УДК 004.056.523:342.8:091.5(045)

DOI: 10.18372/2073-4751.77.18656

Зудов О.М., к.т.н.,
orcid.org/0000-0003-3313-1659,
e-mail: oleh.zudov@npp.nau.edu.ua,
Горіна В.В.,
orcid.org/0000-0002-0052-0466,
e-mail: violetta.horina@npp.nau.edu.ua,
Рибасова Н.О.,
orcid.org/0000-0002-0778-072X,
e-mail: natalka.rybasova@npp.nau.edu.ua

ПРОТОКОЛИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ НА ОСНОВІ КРИПТОГРАФІЧНОЇ СХЕМИ "СЛІПОГО ПІДПИСУ" І БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

Національний авіаційний університет

Вступ

Електронне голосування (*E-voting*) стає ключовим елементом демократії. Нещодавня пандемія кинула новий виклик в цій області, хоча інтерес до проблеми існує давно. Основи принципів електронного голосування було закладено ще наприкінці двадцятого століття, разом із розвитком сучасних основ криптографії. Відомі науковці, що заклали основи сучасних криптографічних систем, такі як Аді Шаимір, Девід Чаум, Брюс Шнайєр та інші приділяли увагу і цьому важливому застосунку криптографії [1].

Першою країною, що провела електронні вибори на національному рівні, була Естонія, яка провела у 2005 році вибори у місцеві органи влади, використовуючи в тому числі голосування в Інтернет, а також парламентські вибори 2011 року. З того часу інтерес до технології електронного голосування зростає.

Водночас виникають питання стосовно безпеки, анонімності та довіри. Критики систем електронного голосування справедливо вказують на суперечливість вимог відкритості і анонімності. Збільшуючи один параметр, ми послабляємо інший. У даній статті розглядається можливості і варіанти застосування протоколу електронного голосування на основі "сліпого підпису" як одного з можливих шляхів у розв'язанні цих проблем.

Аналіз сучасного стану технологій електронного голосування

1. Актуальність.

Пандемія *COVID*-19 визначила нові виклики для суспільства і технологій, виборчий процес не є винятком. Актуальність електронного голосування виросла, зокрема через потребу в безконтактних методах голосування та підвищення ефективності виборчих процесів. І якщо електронна комерція, банкінг та інші подібні технології швидко стали популярними, а надійність їх викликає довіру споживачів, саме завдяки криптографічним методам захисту інформації, то електронне голосування все ще знаходиться на стадії дослідження, розробок, удосконалень і модифікацій алгоритмів і протоколів, а рівень довіри серед громадськості, політиків і фахівців суспільних наук не дуже високий. Причиною є суперечливість вимог до процесу голосування, який повинен одночасно бути прозорим і анонімним. Електронне голосування повинно забезпечувати надійну аутентифікацію виборців і при цьому анонімність їх голосів, прозорість процесу та відсутність можливості зловживань. Ці вимоги часто конфліктують між собою, і часто автори нових протоколів голосування вирішують завдання щодо пошуку компромісу.

Ще однією проблемою є те, що електронні вибори вимагають кваліфікованих спостерігачів, часто IT-фахівців, для

ефективного контролю за процесом голосування, в той же час для спостереження і контролю "класичних" виборів від організації і осіб не потрібно вимагати розуміння сучасних основ криптографії та інформаційних технологій.

Таким чином, розробка нових підходів до організації електронних виборів є актуальною і важливою темою досліджень.

2. Основні вимоги до протоколів електронного голосування.

Існують різні системи електронного голосування, які використовують криптографічні протоколи [3-8]. Проте, не всі з них можуть ефективно вирішувати поставлені вимоги. Наприклад, протоколи на основі розділення секрету, *ANDOS*, та розділення довірчих агенцій вже застосовуються, але мають свої недоліки.

Недоліки існуючих систем електронного голосування можна умовно розділити на дві категорії.

Концептуальні недоліки.

Існуючі системи не завжди забезпечують повну анонімність, оскільки існує можливість встановлення зв'язку між виборцем і його голосом (проблема приватності). Додатково, не завжди існує повна довіра до виконавців, агенцій чи виборчих комісій (проблема довіри).

Такі проблеми з одного боку можуть налякати виборця щодо можливості порушення тайни голосування, а з іншого боку залишають відкритими питання маніпуляції результатами виборів недоброчесними організаторами. Також "ідеальний" протокол електронного голосування повинен зменшувати (або повністю усувати) можливість змови деяких учасників виборчого процесу і купівлю/продаж голосів.

Технічні недоліки.

Технічні недоліки включають:

- складність реалізації;
- вразливість до різноманітних атак на безпеку.

Багато авторів і дослідників висувають різні, часто суперечливі вимоги до електронних виборів. Перерахуємо найбільш важливі.

1. ***Зручність***: система повинна дозволяти виборцям проголосувати швидко, за один сеанс; не повинна вимагати спеціальних навичок; не повинна залякувати виборців; повинна забезпечувати рівний доступ виборців.
2. ***Стійкість до атак***: необхідно враховувати можливість атаки серверів з боку зловмисників (наприклад, *Dos*/*DDoS* атаки) і не допускати вразливостей криптографічних протоколів.
3. ***Прозорість і можливість перевірки***: виборці повинні мати загальні знання та розуміння процесу голосування має бути можливість перевірити, чи всі голоси були правильно враховані під час остаточного підрахунку виборів.
4. ***Автентичність виборця***: виборець повинен ідентифікувати себе (щодо бази даних реєстрації), щоб мати право голосу.
5. ***Анонімність виборця***: голоси не пов'язуються з ідентифікацією виборця.
6. ***Унікальність***: жоден виборець не повинен мати можливість голосувати більше одного разу.
7. ***Відсутність можливості примусу та продаж голосів***: як варіант виконання цієї умови зазвичай пропонується схема, де виборці не повинні мати можливість довести іншим, як вони проголосували.

Дана стаття зосереджує увагу саме на цій останній умові 7, оскільки деякі дослідники вважають цю вимогу опціональною і не приділяють питанню протидії торгівлі голосами достатньо уваги.

3. Існуючі системи на основі криптографічних протоколів

Нижче наведено короткий огляд деяких існуючих протоколів, які є найбільш популярними і перспективними на сьогоднішній день.

ZKP (*zero-knowlage* протокол, або "протокол продажу секретів"). За допомогою цієї схеми у варіанті її застосування для електронного голосування виборча комісія розподіляє ключі шифрування серед виборців, при цьому ані організатори, ані інші виборці не знають, якій ключ хто

отримав [1]. Недолік даної системи в її вразливості до змови агенції (виборчої комісії) з деякими виборцями.

ANDOS – протокол, у якому замість традиційного асиметричного шифрування використовує криптографічну хеш-функцію, яку застосовують для бюлетеня виборця [2]. Хоча анонімність виборця забезпечується в цьому випадку надійністю картографічних схем, даний протокол не захищає від недоброчесної виборчої комісії, залишаючи способи шахрайства з неіснуючими голосами.

Helios Voting Protocol. Цей протокол використовує криптографію на основі гоморфних шифрів для забезпечення анонімності та можливості перевірки голосів [3]. Відкритість коду сприяє прозорості та перевірці. Недоліком даної схеми є насамперед те, що її реалізація вимагає великих обчислювальних ресурсів для шифрування та декриптування, що може ускладнити широкомасштабне впровадження.

Проєкти *Belenios* та *ThreeBallot* використовують *End-to-End Verifiable Systems* [4]. Схема забезпечує можливість виборців перевіряти, чи був врахований їх голос. Такі системи пропонують високий рівень прозорості. На жаль, може виникнути проблема конфіденційності, оскільки виборці можуть бути в складній ситуації зберігати свій голос, не розголошуючи його. *ThreeBallot* використовує систему з трьома етапами голосування, що дозволяє виборцям вибирати між декількома варіантами анонімності та перевірки голосів, але це може бути складним для виборців зрозуміти та використовувати, що може призвести до помилок.

Модифікації протоколів електронного голосування

Для захисту цілісності даних електронних виборів, а також для унеможливлення зловживанням недоброчесними агентами були запропоновані реалізації протоколів на основі *блокчейн* технології [8]. Вона забезпечить впевненість в тому, що дані, збережені в системі, не бути змінені, а також розподіляє функції учасників, зменшуючи можливості для зловживань. Але до того, як дані потраплять до блокчейну, існує досить просторе поле для зловмисників, де вони могли б вплинути на результат голосування.

Надійнішим варіантом буде техніка поділу приватного ключа шифрування після генерації добре відома *схема поділу секрету Шаміра* [1]. Ключова пара створюється, публічний ключ зберігається у блокчейні як відкритий ключ голосування, а приватний ключ поділяється кілька частин, які незалежно зберігаються довіреними учасниками. Щоб підбити підсумки голосування, приватний ключ необхідно зібрати і після цього розшифрувати бюлетені. Якщо хтось із довірених учасників “захворів”, схема Шаміра передбачає можливість збирання приватного ключа меншою кількістю учасників. Тобто якщо ключ був розбитий на n частин, зібрати його можна, використовуючи k частин, де $k < n$. Такий варіант виглядає набагато надійнішим і більш продвинутим. Але все одно він не позбавлений вразливостей. По-перше, у проміжок часу між генерацією ключа та його поділом він є очевидною мішенню для зловмисників. По-друге, після збирання ключа є можливість розшифрувати кожен індивідуальний бюлетень. Це не дозволить їх відфільтрувати, тому що вони вже перебувають у блокчейні та нікуди звідти не подінуться. Але це дозволить порушити конфіденційність голосування. На сервері є зв'язка ідентифікатора користувача та публічного ключа учасника голосування, а в блокчейні – зв'язка публічного ключа і тепер уже розшифрованого бюлетеня.

Можна запропонувати механізми розриву першої зв'язки – персональних даних та відкритого ключа через техніку так званого “*сліпого підпису*”. Схема підпису наосліп була запропонована і запатентована Девідом Чаумом ще у 1988 році [5], і багатьма авторами розглядається як основний компонент процедури електронного голосування. Наприклад, він використовується у системі *Scantegrity II* [6].

Зазвичай, авторами пропонується використання технології сліпого підпису для

підписування виборчих бюлетенів. Такий підхід застосовується у найбільш відомих схемах електронного голосування, а саме у *схемі Фудзіок-Окамото-Оти* [9] і *протоколі SENSUS* [10].

Але даний підхід не вирішує проблеми конфіденційності, яка висвітлена вище. Якщо ж замість "осліплення" бюлетеня підписувати наосліп відкритий ключ потенційного виборця, таємність його голосу зберігається. Даний підхід вперше було запропоновано Ци Хе і Чжунмінь Су, технологія зараз відома під назвою *протокол He-Su* [7]

Отже, основна ідея полягає в тому, що виборець підписує свій відкритий ключ, а не голос. Для шифрування голосу використовується криптографічна схема *RSA*. Цей підхід гарантує, що навіть недобросовісна виборча комісія не може співставити конкретного виборця з його вибором, навіть після розшифрування та оприлюднення результатів. Крім того, оскільки публікуються у відкритий доступ списки виборців і їх авторизовані ключі, достатньо проблематично для зловмисників використовувати неіснуючі голоси, а публікація можливість перевірки результатів голосування унеможливлює зарахувати голоси виборців, які зареєструвалися, але не проголосували. В оригінальному варіанті, запропонованому авторами, функції виборчої комісії розділені, тобто у процедурі беруть участь три сторони: виборці, реєстратор (валідатор) і адміністратор (рахувальна комісія). Але оскільки сама процедура виключає можливість змови двох останніх, їхні функції може виконувати один організатор – виборча агенція.

В такому варіанті процедура голосування має наступний вигляд.

- Виборці ідентифікуються будь-яким способом (*ID* картки, документи, ЕЦП, біометрична ідентифікація) і реєструються як учасники голосування. Для цього вони генерують пару закритий/відкритий ключ згідно зі схемою *RSA*. Відкритий ключ маскується (осліплюється) і відправляється організатору (агенції, виборчій комісії) для підпису наосліп.
- Організатор підписує наосліп відкриті ключі виборців, не знаючи самих ключів. Це в подальшому забезпечує анонімність голосів. Кожний зареєстрований виборець може підписати наосліп тільки один ключ, тому це унеможливлює повторне голосування.
- Списки виборців публікуються у відкритий доступ.
- Виборець віддає свій голос, діючи анонімно. Голос шифрується за схемою *RSA* і подається разом з відкритим ключем. Фактично, відкритий ключ є псевдонімом виборця.
- Після закінчення голосування голоси виборців дешифруються, підраховуються і публікуються.

Опишемо цей алгоритм більш детально. Нижче будуть використовуватися традиційні позначення: E і D – відповідно відкритий (*Encrypting*) і закритий (*Decrypting*) ключі у схемі асиметричного шифрування, K – ключ (*key*) у схемі симетричного шифрування; індекси: v – виборець (*voter*); a – агенція або адміністратор (суміщує функції організатора, автентифікатора і лічильної комісії).

Етап 1 (реєстрація).

Адміністратор:

- публікує свій відкритий ключ E_a;
- перевіряє автентичність виборця.

Виборець:

- генерує пару ключів – D_v (приватний) та E_v (відкритий);
- генерує випадкове число R (що маскує множник);
- обчислює $E_a(R)\cdot h(E_v)$, де E_a – відкритий ключ адміністратора, h – криптографічна хеш-функція;
- надсилає результат адміністратору.

Адміністратор:

- Підписує прийняте повідомлення $D_a(E_a(R)\cdot h(E_v))$, де D_a особистий ключ адміністратора; оскільки криптосистема *RSA* є *гомоморфною щодо множення*, то результатом буде:

$$Da\big(Ea(R)\cdot h(Ev)\big) = R\cdot Da\big(h(Ev)\big) \quad (1)$$

- надсилає результат виборцю; таким чином, виборець має підписаний хеш свого приватного ключа, замаскований осліплюючим множником *R*;
- публікує список авторизованих виборців.

Виборець:

- прибирає маскуючий множник *R* з отриманого повідомлення;
- розшифровує підпис адміністратора і перевіряє рівність:

$$Ea\left(Da\big(h(Ev)\big)\right) = h(Ev) \qquad (2)$$

Якщо рівність виконується, виборець переконується у тому, що має підписаний адміністратором ключ;

- анонімно відправляє адміністратору E_v та $D_a(h(Ev))$.

Адміністратор:

- перевіряє рівність:

$$Ea\left(Da\big(h(Ev\,)\big)\right) = h(Ev\,) \qquad (3)$$

- за умови правильної рівності авторизує ключ E_v;
- публікує список авторизованих ключів (псевдонимів виборців).

Зауважимо, що на цьому етапі недоброчесний адміністратор може опубліковувати неіснуючі ключі – так звана проблема "мертвих душ". Кожен виборець може перевірити наявність свого ключа в опублікованому списку, але не може переконатися, що увесь список коректний. Звісно, список ключів не повинен бути більше списку зареєстрованих виборців. Але можуть бути виборці, що зареєструвалися, а потім продали своє право голосу, і далі від їхнього імені діють інші особи.

Етап 2 (голосування).

Виборець:

- відправляє трійку E_v, $K_v(B_v)$, $D_v(h(K_v(B_v)))$, де K_v – секретний ключ виборця (для симетричного шифрування), B_v – бюлетень;

Адміністратор:

- перевіряє, чи є ключ $E\ v$ авторизованим;
- перевіряє рівність:

$$Ev\left(Dv\left(h\big(Kv(Bv)\big)\right)\right) = h\big(Kv(Bv)\big) \qquad (4)$$

при позитивному результаті публікує трійку *Ev*, *Kv*(*Bv*), *Dv*(*h*(K*v*(*Bv*))).

Виборець:

- перевіряє в цьому опублікованому списку наявність запису про свій голос;
- якщо це передбачено регламентом виборів, на цьому етапі виборець може декілька разів змінити свій голос, відправивши нову трійку.

Етап 3 (підрахунок і оголошення результатів).

Виборець:

- відправляє трійку E_v, K_v, $D_v(h(K_v))$.

Адміністратор:

- перевіряє рівність:

$$Ev\left(Dv\big(h(Bv)\big)\right) = h(Bv) \qquad (5)$$

- у разі рівності розшифровує бюлетень $K_v^{-1}(K_v(B_v)) = B_v$;
- підраховує результати і публікує їх. Також публікує у відкритий доступ усю інформацію, що стосується бюлетенів і псевдонімів виборців, а саме: B_v, $K_v(B_v)$, K_v, $D_v(h(K_v(B_v))$, $D_v(h(K_v)))$, E_v. Усі бажаючі, включаючи виборців, можуть перевірити коректність дешифрування і підрахунку.

Гарантією анонімності є процедура підпису наосліп. В той же час відкритість даних щодо списку виборців, їх підписаних ключів і результатів підрахунку голосів робить систему прозорою і позбавляє недоброчесних організаторів/виборчих комісій можливостей маніпуляції результатами і фальсифікації. А гарантією відсутності повторного голосування є те, що виборець має тільки один підписаний ключ шифрування. Важливо, що схема передбачає можливість виборцю переголосувати до закінчення виборів, тобто змінити свій голос. Зауважимо, що дослідники вважають це аргументом на користь стійкості схеми щодо вимоги 7 – начебто зловмиснику невигідно купувати голос виборця, якщо далі виборець може змінити свій

вибір. Нижче ми розглянемо, чому це не зовсім так.

Проблема продажу голосів і варіант її вирішення

Схема виборів за протоколом *He-Su* багатьма дослідниками вважається найбільш досконалою. Дійсно, вона на перший погляд задовольняє усім вимогам, перерахованими вище. Особливо виділяють вимогу 7, а саме неможливість для виборця довести, як саме він проголосував, оскільки вважається, що це є перешкодою для торгівлі голосами. Дійсно, з розглянутих схем тільки протокол *He-Su* має таку властивість. Але дане твердження на нашу думку все ж є сумнівним. Розглянемо ситуацію, коли зловмисник пропонує викупити не голос виборця, а його приватний ключ ще на етапі реєстрації. У разі згоди далі зловмисник може повністю діяти від імені виборця, віддаючи його голос на власний розсуд.

Зазвичай, такий сценарій рідко розглядається спеціалістами з криптографії. Більше того, вимога 7 вважається необов'язковою при розгляді протоколів електронного голосування.

Справедливою є думка, що питання захисту від продажу голосів взагалі може лежати не в математичній, а в юридичній площині. Але якщо розглядати проблему з позиції теорії ігор, то вона математична. Дійсно, якщо закон забороняє купівлю/продаж під страхом достатньо жорсткого покарання, виборцю стає *невигідно* йти на змову з покупцем голосів. Тобто проблему можна було б вирішити шляхом підвищення жорсткості закону. На жаль, на практиці довести факт продажу голосу може бути проблематичним. Виборець може, наприклад, стверджувати, що його голос або ключ не купили, а вкрали. Сучасні месенджери і технології криптовалют дозволяють вести перемовини і розрахунки між продавцем і покупцем голосів дистанційно і анонімно.

Виходячи із вищесказаного нами було поставлено задачу унеможливити саму процедуру продажу приватного ключа в протоколі *He-Su* (оскільки купувати голос, як зазначалося, не має сенсу за відсутності можливості підтвердити свій вибір у даній схемі, або ж за наявності можливості переголосувати таємно від покупця пізніше).

Ключовою ідеєю запропонованого підходу є використання подвійної біометричної ідентифікації (наприклад на основі відбитка пальця). Біометрична автентифікація вже стала звичайною процедурою в багатьох галузях, а її методи постійно розширюються і вдосконалюються. Крім того, біометрія комбінується з методами криптографії, як для захисту самих біометричних даних [11], так і для генерації індивідуальних криптографічних ключів авторизації і доступу [12].

Ідея використання комбінації криптографічних і біометричних методів для електронного голосування не нова. Так, наприклад у роботі [13] пропонується поєднати технологію блокчейн із біометричною автентифікацією виборця під час голосування. У якості біометричного параметра автори пропонують сканування райдужної оболонки ока. З одного боку це вимагає невеликої технічної складності, але даний метод не є дуже надійним у порівнянні з іншими біометричними методами автентифікації. В той же час пропонується використовувати не самі біометричні дані (в даному випадку зображення ока), а тільки набір визначальних параметрів після обробки даного зображення, що, очевидно, має сенс з точку зору приватності і захисту персональних даних.

Сучасні системи біометричної автентифікації включають системи ідентифікації відбитків пальців, сканування сітківки ока і його райдужної оболонки, геометрію руки, обличчя, ДНК та інші.

Відомі методи генерації криптографічного ключа на основі біометричних даних [12, 14]. Такий ключ може бути відкритим криптографічним, який підписує адміністратор в протоколі *He-Su*. Тоді на другому етапі користувачу треба не тільки пред'явити підписаний ключ, але й авторизуватися за допомогою біометрії. При цьому кінцевий пристрій користувача

(наприклад, смартфон) формує надсилає підписаний хеш біометричної інформації. В цьому випадку анонімність виборця зберігається. Але для голосування потрібна фізична присутність виборця, що робить продажу голосу проблематичною, особливо дистанційно.

Більшість сучасних смартфонів здатні забезпечити біометричну автентифікацію. Якщо в якості біометричних даних, з яких генерується криптографічний ключ використовувати комбінацію 3*D* моделі обличчя і зображення райдужної оболонки ока, то це можна реалізувати за допомогою будь-якого гаджета із камерою. Але треба зазначити, що рівень помилок як першого так і другого роду для цих методів достатньо високий. Більш надійним є сканер відбитка пальця. Але в сучасних смартфонах біометричні шаблони відбитків пальців зберігаються у захищеній області, до якої не будуть мати доступ застосунок для генерації криптографічних ключів. Єдине, що можна забезпечити – це авторизація і біометричний доступ до самого застосунку.

Виходячи із вищесказаного, пропонується наступний алгоритм проведення виборів на основі комбінації протоколу *He-Su* і біометрії. На етапі особистої реєстрації виборець пред'являє не тільки свої документи/ідентифікатори, але й авторизується за допомогою відбитку пальця в застосунку (рис. 1). Надалі за допомогою застосунка підписує наосліп свій криптографічний ключ. На етапі голосування виборець також анонімно голосує із застосунка, використовуючи біометрію (рис. 2), що ускладнює продаж голосу без фізичної присутності виборця (наприклад, продаж через анонімний месенджер). Нарешті на етапі підрахунку і публікації результатів (рис. 3) виборці відправляють ключі розшифрування також через застосунок.

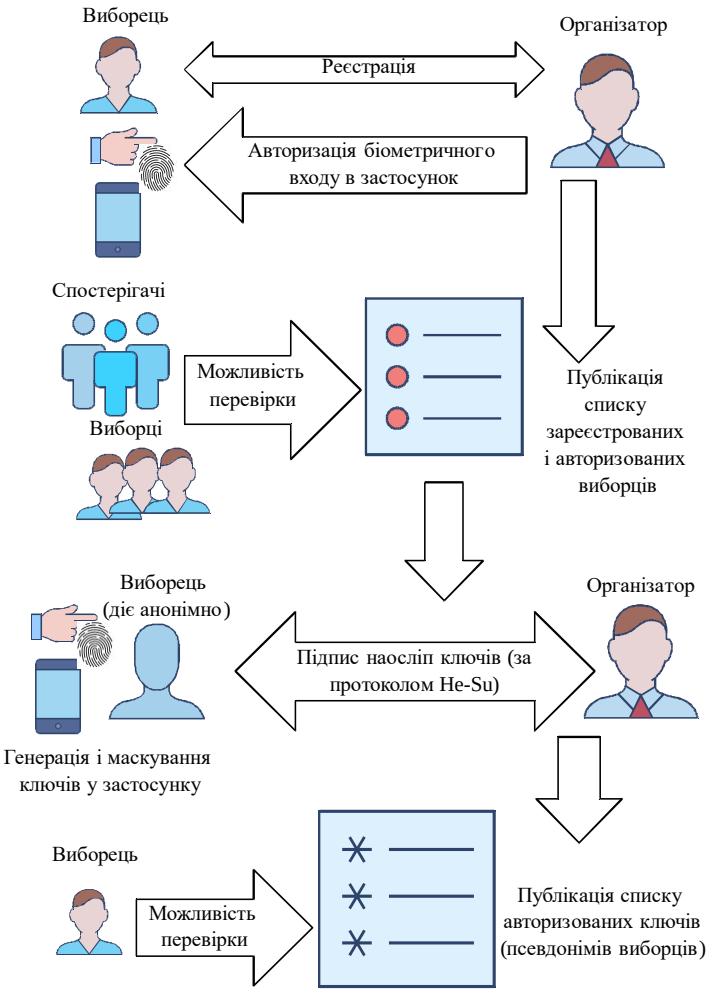

Рис. 1. Етап реєстрації

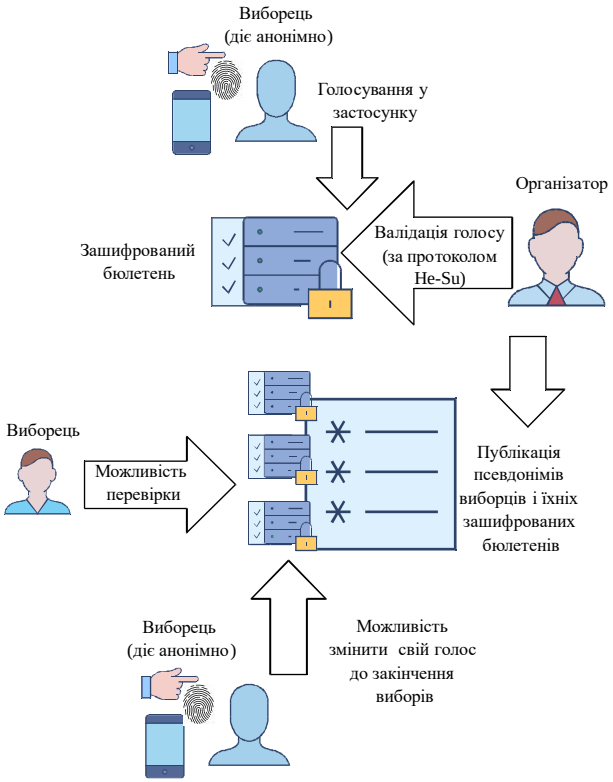

Рис. 2. Етап голосування

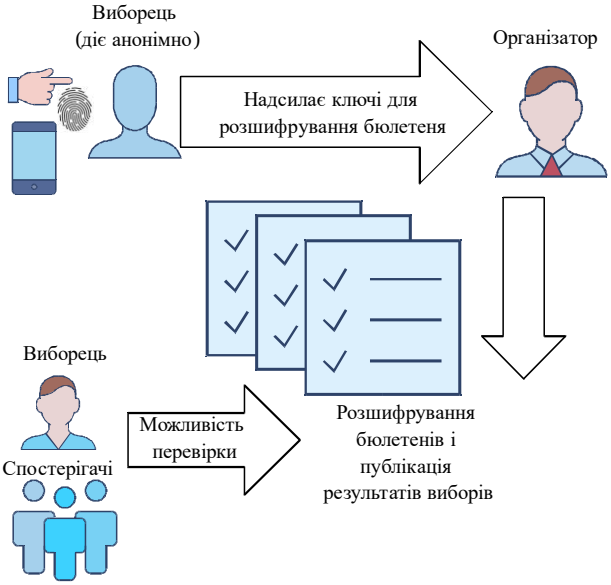

Рис. 3. Етапі підрахунку і публікації результатів

Звичайно, даний підхід не дає гарантії повного виключення продажу голосів (або примусу до голосування певним чином), оскільки залишається можливість присутності "людини за спиною". Тобто виборець свідомо може голосувати в присутності іншої особи. Тому бажано комбінувати криптографічні методи з юридичною відповідальністю за такі дії, як було зазначено вище. Підвищення технічної складності торгівлі голосами підвищує загальну якість процесу виборів і рівень довіри результатам у суспільстві.

Висновки

Електронне голосування перетворюється із дослідницьких проектів у реальність. Задача забезпечення демократичних виборів ставить суперечливі вимоги до системи електронного голосування, оскільки необхідно зберегти анонімність виборців і

при цьому запобігти шахрайству і зловживанням. Для вирішення цих питань залучаються методи криптографії, такі як симетричне і асиметричне шифрування, хешування, доведення з нульовим знанням, алгоритм розділення секретів і особливо криптографічний підпис наосліп. У даній статті були проаналізовані вимоги до електронного голосування і розглянуті деякі відомі схеми і підходи. Найбільш досконалою на нашу думку є протокол Хе-Су, оскільки він задовольняє майже усім вимогам, що пред'являються до процесу електронних виборів. Не до кінця вирішеною проблемою цього протоколу, як і інших відомих схем, є проблема продажу голосів виборців. У роботі пропонується застосовувати криптографічні методи в комбінації з біометричною автентифікацією для часткового вирішення цієї проблеми. Запропонований алгоритм проведення виборів ґрунтується на протоколі Хе-Су, що використовує гомоморфність криптографічної системи *RSA* процедуру сліпого підпису. Введення в алгоритм процедури біометричної автентифікації зменшує на нашу думку ймовірність продажу голосів недоброчесними виборцями, оскільки це стає складно зробити без фізичної присутності. Найбільш зручним видається біометрія відбитку пальця і використання мобільного застосунку, біометричний вхід у який авторизує організатор виборів.

Література

1. Schneier B. Applied Cryptography. Protocols, Algorithms, and Source Code in C. 2nd ed. New York : John Wiley & Sons, Inc., 1996. 784 p.

2. Brassard G., Crepeau C., Robert J.-M. All-or-Nothing Disclosure of Secrets. *Lecture Notes in Computer Science. Vol. 263. Advances in Cryptology - CRYPTO '86. Proceedings* / ed. by A. M. Odlyzko. Berlin, 1987. P. 234–238.

3. Heliosvoting project. URL: https://heliosvoting.org/.

4. Cortier V., Gaudry P., Glondu S. Features and usage of Belenios in 2022. *Electronic Voting* : proceedings of the 7th International Joint Conference, E-Vote-ID 2022, Bregenz, Austria, 4–7 October, 2022 / University of Tartu Press .Tartu, 2022. P. 53–56.

5. Chaum D. Blinding for unticipated signature. *Lecture Notes in Computer Science. Vol. 304. Advances in Cryptology – EUROCRYPT '87. Workshop on the Theory and Application of Cryptographic Techniques, Amsterdam, The Netherlands, April 13-15, 1987. Proceedings* / ed. by D. Chaum, W. L. Price. Berlin, 1988. P. 227–233.

6. Scantegrity. URL: http://www.scantegrity.org/

7. He Q., Su Z. A New Practical Secure e-Voting Scheme. *IFIP/SEC'98* : proceedings of the 14th International Information Security Conference, Vienna/Budapest, Austria/Hungary, 31 August-4 September, 1998 / Austrian Computer Society. 1998. P.196–205.

8. Yang C.-H., Su P.-C., Su T.-C.. A novel electronic voting mechanism based on Blockchain technology. *KSII Transactions on Internet and Information Systems*. Vol. 17, no. 10. P. 2862–2882.

9. Fujioka A., Okamoto., Ohta K. A practical secret voting scheme for large scale elections. *Lecture Notes in Computer Science. Vol. 718. Advances in Cryptology - AUSCRYPT '92. Workshop on the Theory and Application of Cryptographic Techniques, Gold Coast, Queensland, Australia, December 13-16, 1992. Proceedings* / ed. by J. Seberry, Y. Zheng. Berlin, 1993. P. 244–251.

10. Cranor L., Cytron R. K. Sensus: A Security-Conscious Electronic Polling System for the Internet. *30th Hawaii International Conference on System Sciences (HICSS)* : Volume 3: Information System Track-Organizational Systems and Technology, Maui, HI, USA, 3–6 January, 1997 / IEEE. Los Alamitos, 1997. P. 561–570.

11. Kakkad V., Patel M., Shah M. Biometric authentication and image encryption for image security in cloud framework. *Multiscale and Multidisciplinary Modeling, Experiments and Design*. 2019. Vol. 2. P. 233–248.

12. Gardham D., Manulis M., Drăgan C. C. Biometric-authenticated searchable encryption. *Lecture Notes in Computer Science.*

Vol. 12147. Applied Cryptography and Network Security. 18th International Conference, ACNS 2020, Rome, Italy, October 19–22, 2020, Proceedings, Part II / ed. by M. Conti et al. Cham, 2020. P. 40–61.

13. Pawade D. et al. Secure online voting system using biometric and blockchain. *Advances in Intelligent Systems and Computing. Vol. 1042. Data Management, Analytics and Innovation. Proceedings of ICDMAI 2019, Volume 1* / ed. by N. Sharma, A. Chakrabarti, V. E. Balas. Singapore, 2020. P. 93–110.

14. Chang Y.-J., Zhang W., Chen T. Biometrics Based Cryptographic Key Generation. 2004 *IEEE Conference on Multimedia and Expo* : proceedings, Taipei, Taiwan, 27–30 June 2004 / IEEE, 2005. P. 2203–2206.

Зудов О.М., Горіна В.В., Рибасова Н.О.

ПРОТОКОЛИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ НА ОСНОВІ КРИПТОГРАФІЧНОЇ СХЕМИ "СЛІПОГО ПІДПИСУ" І БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

В роботі проведено аналіз вимог до процедури електронного голосування і визначені деякі проблеми, які виникають при реалізації схем проведення виборів. Незважаючи на велику кількість існуючих схем проведення електронного голосування, що використовують різноманітні криптографічні методи, залишаються недоліки і вразливості, що потребують особливої уваги. Однією з таких проблем є запобігання продажу голосів. За основу вибрано один з найдосконаліших методів проведення голосування, а саме протокол Хе-Су, оскільки він задовольняє майже усім вимогам, що пред'являються до процесу електронних виборів. У роботі пропонується застосовувати криптографічні методи в комбінації з біометричною автентифікацією для часткового вирішення проблеми торгівлі голосами. Запропонований алгоритм проведення виборів ґрунтується на протоколі Хе-Су, що використовує гомоморфність криптографічної системи RSA процедуру сліпого підпису. Введення в алгоритм процедури біометричної автентифікації зменшує на нашу думку ймовірність продажу голосів недоброчесними виборцями, оскільки це стає складно зробити без фізичної присутності. Найбільш зручним видається біометрія відбитку пальця і використання мобільного застосунку, біометричний вхід у який авторизує організатор виборів.

***Ключові слова**: електронне голосування; криптографічні протоколи; підпис наосліп; біометрична автентифікація.*

Zudov O.M., Gorina V.V., Rybasova N.O.

ELECTRONIC VOTING PROTOCOLS BASED ON BLIND SIGNATURE CRYPTOGRAPHIC SCHEME AND BIOMETRIC AUTHENTICATION

The paper analyzes the requirements for the electronic voting procedure and identifies some problems that arise during the implementation of election schemes. Despite the large number of existing electronic voting schemes that use various cryptographic methods, there are still shortcomings and vulnerabilities that require special attention. One such problem is the prevention of vote selling. One of the most advanced voting methods, namely the He-Su protocol, was chosen as the basis, as it meets almost all the requirements for the electronic election process. The paper proposes to use cryptographic methods in combination with biometric authentication to partially solve the problem of vote selling. The proposed election algorithm is based on the He-Su protocol, which uses the homomorphism of the RSA cryptographic system and the blind signature procedure. Introducing the biometric authentication procedure into the algorithm reduces, in our opinion, the probability of votes being sold by unscrupulous voters, as it becomes difficult to do this without physical presence. Fingerprint biometrics with the use of a mobile application, and a biometric login authorized by the election organizer, appear to be the most convenient.

***Keywords**: E-voting; cryptographic protocols; blind signature; biometric authentication.*