскільки у цьому випадку необхідно забезпечити конфіденційність та цілісність даних, що передаються через мережу Інтернет. Це здійснюється за рахунок застосування асиметричної криптографії, зокрема алгоритмів цифрового підпису та направленого шифрування. Задля забезпечення повної анонімності використовуються алгоритми сліпого підпису та гомоморфне шифрування. Останнє, зокрема, не потребує розшифрування окремих голосів у процесі підрахунку.

За принципом побудови віддалені системи електронного голосування поділяються на централізовані та децентралізовані. Централізована система голосування має ієрархічну структуру, де вся інформація щодо голосування акумулюється у центральному довіреному вузлі, який здійснює підрахунок голосів та публікацію результатів голосування. Недоліками централізованого підходу є наступні:

- збій у роботі центрального вузла призведе до зупинки всієї системи голосування;
- збій у роботі центрального вузла може призвести до втрати всіх даних;
- виборці повинні довіряти центральному вузлу.

У децентралізованій системі немає єдиного довіреного центру, натомість всі вузли є рівноправними учасниками, що можуть працювати без довіри один до одного. Крім того, збій одного з вузлів не вплине на функціонування всієї системи, а інформація щодо голосування зберігається розподілено на різних вузлах. Однак, очевидно, що цей підхід є набагато складнішим у реалізації, ніж централізована система віддаленого електронного голосування.

Майже всі відомі системи електронного голосування в різних країнах є централізованими. Однак, з огляду на очевидні переваги, саме децентралізована система електронного голосування видається найбільш перспективним варіантом у контексті розробки національної системи голосування.

Проблема побудови такої системи може бути вирішена шляхом застосування технології блокчейн, яка в останні роки набула розвитку як у світі в цілому, так і в Україні зокрема. Багато компаній в Україні задіяно у проектах, пов'язаних з блокчейном, реалізований електронний аукціон на блокчейні тощо.

Блокчейн представляє собою ланцюжок з блоків даних (що містять транзакції), який одночасно зберігається різними вузлами мережі. Нові блоки даних можуть бути додані до ланцюжка лише за згодою більшості вузлів в результаті досягнення консенсусу, а блоки, щодо яких вузли вже дійшли згоди, не можуть бути модифіковані у майбутньому. Технологія блокчейн базується на використанні надійної криптографії та дозволяє забезпечити:

- розподілене зберігання інформації на різних вузлах;
- функціонування системи у разі збою одного або декількох вузлів;
- надійність та безпеку операцій в режимі повної недовіри між вузлами.

Побудова системи електронного голосування на основі блокчейну дозволить забезпечити виконання таких властивостей як:

- прозорість: достовірність транзакції, що містить голос виборця, може бути перевірена учасниками протоколу голосування у будь-який момент;
- цілісність: транзакція, що містить голос виборця, не може бути модифікована або вилучена з блокчейну після того, як блок, в якому міститься ця транзакція, було прийнято у результаті консенсусу;
- анонімність голосування, що не дозволяє зв'язати транзакцію, що містить голос виборця, з його особою (ідентифікаційними даними);
- автоматичний підрахунок голосів та публікація результатів голосування.

Впровадження технології блокчейн підвищує довіру до інформаційних ресурсів, надійність збереження інформації та якість наданих послуг. Відмітимо, що в Україні технологія блокчейн вже знайшла застосування при розробці електронних реєстрів.

На сьогодні голосування на блокчейні не набуло широкого впровадження державними інституціями, проте є приклади таких протоколів та їх застосування на приватному рівні.

З огляду на сказане та в контексті реалізації плану "Держава у смартфоні", вважаємо розробку системи електронного голосування, що базуватиметься на використанні технології блокчейн, найбільш перспективним варіантом розбудови національної системи електронного голосування.

Обгрунтування вимог та умов застосування національної системи електронного голосування в Україні

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). Можна виділити такі обов'язкові вимоги до систем електронного голосування [1]:

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

Додатково висуваються бажані вимоги [1]:

- кожен легітимний виборець може перевірити, чи правильно враховано його голос;
- кожен легітимний виборець може змінити свою думку і змінити свій вибір протягом певного періоду часу;
- система повинна бути захищена від продажу голосів виборцями;
- у разі неправильного підрахунку голосів кожен законний виборець може повідомити про це систему, не виявляючи його особистості;
- неможливість відстежити, звідки віддалено проголосував виборець;
- 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).

Коректна реалізація всіх зазначених вище вимог неможлива лише технічними засобами або лише нормативним регулюванням. Система електронного голосування не залежно від її архітектури повинна складатися із взаємопов'язаних частин.

Можна виділити такі складові частини (підсистеми/рівні) системи електронного голосування (рис. 1):

- нормативно-правовий рівень;
- організаційний рівень;
- рівень процесів;
- технологічний рівень.

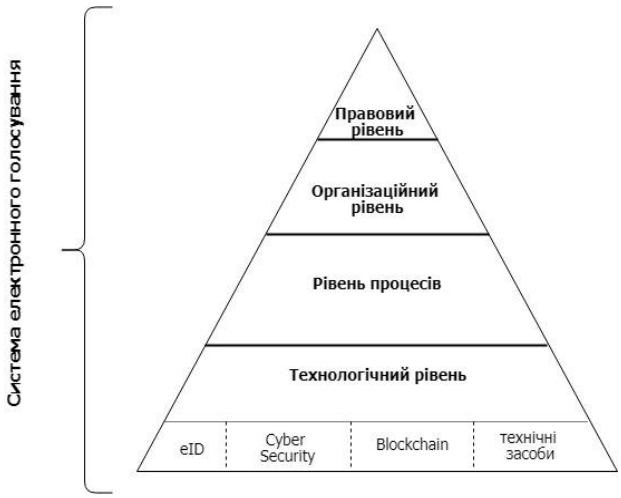

Рис. 1. Рівні системи електронного голосування

Нормативно-правовий рівень включає в себе українські та гармонізовані міжнародні стандарти щодо проведення процедури волевиявлення. Зокрема, на національному рівні мають бути враховані наступні вимоги виборчих процедур, передбачених Конституцією України, Законом України "Про вибори депутатів Верховної Ради Автономної Республіки Крим, місцевих рад та сільських, селищних, міських голів" [2], Законом України "Про вибори президента України" [3], а також прийнятими відповідно до них іншими актами законодавства.

Виборчий процес має здійснюватися на засадах [2, 3]:

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

Організаційний рівень включає в себе вимоги щодо архітектури системи електронного голосування.

Традиційна процедура голосування базується, по-перше, на надійній ідентифікації особистості виборця, по-друге – на вимозі збереження його анонімності. Тобто, відповідальні за підрахунок голосів точно впевнені, що голос надійшов від легітимного виборця, проте, вони не мають уявлення від кого саме. Для електронного голосування обидві ці вимоги мають бути збережені. Крім того можна виділити такі основні загрози для систем електронного голосування:

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

Рівень процесів описує порядок та процедури взаємодії всіх сторін. Можна виділити такі основні процеси:

- формування списку легітимних виборців;
- формування списку кандидатів;

- волевиявлення;
- підрахунку голосів.

Технологічний рівень включає низку методів, технологій, протоколів та конкретних засобів, направлених на технічну реалізацію процедури електронного волевиявлення.

Обґрунтування структури та основних складових національної системи електронного голосування в Україні

Проведений аналіз [6, 7 – 9] показав, що будь-яка класична (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 [10 – 17]. Особливо це стосується систем, які обробляють критичну інформацію, таку як персональні дані виборців. Традиційним "слабким місцем" будь-якої централізованої структури є її вершина (тобто центральний орган управління), вихід із ладу його внаслідок спрямованої атаки або незапланованого збою фактично означає зупинку функціонування всієї системи. Виходом вбачається перехід на децентралізовані системи.

На рис. 2 схематично зображено структуру традиційної, ієрархічної централізованої структури (ліворуч), та децентралізованої (праворуч). У табл. 1 наведено коротку порівняльну характеристику таких систем з приводу наявних переваг та недоліків.

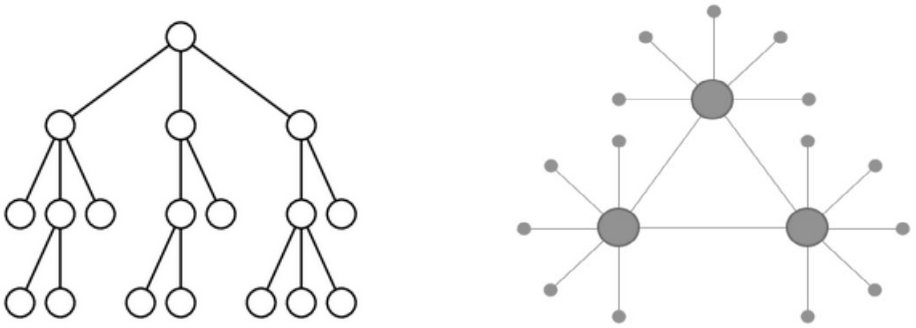

Рис. 2. Централізована ієрархічна (ліворуч) та децентралізована (праворуч) структури

Таблиця 1

Наявні переваги та недоліки централізованих ієрархічних систем

Централізована ієрархічна структура	**Децентралізована структура**
Єдина точка збою • Якщо центр несправний або скомпрометований, то вся система компрометується	Стійкість до збоїв • Центр відсутній, компрометація окремих складових не критична
Користувачі повинні довіряти центру • Необхідність застосування третьої довіреної сторони	Режим повної недовіри • Сторони можуть працювати без довіри один до одного • Довірена сторона не потрібна
Єдиний центр зберігання інформації • Втрата даних у разі збою або порушення центрального серверу	Розподілене зберігання • Однакові дані одночасно зберігаються на різних вузлах • Втрата фактично виключена

Особливо важливим питанням при цьому є формулювання політики та вимог, по яким функціонує децентралізована система. Необхідно забезпечити всім користувачам єдине бачення стану системи в кожний конкретний момент часу. Це можливо із використанням технології blockchain.

В децентралізованому підході забезпечення надійної електронної ідентифікації за допомогою класичного електронного підпису, проте без використання додаткових маскуючих механізмів (наприклад, сліпих підписів), неможливо досягти анонімності виборців. Для того щоб зберегти анонімність та в той же час не перевантажувати протоколи взаємодії, пропонується організувати дворівневу архітектуру системи електронного голосування (рис. 3).

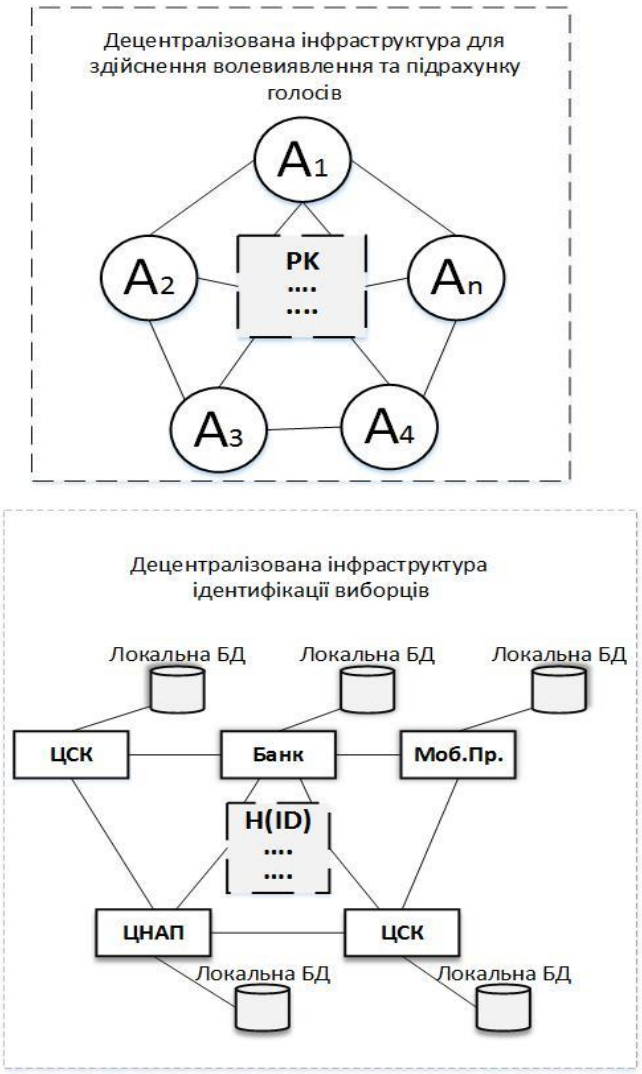

Рис. 3. Рівні системи електронного голосування

Децентралізована інфраструктура ідентифікації виборців (ДІ eID)

Дана інфраструктура 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:

- засобів BankID;
- засобів MobileID;
- електронного паспорта громадянина;
- цифрового (електронного) підпису:
- програмний носій цифрового підпису;
- апаратний носій цифрового підпису.

Відповідно до висунутих вимог, в ролі *IdP* можуть виступати:

- банківські установи;
- мобільні оператори;

- центри міграційної служби (центри надання адміністративних послуг – ЦНАП);
- центри сертифікації ключів національної системи ЕЦП.

Регламенти функціонування провайдерів встановлюються Законом України "Про електронні довірчі послуги" [4], імплементованим Регламентом ЄС [5] та іншими міжнародними та національними нормативними документами.

Вимоги та процедури ідентифікації залежать від конкретного провайдера.

Мережа провайдерів ідентифікації сформована 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 використання локальних баз даних покладається на IdP.

Для організації інфраструктури ідентифікації в рамках децентралізованої системи електронного голосування, IdP об'єднуються в окрему приватну мережу блокчейн (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.

Децентралізована інфраструктура для здійснення дистанційного волевиявлення та підрахунку голосів

Інфраструктура має забезпечувати процес дистанційного волевиявлення зареєстрованих (авторизованих) легітимних виборців та процес підрахунку голосів. Додатково в даній інфраструктурі повинні бути організовані процеси реєстрації кандидатів. Довіреними вузлами в даному випадку будуть виступати аналоги територіальних виборчих громад, проте завдяки децентралізованому підходу та технології blockchain наявність головного органу (центральної виборчої комісії) не потрібне. Така організація значно зменшує ризики, пов'язані із людським фактором, включаючи можливості підкупу членів центральної виборчої комісії.

Для організації інфраструктури дистанційного волевиявлення в рамках децентралізованої системи електронного голосування представництва відповідальних за проведення виборчого процесу, наприклад територіальні виборчі громади (A1, A2,...,An), подібно до провайдерів ідентифікації, об'єднуються в окрему приватну мережу блокчейн (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).

Процес 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.

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 (рис. 4) 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.

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 (рис. 5).

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 (рис. 6). Процедура первинної ідентифікації має проводитися відповідно до правил конкретного IdP.

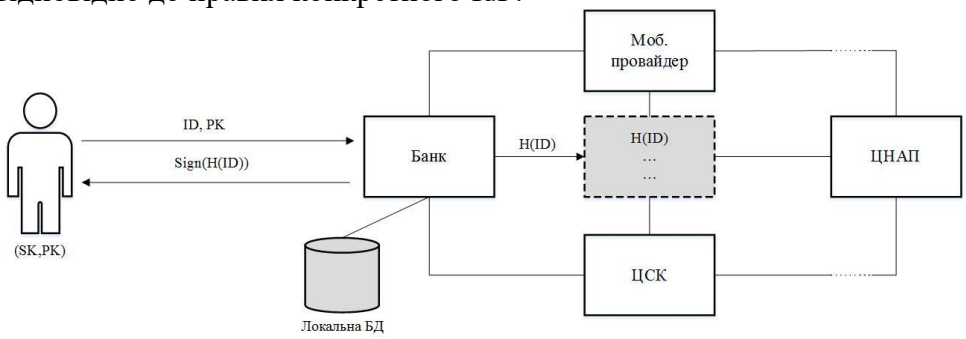

Рис. 4. Процедура ідентифікації на основі відкритого ключа (локального ідентифікатора)

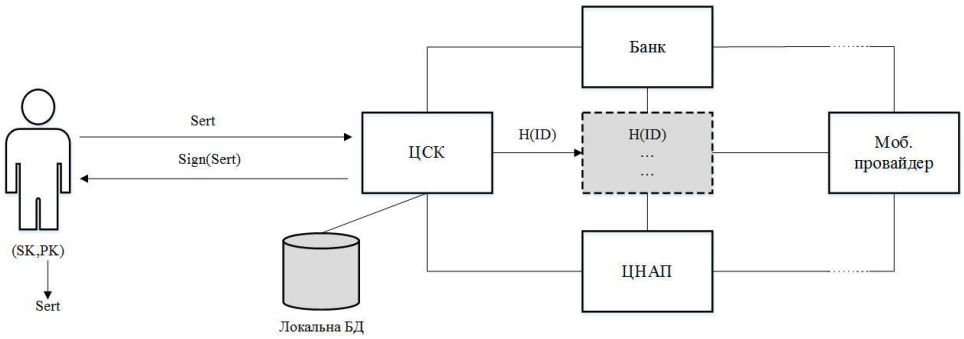

Рис. 5. Процедура ідентифікації на основі сертифікату

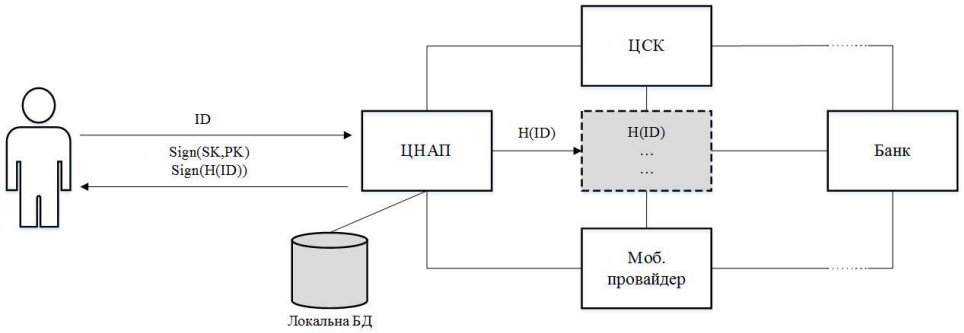

Рис. 6. Процедура ідентифікації на основі персональних даних

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.

Процес формування списку 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.

Відповідальність за процедуру реєстрації (рис. 7) кандидатів покладено на валідаторів верхньої мережі Blockchain.

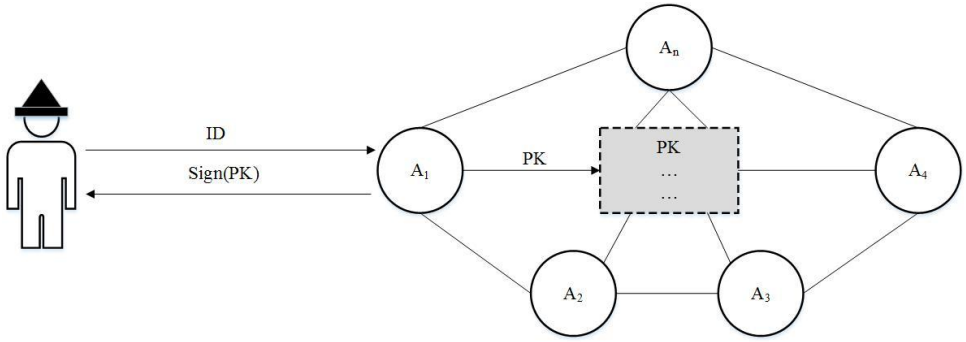

Рис. 7. Процедура реєстрації кандидатів

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 до списку. При цьому представництва Агентства несуть відповідальність за дотримання всіх правил та політик ідентифікації кандидатів та перевірку на відповідність вимогам, які встановлені національним законодавством.

Процес 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.

Необхідно зазначити, що запропонований підхід може бути використаний навіть у перехідний період, коли частина виборців вже буде використовувати електронні засоби, а частина все ще буде віддавати перевагу класичним паперовим бюлетеням. Хоча при цьому виборцю, який бажає проголосувати за допомогою паперового бюлетеню, необхідно буде пройти процедуру ідентифікації у нижній мережі blockchain (нагадуємо, що це можливо зробити, навіть не маючи жодних технічних засобів), безпосередньо процес волевиявлення може бути здійснений класичним способом на виборчій дільниці (в даному випадку в межах контрольованої зони одного із представництв децентралізованого Агентства). Для цього передбачається процедура анулювання токена для голосування такого виборця перед наданням йому паперового бюлетеня.

Процес підрахунку голосів у децентралізованій інфраструктурі для здійснення дистанційного волевиявлення та підрахунку голосів

Підрахунок голосів здійснюється автоматично. Результати стають доступними для всіх після завершення часу, відведеного для голосування. Концепція та архітектура системи також передбачає можливість організації моніторингу явки виборців, а також з невеликими додатковими модернізаціями можливість проведення аналізу результатів волевиявлення, наприклад розподіл суспільної думки по регіонах без втрати анонімності виборців.

Висновки та рекомендації

Дослідження довели, що класичні (централізовані ієрархічні) системи голосування не завжди відповідають сучасним вимогам інформаційного демократичного суспільства. Особливо це стосується державних систем із перехідною моделлю управління, коли демократичні цінності не мають сталого історичного підґрунтя або обтяжені авторитарними періодами із свавіллям та беззаконням можновладців. Зокрема, більшість пострадянських держав перебувають під наслідком тривалого тоталітарного правління, коли безальтернативне голосування та «правильний» підрахунок голосів були звичайною практикою ієрархічних суспільних від-

носин. І навіть сьогодні нерідкі прецеденти застосування адміністративного ресурсу, які, хоча і скасовуються інколи через революційні події, але можуть повністю спаплюжити народовладдя через підробку або викривлення результатів волевиявлення. Ієрархічні централізовані системи голосування зазвичай використовуються як вдалий механізм приховування можновладцями своїх корисних намірів, коли різними шляхами за стіною потужних адміністративних парканів та силами державних установ реалізується узурпація влади – від друку додаткових бюлетенів, примусового голосування ув'язнених і т.д. до втручання в електронні системи центральної виборчої комісії. Звісно, що всі переваги централізованих систем (керованість, надійність, автономність і т.д.) нівелюються через можливість викривлення результатів голосування, тобто у разі, коли система не спроможна виконати завдання за призначенням. Отже дослідження, розробка та впровадження нових інформаційних систем і технологій електронного голосування, які б унеможливлювали втручання та викривлення волевиявлення через децентралізацію (звісно із збереженням всіх системних якостей з безпеки та надійності), є безумовно важливим та актуальним науково-прикладним завданням загальнонаціонального значення.

Аналіз показав, що на сьогодні вже створено основне науково-технологічне підґрунтя для розбудови інформаційних систем якісно нового рівня. Це децентралізовані електронні системи, які побудовані за технологією блокчейн та які здатні краще забезпечити функціонування в умовах збільшення спектру інформаційних послуг та при зростанні кількості користувачів. Децентралізоване збереження даних та, що найголовніше, децентралізоване, неупереджене та незалежне прийняття рішення в блокчейн-системах є запорукою розбудови якісно нової загальнонаціональної системи електронного голосування, здатної докорінно змінити соціальні відносини від ієрархічного «начальник-підлеглий» до децентралізованого «партнер-партнер». Впровадження такої системи має за мету унеможливити втручання в виборчий процес, зробити його прозорим та безпечним, підвищуючи тим самим довіру до національної влади, державних інформаційних ресурсів, зменшити час та накладні витрати, підвищити безпеку, тощо. Отже, враховуючи основні засади національного інформаційного суверенітету та з погляду на розбудову демократичного інформаційного суспільства в Україні доцільним є впровадження децентралізованих систем та мереж, які спроможні надавати якісно нові послуги та сервіси, в тому числі, забезпечуючи незалежність, неспростовність, прозорість та безпеку інформаційних ресурсів на всіх етапах їх життєвого циклу.

Сучасна система електронного голосування являє собою взаємопов'язану сукупність правил, методів, процесів, засобів і технологій, а також правових норм, що забезпечують і регулюють дистанційне легітимне волевиявлення авторизованих користувачів (виборців). Електроне голосування охоплює процеси на чотирьох базових рівнях: нормативному, організаційному, рівні процесів та технологічному рівні. Кожен з рівнів забезпечує виконання певних процесів, які забезпечуються окремими технічними, технологічними та нормативно-правовими механізмами. Зокрема, нормативно-правовий рівень забезпечує виконання як гармонізованих міжнародних, так і національних українських стандартів та інших нормативно-правових актів щодо проведення процедури волевиявлення із врахуванням засад законності та заборони незаконного втручання у виборчий процес, політичного плюралізму, публічності і відкритості, рівності суб'єктів виборчого процесу перед законом та прав усіх кандидатів, свободи агітації, рівних можливостей доступу до засобів інформації, неупередженості органів державної влади, місцевого самоврядування, посадових і службових осіб, керівників підприємств, установ і організацій, тощо. Організаційний рівень забезпечує виконання вимог архітектури системи електронного голосування, надійної ідентифікації особистості виборця, вимог збереження анонімності підрахунку голосів, відповідальності організаторів, тощо. Рівень процесів забезпечує встановлений порядок та процедури взаємодії всіх сторін, зокрема, процесів формування списку легітимних виборців та списків кандидатів (альтернатив голосування), процесів волевиявлення та підрахунку голосів, тощо. Технологічний рівень за-

безпечує виконання методів, технологій, протоколів та конкретних засобів технічної та технологічної реалізації процедури електронного волевиявлення.

Для практичної розбудови національної системи електронного голосування в Україні із врахуванням міжнародного досвіду з розгортання, експлуатації та результатів аналізу безпеки інформаційних технологій запропоновано конкретні пропозиції з обґрунтування архітектури, базової моделі та протоколів взаємодії системи електронного блокчейн-голосування. Запропонована, досліджена та випробувана шляхом фізичного прототипування дворівнева архітектура системи електронного блокчейн-голосування. Нижній (перший) рівень цієї системи дозволяє, враховуючи досвід розбудови національних інформаційних комплексів та систем, забезпечити виконання всіх складових процесу електронної ідентифікації за допомогою вже існуючих технічних засобів та організаційно-правових заходів, таких, наприклад, як BankID, MobileID, електронний підпис, тощо. Це забезпечить інтероперабельність системи електронного голосування, успадковуваність вже впроваджених національних інформаційних систем і технологій (зокрема, національної системи електронних довірчих послуг) та відтворюваність результатів фізичного прототипування блокчейн-голосування. Верхній (другий) рівень призначено для реалізації волевиявлення та підрахунку голосів із забезпеченням керівних принципів демократичного волевиявлення (схвалених Венеціанською комісією), зокрема, незалежного контролю за правильністю складання списків виборців; можливості анонімного голосування тільки тими особами, які мають на це право; незмінність та неспростовність результатів волевиявлення; легкість та прозорість перевірки правильності підрахунку голосів, тощо. Отримані результати фізичного прототипування дозволяють стверджувати про ґрунтовність та виваженість розробленої архітектури, її спроможність забезпечити виконання базових вимог децентралізованого електронного голосування, вимог інформаційної та функціональної безпеки та надійності інформаційних технологій. Практичне впровадження розробленої архітектури блокчейн-голосування підвищить довіру до інформаційних ресурсів та сервісів (що є особливо актуальним для державних установ); зменшить час та накладні витрати; унеможливить втручання централізованих установ та можливі корупційні дії; підвищить надійність збереження інформації та якість наданих послуг.

Список літератури:

1. Hannu Nurmi, Arto Salomaa. Conducting secret ballot elections in computer networks: Problems and solutions // Annals of Operations Research / University of Turku. 1994. №51. P.185-194.
2. Закон України “Про вибори депутатів Верховної Ради Автономної Республіки Крим, місцевих рад та сільських, селищних, міських голів”.
3. Закон України “Про вибори президента України”.
4. Закон України “Про електронні довірчі послуги”.
5. Регламент (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року «Про електронну ідентифікацію та довірчі послуги для електронних транзакцій у межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС» (1) (COM (2012) 0238-C7-0133/2012 – 2012/0146 (COD)).
6. Горбенко І.Д., Кузнецов О.О., Потій О.В., Горбенко Ю.І., Полуяненко М.О. Технологія блокчейн: огляд, сучасні проблеми та перспективи впровадження в Україні // ІІ міжнар. наук.-практ. конф. “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS), 11-12 квітня 2019 р., м. Київ, 2019. С. 217-220.
7. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography, CRC Press, 1997, 794 p.
8. Yu. I. Gorbenko, K. V. Isirova. Improved mechanism of one-time keys for post-quantum period based on the hashing functions // Telecommunications and Radio Engineering. 2018. Vol. 77, Issue 14. P. 1277-1296.
9. Andrushkevych A., Gorbenko Y., Kuznetsov O., Oliynykov R., Rodinko M. A. A Prospective Lightweight Block Cipher for Green IT Engineering // Kharchenko V., Kondratenko Y., Kacprzyk J. (eds) Green IT Engineering: Social, Business and Industrial Applications. Studies in Systems. Decision and Control. 2019. Vol. 171. Springer, Cham, pp. 95-112. DOI: 10.1007/978-3-030-00253-4_5
10. Потій О. В., Ісірова К. В. Аналіз вимог та моделей безпеки для постквантової криптографії // Математичне та комп’ютерне моделювання. Серія: Технічні науки : зб. наук. праць / Інститут імені В. М. Глушкова Національної академії наук України, Кам’янець-Подільський нац. ун-т імені Івана Огієнка. Кам’янець-Подільський : Кам’янець-Подільський нац. ун-т ім. Івана Огієнка, 2017. Вип. 15- с. 192-197

11. Kateryna Isirova. Blockchain Technology as the Prospective Instrument for Ensuring Electronic Trust Services in Conditions of Cyberthreats // European Cybersecurity Journal. 2018. Issue 5 (1). P 34-43

12. Gorbenko I., Kuznetsov A., Gorbenko Y., Vdovenko S., Tymchenko V., Lutsenko M. (). Studies on Statistical Analysis and Performance Evaluation For Some Stream Ciphers // International Journal of Computing. 2019. 18(1). P. 82-88.

13. Bernstein D., Buchmann J., Dahmen E. Post-Quantum Cryptography. Springer-Verlag, Berlin-Heidleberg, 2009. 245 p.

14. Pass R., Seeman L., Shelat A. Analysis of the blockchain protocol in asynchronous networks // Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2017. P. 643-673.

15. Isirova K., Potii O. Decentralized public key infrastructure development princi-ples // IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). Kiev, 2018. P. 305-310.

16. Kovalchuk L., Kaidalov D., Nastenko A., Rodinko, Shevtsov O., Oliynykov R. Decreasing Security Threshold Against Double Spend Attack in Networks with Slow Synchronization // IEEE INFOCOM 2019, Paris, France, 2019. P. 216-221. doi: 10.1109/INFCOMW.2019.8845301

17. Nurmi H., Salomaa A. Conducting secret ballot elections in computer networks : Problems and solutions // Annals of Operations Research, 1994. Vol. 51, no. 4. P. 185–194.

Харківський національний
університет імені В. Н. Каразіна;
АТ «Інститут інформаційних технологій»

Надійшла до редколегії 15.01.2020