

Приватний вищий навчальний заклад «Міжнародний науково-технічний  
університет імені академіка Юрія Бугая»  
Полтавський інститут бізнесу  
Кафедра програмної інженерії та інформаційних технологій

## Випускна бакалаврська робота

на здобуття вищої освіти першого (бакалаврського) рівня студента зі  
спеціальність 121 «Інженерія програмного забезпечення»

### **Серверне та клієнтське програмне забезпечення для проведення електронних таємних виборів**

Виконала: студентка Малеванченко Вікторія

Науковий керівник:

Галузь знань 12 «Інформаційні технології»,

Полтава – 2020

## ЗМІСТ

ВСТУП.

РОЗДІЛ 1. СУЧАСНИЙ СТАН ЕЛЕКТРОННОГО ГОЛОСУВАННЯ.

- 1.1. Історія електронного голосування та спроби його реалізації.
- 1.2. Вимоги до електронного голосування.
- 1.3. Протоколи електронного голосування, їх переваги та недоліки.

РОЗДІЛ 2. ОСОБЛИВОСТІ СУЧАСНОГО ВИБОРЧОГО ПРОЦЕСУ В УКРАЇНІ ТА МОЖЛИВОСТІ ЙОГО РЕАЛІЗАЦІЇ ШЛЯХОМ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ.

- 2.1. Загрози для виборчого процесу та пріоритети щодо їх запобігання.
- 2.2. Мережева анонімність та таємність голосування.
- 2.3. Проблема первинної аутентифікації виборців.

РОЗДІЛ 3. КОМПЛЕКСНИЙ ПРОТОКОЛ ТАЄМНОГО ГОЛОСУВАННЯ, АДАПТОВАНИЙ ДО НАЦІОНАЛЬНИХ ВИБОРІВ ТА СУЧАСНИХ УМОВ ЇХ ПРОВЕДЕННЯ.

- 3.1. Базові компоненти протоколу.
- 3.2. Етапи таємного голосування .
- 3.3. Реалізація клієнт-серверного програмного забезпечення для таємного голосування.

ВИСНОВКИ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.

**Актуальність роботи.** Особливої актуальності дана тема набула в зв'язку з подіями останнього року: епідемією Covid-19 та виборами в Білорусі та США, де відзначені фальсифікації, що могли спотворити загальний результат. Так, в Білорусі спільнота вказує на грубі порушення підрахунку голосів з боку рахункової комісії. В США відзначається інша ситуація – спроби «вкидання» бюлетенів, надісланих поштою. Останній випадок яскраво свідчить про недопустимість перекладання відповідальності щодо захисту виборів на організації, які безпосередньо не являються учасниками виборчого процесу. Тому забезпечення захисту виборів повинне бути реалізоване виключно структурами, що проводять ці вибори та ніяким чином не спиратися на будь-які інші системи захисту (пошту, банки, мобільні оператори та ін.).

**Метою** роботи є вдосконалення виборчого процесу в сучасних умовах з урахуванням його національних особливостей шляхом впровадження електронних програмних засобів з використанням криптографічно стійких алгоритмів та протоколів.

**Об'єкт дослідження:** електронний виборчий процес з урахуванням сучасних умов та його національних особливостей.

**Предмет дослідження:** алгоритми серверного та клієнтського програмного забезпечення, що реалізують електронне голосування з урахуванням визначених вимог.

**Задачі дослідження:**

1. Проаналізувати особливості виборчого процесу в сучасних умовах (з урахуванням протиепідемічних заходів, пов'язаних з епідемією Covid-19).
2. Дослідити національні особливості виборчого процесу в Україні, оцінити можливі безпекові загрози, враховуючи досвід попередніх виборів в Україні, Росії, Білорусі та США.
3. Розробити протокол, що найбільш повно відповідає вимогам до виборів в Україні, з використанням сучасних криптографічно стійких елементів.

4. Розробити та апробувати програмне забезпечення, що реалізує цей протокол та відповідає основним вимогам до захищеного коду.

5. Проаналізувати якість інтерфейсу користувача шляхом аналізу його зрозумілості студентами нетехнічних спеціальностей, розробити ефективну інструкцію користувача.

**Наукова новизна** одержаних результатів визначається розробкою протоколу електронного голосування, що забезпечує основні вимоги до проведення таємного голосування з урахуванням національних особливостей процесу голосування та характерних безпекових загроз.

**Практичне значення** одержаних результатів. Запропонована модифікація протоколу таємного голосування в поєднанні зі способом первинної ідентифікації виборця та з використанням мережевого анонімізатора Tor можуть бути використані в якості компонентів для інтеграції з системами голосування державного масштабу. Вихідні коди можуть бути використані у вигляді готових модулів та бібліотек, що відповідають вимогам до криптографічного захисту.

## Реферат:

Електронне таємне голосування особливо актуальне в умовах протикарантинних заходів, зумовлених епідемією Covid-19, тому що не може впливати на епідемічну ситуації та не може бути відмінене у випадку її погіршення. Використання сучасних криптографічних алгоритмів виключає можливість спотворення результатів виборів організаторами чи іншими зацікавленими сторонами. Публічний та індивідуальний контроль на всіх етапах голосування надають виборам повну прозорість. Використання мережі DarkNet (прихованого onion-сервісу) забезпечує таємність голосування та контролю за їх результатом з боку виборців та волонтерів. Запропонований доказово стійкий протокол таємного голосування базується на відомому протоколі He-Su, адаптованому з урахуванням пріоритетів основних безпекових загроз в сучасних національних умовах та доповнений захищеним механізмом первинної аутентифікації виборця за протоколом з нульовим розголошенням SPEKE з використанням паперового запрошення у вигляді QR-коду. Анонімізатор Tor, інтегрований в серверне та клієнтське програмне забезпечення, запобігає відслідковуванню IP-адрес виборців.

Робота містить 72 сторінок друкованого текст, включає вступ, три розділи, висновки та практичні рекомендації, містить 1 таблицю та 21 рисунок. Список використаних джерел містить 35 посилань. Повний відкритий вихідний код сервера таємного голосування (Linux, Windows), утиліти для роботи з базою даних виборців (Windows) та клієнтського додатку (Android, Windows) розміщені у персональному GitHub-репозиторії автора та доступні за посиланням: <https://github.com/vikanmtu>. Вихідний код виконаний на мовах ANSI C (ядро протоколу, криптографічні примітиви) та C++ (графічний інтерфейс для Windows та Android) та безпосередньо містить всі необхідні бібліотеки на мові C, не використовує зовнішніх залежностей та відповідає вимогам щодо криптографічної стійкості. Код містить близько 600 файлів та

близько 20000 рядків, з яких близько 30% є авторськими. Підготовлене програмне забезпечення (виконуючі файли сервера, менеджера бази даних та клієнтські додатки) доступні в сховищі проекту та підготовлені для інсталяції на Windows та Android пристрої для тестування, супроводжуються детальною інструкцією по налаштуванню серверу (завдяки використанню Tor він не потребує виділеного хостингу чи статичної IP-адреси та може бути запущений на будь-якому Windows-комп'ютері, підключеному до Інтернет), створенню бази виборців та списку кандидатів, підготовці індивідуальних запрошень у вигляді QR-кодів та роботі виборця з додатком користувача на мобільному телефоні, планшеті чи ноутбукові. Результати тестового голосування будуть доступні на сервері через web-браузер з будь-якого пристрою, підключеного до мережі Інтернет.

## РОЗДІЛ I. СУЧАСНИЙ СТАН ЕЛЕКТРОННОГО ГОЛОСУВАННЯ.

### 1.1 Історія електронного голосування та спроби його реалізації.

Ідея електронних виборів привернула загальну увагу в останні 20 років. Перші публікації на цю тему з'явилися ще наприкінці минулого століття, але остаточного вирішення всіх питань до цих пір немає, тема все ще розвивається. У електронних виборів чимало переваг перед виборами звичайними. Хоча придумати схему і зробити електронні пристрої досить дорого, в дійсності електронні вибори дешевше, оскільки витрати на них є одноразовими. Одне і те ж обладнання або програмне забезпечення можна буде використовувати багаторазово. З'являється можливість частіше проводити вибори, люди будуть більше брати участь в управлінні державою, чинити більший вплив на політику. Другий важливий аргумент на користь електронних виборів - мобільність. Електронні комунікації можна провести навіть в ті куточки земної кулі, де важко організувати виборчі дільниці. Нарешті, результати електронних виборів перевірятися, тобто можна повністю контролювати підрахунок голосів. Проекти впровадження системи електронних виборів всерйоз обговорюються в Данії, Естонії, в штаті Арізона (США).

Виборці в Естонії [13] мають можливість віддати свій голос через Інтернет на місцевих та парламентських виборах. Вони або використовують своє національне посвідчення особи, обладнане мікрочіпом, або мобільний телефон із додатком Mobile-ID. Естонія була першою країною у світі, яка запровадила Інтернет - голосування на національних виборах, а електронне голосування із обов'язковими результатами проводиться з 2005 року. Естонські голоси в Інтернеті можна віддати в дні попереднього голосування, тобто з 10-го по 4-й день до виборів. Таким чином, це схоже на попереднє голосування за допомогою паперових бюлетенів.

Інтернет - голосування популярне насамперед тому, що воно є ефективним та зручним, процедура займає лише кілька хвилин. Сьогодні близько третини голосів віддається через Інтернет. Але зростання кількості користувачів відбувається повільно, враховуючи те, що на охоплення однієї третини виборців пішло 15 років, і що Естонія є лідером у сфері електронного врядування, де багато людей звикли взаємодіяти з державними установами в режимі он-лайн. Фонові змінні, такі як вік та стать, майже не впливають на використання он-лайн - голосування або взагалі не впливають на нього. Основна різниця в структурі голосування стосується відстані; Люди частіше голосують в Інтернеті, а не на папері, коли живуть на відстані більше 30-хвилин до виборчої дільниці. Так само естонці, які проживають за кордоном, частіше голосують через Інтернет. Приблизно 90% голосів з-за кордону на виборах в Естонії віддається зараз як он-лайн голоси; навряд чи хтось голосує поштою чи в посольствах.

Немає доказів того, що он-лайн - голосування в Естонії призвело до збільшення явки виборців. Аналіз показує, що загальна явка дійсно зросла незначно після запровадження Інтернет - голосування, але не можна стверджувати, що це стосувалося лише он-лайн голосування як такого.

Естонія вирішила створити окрему установу на державному рівні, Комітет з електронного голосування для управління Інтернет - системою голосування, щоб забезпечити довіру до системи. Незважаючи на те, що он-лайн - система голосування була повністю функціональною до 2005 р. І була запущена в масштабах всієї країни за один раз, процедури були суцільно вдосконалені. Система, що використовується в даний час, була завершена до місцевих виборів 2017 року

Виборці мають можливість змінити свій голос, оскільки це було визнано необхідним для забезпечення свободи волевиявлення виборця. Можливість змін захищає виборця від впливу на його результат голосування. Вплив на виборця не може бути ефективним, оскільки виборець може змінити своє



рішення пізніше в електронному вигляді або за допомогою бюлетеня для голосування на виборчій дільниці.

У рішенні, винесеному в 2005 році, Верховний суд Естонії зазначив наступне: «Зрозуміло, що у випадку електронного голосування у неконтрольованій ситуації, тобто через Інтернет за межами дільниці для голосування, державі важче гарантувати, що голосування вільне від зовнішнього впливу та є таємним. /../ Суд вважає, що можливість зміни результату власного електронного голосування необхідна для гарантування свободи виборів та таємниці голосування».

У Швейцарії он-лайн - голосування пілотувалось на місцевих референдумах у десяти кантонах. Умови введення он-лайн голосування у Швейцарії були дуже конкретними, оскільки референдуми відбуваються приблизно чотири рази на рік, що може спричинити втому виборців. Крім того, голосування «без нагляду» є звичним явищем і вважається кращим ніж голосування на папері на виборчих дільницях, тобто близько 90% усіх голосів віддається за допомогою голосування поштою. Обґрунтуванням прийняття он-лайн системи у Швейцарії було покращення зручності для виборців та збільшення явки, яка є досить низькою.

Через проблеми з безпекою пілотування було зупинено в 2019 році. Тим не менше, он-лайн - голосування продовжує розглядатися як важлива послуга для виборців, і намір полягає у встановленні стабільного її функціонування із використанням систем останнього покоління в найближчі роки.

В Канаді он-лайн - голосування застосовується на муніципальному рівні в деяких провінціях, де муніципалітетам дозволено організовувати такі процедури. Не існує національного стандарту он-лайн - голосування; муніципалітети розробили власні системи або використали те, що створили інші. Тоді як деякі муніципалітети вимагали від виборців попередньої реєстрації для отримання ПІН-коду, необхідного для он-лайн - голосування, інші просто розсилали ПІН-коди всім виборцям зі списку виборців.

## **1.2. Вимоги до електронного голосування.**

Електронне голосування - це спосіб волевиявлення громадян на основі інформаційних та комунікаційних технологій, що охоплює різні форми голосування (вибори, референдуми, вивчення громадської думки, проведення громадських слухань та обговорень) та здійснюється за допомогою Інтернет з використанням біометричних параметрів або цифрового підпису особи [1].

Метою запровадження електронного голосування є створення демократичних умов для суб'єктів виборчого процесу та забезпечення прав і можливостей віддаленого доступу виборців до систем голосування. Електронне голосування включає забезпечення достовірності волевиявлення громадян та захисту результатів голосувань з питань як державного, так і місцевого управління, а також щодо програм розвитку територій і держави в цілому за широкою участю громадськості [2].

Втілення європейських стандартів якості електронних адміністративних послуг [6], відкритості і прозорості діяльності як державних, так і місцевих органів влади шляхом ефективного використання широкого спектру функціональних можливостей електронних технологій. Ефективне залучення найбільшої кількості громадян до участі у вирішенні державних проблем внаслідок суттєвого зниження ризиків щодо фальсифікацій результатів та доступності системи, а відтак зростання довіри та відчуття відповідальності за прийняті рішення. Необхідна мінімізація впливу людського фактора на кінцевий результат під час проведення виборів чи голосувань з інших питань [3]. Важливим є забезпечення належних конституційних прав особам, відсутнім у період голосування за місцем проживання або нездатним самотійно пересуватися, тобто інвалідам та людям похилого віку [4,5].

Електронне голосування здійснюється на таких принципах [7]:

1. Універсальність права голосу: всі люди мають право голосу на підтримку кандидата чи питання у разі проведення референдуму незалежно від раси, кольору шкіри, політичних, релігійних та інших переконань, статі,

етнічного та соціального походження, майнового стану, місця проживання, мовних або інших ознак.

2. Рівність права голосу: кожен виборець має рівну кількість голосів (право одного голосу або можливість голосувати декілька разів з урахуванням тільки останнього його голосу).

3. Свобода волевиявлення: особа має право вільно обирати та бути обраною. Здійснення тиску на вибір особи не допускається. Обмеження волевиявлення особи можливе лише у випадках прямо передбачених Законом.

4. Таємність права голосу: виборець має право на власне волевиявлення шляхом таємного голосування, зберігаючи в подальшому конфіденційність свого права вибору, та мати реальні можливості захистити це право [8].

5. Пряме право голосу: вибір, зроблений виборцями, безпосередньо визначає обраних осіб або інше прийняте громадянами колективне рішення.

Система електронних голосувань повинна відповідати таким вимогам [9]:

1. Забезпечувати максимальне використання наявного в Україні електронного комунікаційного обладнання, зокрема того, що перебуває у власності громадян (мобільні телефони, ноутбуки, комп'ютери, тощо).

2. Дозволяти здійснення дистанційного голосування необхідну кількість разів з будь-якої місцевості та з будь-якої виборчої дільниці чи без її відвідання.

3. Підтверджувати голосуючому відповідність зарахування його голосу на будь-якому етапі голосувань та підрахунків, але зараховувати для підрахунку голосів тільки останнє голосування одного і того ж самого виборця.

4. Здійснювати підрахунок голосів у режимі реального часу безпосередньо в процесі голосувань та забезпечувати їх візуалізацію як через електронні системи зв'язку, так і через телевізійні канали.

5. Бути надійною та гарантувати захист від несанкціонованих втручань [10].

6. Відповідати вимогам конфіденційності голосувань, захищеності електронних архівувань та відповідального використання підсумків голосувань.

7. Забезпечувати захищеність від помилок користувачів та обслуговуючого персоналу.

8. Базуватися на модульному принципі, який би дозволяв розширювати масштаби і функціональні можливості системи та подальшого її інтегрування в систему "Електронний уряд".

9. Містити електронну систему поточного контролю за перебігом голосування та підведенням їх підсумків.

10. Взаємодіяти з електронним реєстром виборців (учасників голосувань), електронними підписами або з біометричними даними виборців та іншими унікальними кодами доступу.

Під час підготовки до проведення виборів кожен виборець, який має намір скористатися електронною системою голосування, у визначені терміни перевіряє на сайті ЦВК наявність інформації про нього в електронному реєстрі виборців. У разі відсутності інформації, наявності в ній помилок або з інших причин виборець має можливість виправити ситуацію шляхом входу за допомогою біометричних параметрів чи електронного підпису в електронну базу реєстру з власного електронного пристрою, або шляхом відвідання будь-якої виборчої дільниці на власну сторінку реєстру та внести відповідні уточнення і, таким чином, Єдиний комп'ютерний реєстр виборців актуалізується в автоматичному режимі особисто виборцями. Кандидати, які балотуються на виборах, в електронних виборчих бюлетенях і виборчих списках мають бути позначені відкритими і загальнодоступними цифровими ідентифікаторами та популяризуватися виборчими комісіями через мережу Інтернет, а також через канали телебачення і друковані засоби масової інформації, що дозволяє виборцям протягом виборчої кампанії ретельно ознайомитися з усіма подробицями про всіх кандидатів та скласти об'єктивне

враження про них, а отже зробити свій свідомий вибір та посилити його на зустрічах або інших агітаційних заходах.

Система електронного голосування має забезпечити взаємодію декількох електронних баз даних і, перш за все: електронного реєстру виборців, електронних бюлетенів, виборчих списків, електронних голосувань виборців шляхом введення ними у систему власних біометричних параметрів або електронного підпису та цифрових ідентифікаторів відповідних кандидатів. Єдиний комп'ютерний реєстр виборців повинен мати закриті поля з біометричними параметрами або електронним підписом [11, 12]. Це відкриває доступ до системи голосування тільки шляхом розпізнання введених власних ідентифікаторів і, таким чином, надає можливість контролювати зарахування голосу та отримати доступ до електронної системи голосування в межах, необхідних для здійснення виборцем тільки власного волевиявлення.

Виборець, який обрав електронний спосіб голосування, через свій або такий, що належить будь-якій дільничній виборчій комісії, кінцевий електронний пристрій, вводить у єдиний комп'ютерний реєстр власні ідентифікатори (біометричні параметри чи електронний підпис), або передає через СМС чи ММС повідомлення з відповідним власним ідентифікатором з мобільного телефону. У разі розпізнання ідентифікатора система в автоматичному режимі відкриває йому доступ до його особистого файлу в системі електронних голосувань, до якої він через електронне повідомлення має можливість ввести цифровий ідентифікатор обраного ним кандидата чи питання, яке він підтримує, та в подальшому контролювати відсутність несанкціонованих змін прийнятого ним рішення, аж до кінцевого підрахунку голосів. При цьому має бути передбачена сувора і незворотна кримінальна відповідальність за порушення таємності волевиявлення громадянина, в тому числі за замах на несанкціоновані втручання і фальсифікації в особистому електронному файлі виборця [14, 15].

Громадяни, які беруть участь у голосуванні, поділяються на такі категорії:

1. Виборці, які не бажають користуватися новими технологіями та віддають перевагу існуючим. Для них процес голосування відбувається традиційно за допомогою паперових бюлетенів (Категорія "А") тільки на конкретних виборчих дільницях (крім тих, хто за законом голосує на дому) та в єдиній визначеній для цього даті.

2. Виборці, які бажають скористатися електронною технологією голосувань, але не мають технічних можливостей (мобільних телефонів, ПК тощо), реалізують право свого волевиявлення на будь-якій виборчій дільниці, на яку виборцю зручніше потрапити, також у єдиний визначений день, користуючись кінцевими електронними пристроями будь-якої виборчої дільниці (Категорія "Б").

3. Виборці, які бажають скористатися електронними технологіями голосувань та при цьому мають власні технічні можливості, можуть скористатися системою віддаленого голосування шляхом відправки СМС, ММС або іншого передбаченого Законом способу повідомлення на електронні пристрої системи (Категорія "В").

Виборці категорії передбачених пунктом другим і третім мають можливість здійснювати свій вибір багаторазово протягом періоду голосування, визначеного Центральною виборчою комісією, а система електронних голосувань має забезпечити зарахування тільки останнього їхнього голосу.

### **1.3 Протоколи електронного голосування, їх недоліки.**

Термін «електронне голосування» означає сукупність концепцій. Вони відрізняються за формою виборів (публічні чи приватні) та місцем голосування (дільниця, кіоск чи віддалено). В основному розглядаються такі способи електронного голосування, як електронні урни (kiosk voting), віддалене

електронне голосування, Інтернет – голосування [21]. Електронні урни - спосіб голосування за допомогою спеціалізованих машин в обладнаних для цього дільницях під наглядом урядових працівників. Виборці здійснюють свій вибір за допомогою електронного пристрою (використовуючи сенсорні екрани). Голоси підраховуються на індивідуальних машинах DRE (Direct Recording Electronic). Потім передаються до центральної лічильної комісії одним із доступних способів. Як додатковий засіб безпеки можна роздрукувати бюлетень. Віддалене електронне голосування передбачає голосування будь-яким доступним віддаленим способом - за допомогою Інтернет, текстових повідомлень, інтерактивного кабельного телебачення чи телефонів. Інтернет - голосування - окремий випадок віддаленого електронного голосування, яке здійснюється через Інтернет. Часто терміни «Інтернет - голосування» і «віддалене електронне голосування» вживаються як взаємозамінні. У цій роботі обидва терміни використовуються у другому значенні, якщо попередньо не вказано. Чимало держав для голосування використовують електронні урни, які розміщуються у публічних місцях, і процес голосування контролюється певною платформою (апаратне та програмне забезпечення, за допомогою якого відбувається голосування і саме розміщення). Віддалене Інтернет - голосування передбачає «вкидання» бюлетеня у не призначених для цього місцях (школа, дім, офіс), де виборець чи інші засоби контролюють клієнта. За ідеальних умов, такий тип відкритої мережевої системи уможлиблює голосування із будь-якого місця у зручний для виборця час

Припустимо, що ми відмовляємося від таємниці голосування. Тоді можна запропонувати просту схему проведення виборів.

- Кожен говорить своє рішення; недолік - можна сказати двічі, це важко помітити.
- Всі оголошують своє рішення, надсилають його зі своїм ім'ям і підписом.

Два основні шляхи до запровадження таємниці голосування:

1. Всі бачать голос, але ніхто не знає, чий він. В такому випадку стає неможливо не опубліковувати проміжні результати. Дійсно, у цього підходу безліч недоліків. Головний інструмент для реалізації - анонімний канал (в канал надсилається повідомлення, невідомо, від кого воно виходить). Основна проблема - контроль за виборцями (неможливо проконтролювати, хто проголосував двічі).

2. Всі знають, кому належить даний голос, але ніхто не може розшифрувати вибір. Для того щоб отримати шифротекст всіх бюлетенів, можна використовувати гомоморфне шифрування [16, 17, 18]. Потім, розшифрувавши цей об'єднаний шифротекст, отримуємо суму всіх голосів.

Ситуація така: є безліч незалежних організаторів, більшість з яких чесні. Голоси надсилаються кожному з організаторів на вибір голосуючого (або випадково). Вважається, що організатори не зберуться разом для розшифровки окремих голосів, оскільки вони є чесними [22].

### **Псевдоніми [21].**

Отже, головна проблема анонімного каналу - забезпечення контролю за виборцями. Вирішується вона створенням псевдоніма. Під час першої фази виборець, спілкуючись з організаторами, створює спеціальне повідомлення (псевдонім). Організатори не знають, якому виборцеві який псевдонім належить. Виборець може створити лише один псевдонім. Організатори можуть проконтролювати виборців, склавши список осіб, що беруть участь у виборах. У другій фазі відбувається власне голосування. Виборець посилає за анонімним каналу пару, що складається з псевдоніма і голосу. Організатори підсумовують голоси з відповідним коректним псевдонімом та можуть проконтролювати, скільки різних виборців взяло участь у виборах. Виборець, в свою чергу, може проконтролювати, що його голос був включена в перелік.

### **Протокол He-Su [20]**

Протоколом, заснованим на ідеї сліпого підпису, є протокол He- Su. Він задовольняє майже всім пред'явленим вимогам до таємного голосування. В



даному алгоритмі беруть участь три сторони - виборець, адміністратор і лічильник. Але, на відміну від протоколу Fujioka-Okamoto-Ohta, в схемі He-Su підписується ключ виборця, а не бюлетень. Процес голосування можна розділити на 10 етапів:

**1) Первинне налаштування виборця:**

- Виборець генерує пару ключів -  $D_v$  (закритий) і  $E_v$  (відкритий);
- Генерує випадкове число  $R$  (маскуючий множник);
- Обчислює  $E_a(R) * (h(E_v))$ , де  $E_a$  - відкритий ключ адміністратора,  $h$  - хеш функція;
- Відправляє результат адміністратору.

**2) Адміністратор перевіряє легітимність виборця;**

- Підписує прийняте повідомлення:  $D_a(E_a R * Da(h(E_v))) = R * Da(h(E_v))$ , де  $D_a$  - особистий ключ адміністратора.
- Відправляє результат виборцю;
- Публікує список авторизованих виборців.

**3) Отримання підпису:**

- Виборець прибирає маскуючий множник  $R$  з отриманого повідомлення;
- Перевіряє рівність  $E_a(D_a(h(E_v))) = h(E_v)$ ;
- При правильному результаті виборець переконується в тому, що має підписаний ключ.

**4) Анонімна реєстрація:**

- Виборець відправляє лічильнику  $E_v$  і  $Da(h(E_v))$ .

**5) Авторизація виборця лічильником:**

- Лічильник перевіряє рівність  $E_a(D_a(h(E_v))) = h(E_v)$ ;
- При правильному рівності лічильник авторизує ключ  $E_v$ ;
- Публікує список авторизованих ключів.

**6) Отримання бюлетеня:**

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

### 7) Голосування:

- Лічильник перевіряє, чи є ключ  $E_v$  авторизованим;
- Перевіряє рівність  $E_v (D_v (h (K_v (B_v)))) = H (K_v (B_v))$ ;
- При позитивному результаті публікує  $E_v, K_v (B_v), D_v (h (K_v (B_v)))$ .

### 8) Перевірка виборцем голосу:

- Виборець перевіряє в опублікованому лічильником аркуші наявність запису про свій голос (з пункту 7);
- У разі відсутності запису виборець звертається до відповідних органів.

### 9) Розкриття голосу:

- Виборець відправляє лічильнику  $E_v, K_v, D_v (h (K_v))$ ;

### 10) Врахування голосу лічильником:

- Лічильник перевіряє рівність  $E_v (D_v (h (B_v))) = h (B_v)$ ;
- У разі рівності отримує бюлетень  $K_v -1 (K_v (B_v)) = B_v$ ;
- Публікує інформацію:  $B_v, K_v (B_v), K_v, D_v (h (K_v (B_v))), D_v (h (K_v)), E_v$ .

До переваг протоколу He-Su можна віднести можливість виборця змінювати свій голос під час виборів. Виборець може зробити це, не розкриваючи свій бюлетень. Крім того, протокол досить простий і має малу обчислювальну складність

## РОЗДІЛ 2. ОСОБЛИВОСТІ СУЧАСНОГО ВИБОРЧОГО ПРОЦЕСУ В УКРАЇНІ ТА МОЖЛИВОСТІ ЙОГО РЕАЛІЗАЦІЇ ШЛЯХОМ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ.

### 2.1. Загрози виборчого процесу, та пріоритети щодо їх запобігання.

В останній рік важливу роль відіграє важливий фактор – карантинні заходи, спричинені епідемією Covid-19. Вибори – це завжди скупчення людей, що потенційно небезпечно в умовах епідемії та може значно погіршити епідемічну ситуацію в регіоні. З іншого боку, існує реальна загроза спланованого «зриву» проведення виборів з посиленням на надумане погіршення епідемічної ситуації шляхом введення так званого «локдауну» чи навіть надзвичайного стану правлячими силами, які прогнозують свою поразку у разі, якщо вибори відбудуться.

Залежно від поставлених виборцям питань можна виділити такі типи виборів:

- з відповіддю типу «так / ні»;
- вибір одного з декількох кандидатів ( "1 з L");
- вибір певної кількості з декількох кандидатів ( "K з L") - застосовується, наприклад, на муніципальних виборах; • вибір не більше ніж певної кількості з кандидатів ( " $\leq K$  з L");
- вибір певної кількості з декількох кандидатів з розстановкою пріоритетів, коли стоїть в підсумковому списку раніше вважається важливіше (Упорядкований варіант "K з L");
- "1-L-K" - вибір K елементів з одного з L списків; така система застосовується в США при обранні вибірників (є списки кандидатів в виборщики від L партій, потрібно сформувати команду від однієї партії); • відкрите питання, що має на увазі відкриту відповідь (можна писати будь-який текст).

В даному дослідженні основна увага зверталася на вибори другого типу (вибір одного з декількох кандидатів), що відповідає, наприклад, виборам Президента України.

Іншою важливою характеристикою виборів є таємність, що передбачає неможливість визначення голосу конкретного учасника виборів. Історично склалося, що вибори в Україні таємні: кожен учасник на виборчій дільниці отримує бюлетень, в якому наявний лише порядковий номер та відсутні будь-які персональні дані виборця. За рахунок перемішування бюлетенів у виборчих скриньках в подальшому неможливо пов'язати конкретний бюлетень з конкретним виборцем. Якщо бути відвертим, то теоретично така можливість існує (наприклад, шляхом співставлення краю відриву персональної та анонімної частини бюлетеня), але використання її надто затратне для масової деанонімізації голосів виборців.

Вибори зазвичай проводяться в 3 фази:

1. Ініціалізація: оголошується питання, складається список голосуючих, генеруються ключі для криптосистем.
2. Голосування: в англомовних джерелах учасники виборів називаються voters, організатори виборів - authority. Учасники взаємодіють з організаторами. У підсумку організатори отримують інформацію, яка є відображенням голосу ("електронний контейнер" з голосом).
3. Підрахунок голосів: організатори обчислюють і публікують результати виборів, які учасники та волонтери перевіряють, таким чином впевнюючись у чесності виборів.

### **Вимоги до схеми виборів [23]**

1. Контроль над виборцями. У виборах можуть брати участь тільки занесені в список виборці, одна людина має лише один голос.
2. Анонімність, таємниця голосування. Не можна дізнатися вибір конкретного виборця.

3. Індивідуальний контроль. Кожна людина може перевірити, що його голос підрахований.

4. Універсальний контроль. Можна перевірити, що результат виборів вірний (що не були вкинуті зайві бюлетені).

5. Стійкість. Некоректні дії деяких виборців або невеликої частини організаторів не можуть зірвати вибори.

6. Непідтверджуваність. Після виборів не можна довести, що людина проголосував певним чином. При невиконанні цієї вимоги можна буде, по-перше, укласти договір на покупку голосу, по-друге, змушувати голосувати будь-яким чином (наприклад, в армії або у в'язниці).

7. Не можна голосувати за іншу людину.

8. Не можна скопіювати чужий голос або змінити його (створити інший на його основі).

9. Не повинно бути можливості дізнатися проміжні результати. Спочатку голосування проводиться в зашифрованому вигляді, потім виборці дають розшифрувати свої голоси

Варто зауважити, що у випадку реалізації вимоги 6 (непідтверджуваність) при виконанні індивідуального контролю ми перевіряємо, підрахований чи наш голос взагалі, а не те, як він інтерпретований. Вимога непідтверджуваності несумісна з тим, щоб виборець мав можливість перевірити, чи правильно врахували його голос. Тому виконання даної вимоги залежить від пріоритетів та особливостей конкретних виборів. В нашій роботі ми вважали за краще ігнорувати дану вимогу та забезпечити можливість врахування голосу кожним виборцем. Таким чином, був наданий дієвий механізм захисту від шахрайства саме рахівника, що важливо, зважаючи на аналіз останніх президентських виборів у Білорусі. При цьому проблеми запобігання укладання договору щодо результату голосування (продажу голосу) та голосування під примусом залишаються відкритими. Але ці проблеми значно менш важливі, адже продати голос завжди

можливо іншими шляхами, ніж укладанням договору з оплатою після виборів, а можливість примусу охоплює лише незначну частку виборців і також може бути реалізована іншими шляхами (наприклад, голосування під безпосереднім наглядом або навіть іншою особою).

## **2.2 Мережева анонімність та таємність голосування.**

Для забезпечення мережевої анонімності використовується відомий мережевий анонізатор Tor, який забезпечує так звану цибулинну маршрутизацію. Клієнтське програмне забезпечення Tor маршрутизує Інтернет-трафік через всесвітню мережу добровільно встановлених серверів з метою приховування розташування користувача [27]. Окрім того, використання Tor робить складнішим відслідковування Інтернет - активності як на рівні веб - сайту, так і на рівні Інтернет - провайдера, включаючи «відвідування веб - сайтів, залишені повідомлення та коментарі на відповідних ресурсах, миттєві повідомлення та інші форми зв'язку», до користувача і 22  
призначений для захисту приватності користувача та можливості проведення конфіденційних операцій, приховуючи користувацьку активність в мережі від стороннього моніторингу.

«Цибулева маршрутизація» (англ. Onion Routing) відображає шарову природу шифрування даного сервісу: початкові дані шифруються та розшифровуються багато разів, потім передаються через наступні вузли Tor, кожен з яких розшифровує «шар» шифру перед передачею даних наступному вузлу і, зрештою, до місця призначення. Це зменшує можливість розшифрування оригінальних даних в процесі передачі.

Tor також надає анонімність серверам у формі сервісів з прихованим місцезнаходженням, які є Тор-клієнтами, чи вузлами, на яких виконується спеціально налаштоване серверне програмне забезпечення. Замість видачі IP-адреси сервера (а отже і його місцезнаходження в мережі), приховані сервіси доступні через притаманні Тор-мережі .onion псевдо-домени верхнього

рівня (TLD). Tor-мережа розуміє ці домени верхнього рівня і маршрутизує дані анонімно в та з прихованих сервісів. Використання Tor-клієнту необхідно для отримання доступу до прихованих сервісів. Так як приховані сервіси не використовують вихідні вузли, вони не чутливі до «прослуховувань вихідного вузла» (англ. exit node eavesdropping). Приховані сервіси можуть бути доступні без прямого підключення до мережі Tor через Tor2Web.

В нашому випадку прихований сервіс використовується не з метою приховування сервера голосування, а з метою його ідентифікації: використовуючи конкретну onion-адресу, клієнт може бути впевнений в тому, що спілкується з сервером, який має саме цю, адресу, та в тому, що трафік не може бути перехоплений та змінений зломисником (аналогічно https, але надійніше за рахунок виключення потенційно вразливої інфраструктури сертифікатів з процесу аутентифікації). Ще одною важливою перевагою розміщення сервера в мережі DarkNet є можливість його запуску на комп'ютері з будь-яким доступом до мережі Інтернет. Тобто такий сервер не потребує так званої «білої» статичної IP-адреси та буде доступний з будь-якої точки світу, навіть працюючи на вашому персональному комп'ютері, який знаходиться за декількома роутерами (офісним, організації та провайдера).

Маршрутизатор Tor має відкритий вихідний код. Ми використали бінарні файли, скомпільовані для інших продуктів (Tor-браузері для різних операційних систем). Ці статично лінковані бінарні файли Tor біли включені до складу нашого серверу голосування його (Windows та Linux версій), та до складу нашого клієнтського додатку (Windows та Android-версій). Розроблене нами програмне забезпечення запускає Tor у вигляді демона та взаємодіє з ним через tcp - сокет на localhost - інтерфейсі з використанням проху - протоколу SOCKS5.

### 2.3. Проблема первинної аутентифікації виборців.

Важливою на сьогодні постає проблема електронної ідентифікації громадян, що звертаються для отримання адміністративних послуг, в тому числі, є учасниками виборчого процесу [14]. Адже з урахуванням обраного Україною напрямку щодо європейської інтеграції, вбачається необхідним розвиток системи електронної ідентифікації (eID) шляхом імплементації норм Регламенту eIDAS (Electronic Identification and Signature – Положення Європейського Парламенту та Ради Європейського Союзу щодо електронної ідентифікації та послуг довіри для електронних транзакцій на внутрішньому ринку). За цим документом електронна ідентифікація фізичних і юридичних осіб відбувається шляхом видачі їм в установленому порядку і на основі встановленої схеми спеціальних персональних засобів електронної ідентифікації (електронних карток, паспортів та інших засобів, тобто електронних ідентифікаторів, пов'язаних з конкретною особою). Головною вимогою до eID є забезпечення технологічної можливості здійснення аутентифікації (підтвердження справжності) власника електронного ідентифікатора при виконанні ним будь-яких електронних транзакцій. Ці два аспекти є обов'язковими для надання електронних послуг та здійснення електронних транзакцій. Суб'єкти господарювання для eID використовують електронні цифрові ключі. Такий спосіб широко застосовується при поданні податкових та інших форм звітності, у банківській сфері. Якщо для суб'єкта господарювання-юридичної особи придбання електронного ключа та його підтримка в актуальному стані протягом року є більш-менш доступною послугою, то для фізичної особи-підприємця або для пересічного громадянина така послуга з огляду на її вартість та періодичність використання може бути не вигідною. За останньою версією Регламенту eIDAS, схваленою Європарламентом у березні 2014 року, ділові транзакції в мережі Інтернет повинні здійснюватися за допомогою апаратного чи програмного забезпечення, оснащеного необхідним стеком технологій для генерації єдиного пан-



європейського цифрового підпису. Для приватних осіб таким токеном (ключем) може бути національний електронний паспорт або смартфон. Для юридичних осіб – смарт-карти, USB- токени та інші пристрої. Усі пристрої для генерації цифрового підпису повинні проходити обов’язкову сертифікацію. Упровадження такого підходу в Україні можливе за умови подолання деяких проблем. Створення ЦНАПів за принципом «Єдиного вікна» суттєво підвищило ефективність роботи органів влади, оперативність у видачі довідок та дозволів, зменшило кількість необхідних візитів заявником до різних дозвільних установ. Але, не зважаючи на це, громадянин повинен як мінімум двічі особисто прибути до ЦНАПу – з метою надання заяви (ідентифікації своєї особи) на видачу довідки/дозволу та для отримання саме замовленої довідки/дозволу. Скорочення кількості візитів за рахунок електронної ідентифікації через мережу Інтернет при оформленні заяви на видачу довідки/дозволу є актуальним питанням при наданні електронних адміністративних послуг. У випадку заявників-юридичних осіб засобом eID можуть бути електронні цифрові ключі. З огляду на досвід Європи, для пересічних громадян або фізичних осіб-підприємців, в умовах відсутності національних електронних паспортів, eID токеном може бути звичайна банківська картка. Технологія підтвердження свого eID у такий спосіб дозволить громадянину при оформленні заяви в електронному вигляді надати підтвердження своїх персональних даних з використанням банківської картки через відповідні сервіси банку.

На жаль, система електронної ідентифікації громадян не забезпечує можливість 100-відсоткової персоналізації, що необхідно для використання її для проведення виборів державного масштабу. В нашій роботі ми використали альтернативний спосіб ідентифікації, що не є чисто електронним, але частково вирішує проблему без необхідності впровадження систем ідентифікації на державному рівні. Участь у виборах забезпечується паперовим запрошенням, яке може бути передане виборцю поштою чи кур’єром. Запрошення містить

конфіденційну інформацію та повинно бути захищене від стороннього доступу (передане у закритому конверті з елементами захисту). Для формування запрошення використовується QR-код, що насамперед зручно для користувача, адже його сканування не потребує спеціальних навичок чи технічних засобів.

QR-код (англ. quick response— швидкий відгук)— матричний код (двовимірний штрих-код), розроблений і представлений японською компанією «Denso-Wave» в 1994 році. Основна перевага QR-коду— це легке розпізнавання сканувальним обладнанням (в тому числі й фотокамерою мобільного телефона), що дає можливість використання в торгівлі, на виробництві, в логістиці.

На відміну від старого штрих-коду, який сканують тонким променем, QR-код визначається сенсором як двовимірне зображення. Три квадрати в кутах зображення та менші синхронізувальні квадратики по всьому коду дозволяють нормалізувати розмір зображення і його орієнтацію, а також кут, під яким сенсор розташований до поверхні зображення. Точки переводяться в двійкові числа з перевіркою контрольних сум.

Основна перевага QR-коду — це легке розпізнавання сканувальним обладнанням (в тому числі і фотокамерою мобільного телефону).

Хоча термін «QR code» є зареєстрованим товарним знаком «DENSO Corporation», використання кодів не обкладається ніякими ліцензійними відрахуваннями, а самі вони описані й опубліковані як стандарти ISO. Специфікація QR-коду не описує формат даних.

Найпопулярніші програми перегляду QR-кодів підтримують такі формати даних: URL, веб-сторінки, E-mail (з темою листа), SMS на номер (з темою), MeCard, vCard, географічні координати.

Також деякі програми можуть розпізнавати файли GIF, JPG, PNG або MID менше 4 КБ і зашифрований текст, але ці формати не отримали популярності.

QR-коди найрозповсюдженіші в Японії, країні, де штрих-коди користувалися такою великою популярністю, що обсяг інформації, зашифрованої в коді, швидко перестав влаштовувати індустрію. Японці почали експериментувати з новими способами кодування невеликих обсягів інформації в графічному зображенні. Вже на початку 2000 року вони набули широкого використання у Японії. Їх можна бачити на великій кількості плакатів, упаковок і товарів.

QR-код також вельми поширений у країнах Азії, Китаю, поступово розвивається в Європі та Північній Америці. Найбільше визнання він отримав серед користувачів мобільного зв'язку — встановивши програму - розпізнавач, абонент може миттєво заносити в свій телефон текстову інформацію, додавати контакти в адресну книгу, переходити по web-посиланнях, відправляти SMS-повідомлення тощо.

Провідні японські оператори мобільного зв'язку спільно випускають під своїм брендом мобільні телефони з вбудованою підтримкою розпізнавання QR-коду. Як показало дослідження, провідною компанією «comScore» 2011 року, 20 млн жителів США використовували мобільні телефони для сканування QR-кодів.

У Японії та Австрії QR-коди також використовуються на кладовищах (див. Віртуальне кладовище) та містять інформацію про померлого. Також, QR-коди активно використовують у туризмі. Наприклад, у Львові об'єднання бізнесменів «Туристичний Рух Львова» розмістило QR-коди на понад 80 туристичних об'єктах. Це дає змогу туристам легко орієнтуватися в місті, навіть не знаючи української мови, тому що QR-коди встановлені кількома мовами.

### РОЗДІЛ 3. КОМПЛЕКСНИЙ ПРОТОКОЛ ТАЄМНОГО ГОЛОСУВАННЯ, АДАПТОВАНИЙ ДО НАЦІОНАЛЬНИХ ВИБОРІВ ТА СУЧАСНИХ УМОВ ЇХ ПРОВЕДЕННЯ.

#### **3.1. Базові компоненти протоколу.**

Електронний цифровий підпис - інформація в електронній формі, яка приєднана до іншої інформації в електронній формі (інформації, що підписується) або іншим чином пов'язана з такою інформацією і яка використовується для визначення особи, яка підписує інформацію. За своєю суттю електронний підпис є реквізит електронного документа, що дозволяє встановити відсутність спотворення інформації в електронному документі з моменту формування електронного цифрового підпису та перевірити приналежність підпису власникові [29]. Електронний цифровий підпис призначений для аутентифікації особи, яка підписала електронний документ, і є повноцінною заміною власноручного підпису у випадках, передбачених законом. Використання електронного підпису дозволяє здійснити такі функції.

- Контроль цілісності переданого документа. При будь-якій випадковій або навмисній зміні документа підпис стане недійсним, тому що він був обчислений на підставі вихідного стану документа і відповідає лише йому.

- Захист від змін (підроблення) документа. Гарантія виявлення підробки при контролі цілісності робить підроблення недоцільним в більшості випадків.

- Неможливість відмови від авторства. Так як створити коректний підпис можна, лише знаючи закритий ключ, а він повинен бути відомий тільки власнику, власник не може відмовитися від свого підпису під документом.

- Доказове підтвердження авторства документа. Так як створити коректний підпис можна, лише знаючи закритий ключ, а він повинен бути відомий тільки власнику, власник пари ключів може довести своє авторство підпису під документом.

Залежно від деталей визначення документа можуть бути підписані такі поля, як «автор», «внесені зміни», «мітка часу» і т.д. Але крім «стандартних» функцій за допомогою електронного цифрового підпису можна виконувати і інші функції. В такому випадку схеми цифрового підпису називають схемами з додатковою функціональністю:

- незаперечний електронний цифровий підпис;
- електронний цифровий підпис з призначеним конфірмантом;
- електронний цифровий підпис наосліп;
- групова електронний цифровий підпис;
- електронний цифровий підпис з додатковим захистом.

В Україні юридично значущий сертифікат електронного цифрового підпису видає та засвідчує, наприклад, Приватбанк для своїх клієнтів. При використанні електронного цифрового підпису в електронному документообігові між кредитними організаціями та кредитними бюро активно стала розвиватися інфраструктура електронного документообігу між податковими органами і платниками податків. Завдяки електронному цифрового підпису, зокрема, багато українських компаній здійснюють свою торгово-закупівельну діяльність в Інтернеті, через системи електронної торгівлі, обмінюючись з контрагентами необхідними підписаними документами в електронному вигляді. Це значно спрощує і прискорює проведення конкурсних торгових процедур, особливо в умовах карантинних обмежень, пов'язаних з епідемією Covid-19.

Електронний цифровий підпис - це найбільш зручний сучасний інструмент для обміну юридично значимого електронного документацією і здійснення операцій у віддаленому режимі. Завдяки впровадженню механізму електронного підпису кордони економічних регіонів більше не є обмеженням для економічної діяльності. Перед підприємствами і організаціями з усіх країн та регіонів відкривається можливість вийти на федеральний і міжнародний рівень, вести закупівлю та збут товарів з мінімальними витратами, позбутися

від бюрократичної тяганини. Електронний підпис був створений для того, щоб зробити можливим обмін юридично значимими електронними документами і для вчинення інтерактивних угод. Механізм дії, за допомогою якого цифровий підпис забезпечує юридичну значимість електронного документа, відносно простий і дуже ефективний. По суті, електронний підпис є певною послідовністю символів, отриманою за рахунок перетворення вихідного документа спеціальним програмним забезпеченням ЕЦП. Електронний цифровий підпис може використовуватися в декількох іпостасях. сформовані умови застосування ЕЦП як підпису в документі, аналога власноручного підпису і печатки. Подібним чином ЕЦП використовується в системах електронного документообігу різного призначення (організаційно-розпорядчого, кадрового, законотворчого, торгово-промислового та іншого). Однак область застосування ЕЦП не обмежується наведеним прикладом. Сам по собі електронний цифровий підпис - чудовий механізм забезпечення цілісності і підтвердження авторства і актуальності будь-яких даних, представлених в електронному вигляді. Властивості ЕЦП дозволяють використовувати його з різною метою:

- декларування товарів і послуг (митні декларації);
- реєстрація угод по об'єктах нерухомості;
- використання в банківських системах;
- електронна торгівля і держзамовлення;
- контроль виконання державного бюджету;
- в системах звернення до органів влади;
- для обов'язкової звітності перед державними установами;
- організація юридично значущого електронного документообігу;
- в розрахункових і трейдингових системах.

Цифровий підпис може бути побудований на основі однієї з наведених нижче схем. Перша схема - алгоритми симетричного шифрування. Дана схема передбачає наявність у системі третьої особи - арбітра, що користується

довірою обох сторін. Авторизацією документа є сам факт шифрування його секретним ключем і передача його арбітру. Друга схема - алгоритми асиметричного шифрування. На даний момент такі схеми ЕЦП найбільш поширені і знаходять широке застосування. Звернемо увагу на другу схему і розглянемо алгоритми асиметричного шифрування докладніше. Асиметричні схеми ЕЦП відносяться до криптосистем з відкритим ключем. На відміну від асиметричних алгоритмів шифрування, в яких шифрування проводиться за допомогою відкритого ключа, а розшифрування - за допомогою закритого, в схемах цифрового підпису підписання проводиться із застосуванням закритого ключа, а перевірка - із застосуванням відкритого. Асиметричні схеми відрізняються від симетричних тим, що останні використовують один і той же ключ для шифрування інформації і для її розшифрування. Якщо зашифровану інформацію необхідно передавати в інше місце, то в цьому випадку треба передавати і ключ для розшифрування. Слабке місце тут - це канал передачі даних: якщо він не захищений або його прослуховують, то ключ для розшифрування може потрапити до злоумисника. Системи на асиметричних алгоритмах позбавлені цього недоліку, так як кожен учасник такої системи має пару ключів: відкритий і секретний. Всі асиметричні алгоритми цифрового підпису спираються на наступні обчислювальні проблеми:

- проблему дискретного логарифмування EGSA (Electrical Generating Systems Association).
- проблему факторизації, тобто розкладання числа на прості множники (RSA (літерна аббревіатура від прізвищ Rivest, Shamir і Adleman)).

Обчислення теж можуть проводитися двома способами: на базі математичного апарату еліптичних кривих і на базі полів Галуа (наприклад, DSA (Digital Signature Algorithm)). В даний час найшвидші алгоритми дискретного логарифмування і факторизації є субекспоненціальні. Належність самих проблем до класу NP-повних (від англ. Non-deterministic polynomial) не доведена.

Відомі такі асиметричні схеми:

1. FDH (Full Domain Hash), імовірнісна схема RSA-PSS (Probabilistic Signature Scheme), схеми стандарту PKCS # 1 і інші схеми, засновані на алгоритмі RSA.
2. Схема Ель-Гамала.
3. Американські стандарти електронного цифрового підпису: DSA, ECDSA (DSA на основі апарату еліптичних кривих).
4. Російські стандарти електронного цифрового підпису: ГОСТ Р 34.10-94 (в даний час не діє), ГОСТ Р 34.10-2001.
5. Схема Діффі-Лампорта.
6. Український стандарт електронного цифрового підпису ДСТУ 4145-2002.
7. Білоруський стандарт електронного цифрового підпису СТБ 1176.2-99.
8. Схема Шнорра.
9. Pointcheval-Stern signature algorithm.
10. Ймовірнісна схема підпису Рабіна.
11. Схема BLS (Boneh-Lynn-Shacham).
12. Схема GMR (Goldwasser-Micali-Rivest).

Схема №1, описана вище, базується на алгоритмі RSA. Тому стійкість і широке використання даного алгоритму - результат складності факторизації великих цілих чисел. Ці алгоритми можна застосовувати як для шифрування / розшифрування, так і для генерації / перевірки електронно-цифрового підпису.

Схема №2 - Схема Ель-Гамала. Вона лежить в основі стандартів електронного цифрового підпису в США і Росії (ГОСТ Р 34.11-94). Elgamal є криптосистемою з відкритим ключем, заснованою на труднощах обчислення дискретних логарифмів в кінцевому полі. На відміну від RSA, алгоритм Ель-Гамала не запатентований, тому став більш дешевою альтернативою, тому що не була потрібна оплата внесків за ліцензію. Вважається, що алгоритм потрапляє під дію патенту Деффи-Хеллмана.



Схема № 3 - Американські стандарти електронного цифрового підпису: DSA, ECDSA. При створенні проекту в 1991 році в США одним з основних критеріїв була його патентна чистота. Його надійність заснована на практичній нерозв'язності певного окремого випадку завдання обчислення дискретного логарифма. Довжина підпису в системі DSA менше, ніж в RSA. Одним з головних аргументів проти DSA є те, що, на відміну від загальної задачі обчислення дискретного логарифма, її окремий випадок, використаний у даній схемі, мало вивчений і, можливо, має істотно меншу складність розкриття. Недоліком DSA є те, що її функції обмежені тільки цифровим підписом, система принципово не призначена для шифрування даних. По швидкодії система DSA порівнянна з RSA при формуванні підпису, але істотно (в 10-40 разів) поступається їй при перевірці підпису. Є думка, що цей стандарт небезпечний, так як дозволяє імітувати підміну підпису, дозволяючи пересічному користувачеві вибрати свої секретний і відкритий ключі так, що підписи для двох відомих заздалегідь повідомлень співпадутъ. А це відкриває простір для різних махінацій з використанням ЕЦП.

33

Схема № 4 - нині не діючий стандарт ГОСТ Р 34.10-94. Схема ЕЦП, запропонована в даному стандарті, багато в чому нагадує підпис у DSA.

Схема № 5 - Діффі-Лампорта. Ця система проста у використанні, але у неї є, принаймні, два очевидні недоліки. По-перше, необхідна попередня передача параметрів перевірки. По-друге, що більш важливо, підпис сильно збільшує довжину повідомлення. Якщо в криптосистемі використовуються ключі довжиною, скажімо, 64 біта, то довжина підписаного повідомлення збільшиться в 64 рази.

Схема № 6 - Український стандарт ДСТУ 4145-2002. Алгоритм, заснований на еліптичних кривих. Відноситься до того ж класу, що і ECDSA.

Схема № 7 - Білоруський стандарт СТБ 1176.2-99 - базується на схемі ЕЦП Шнорра.

Схема № 8 - Стійкість схеми Шнорра ґрунтується на важкій задачі обчислення дискретних логарифмів. Даний алгоритм дозволяє проводити попередні обчислення, що зручно при малих обчислювальних ресурсах. Потрібно відзначити, що в протоколі передається тільки три повідомлення. Це було зроблено спеціально для зменшення взаємодії в мережах з низькою пропускнуою здатністю. При однаковому рівні безпеки довжина підписів для Schnorr коротше, ніж для RSA. Підписи Schnorr також набагато коротше за підписи ElGamal.

Схема № 9 - Pointcheval-Stern signature algorithm, базується на схемі підпису ElGamal.

Схема № 10 - імовірнісна схема підпису Рабина. Ця схема є модифікацією функцій RSA за допомогою рандомізованого заповнення.

#### **Схеми підписи з доказовою стійкістю:**

Схема № 11 - схема BLS (Boneh-Lynn-Shacham). Вона є найбільш короткою відомої схемою ЕЦП. Дана схема використовує еліптичні криві, але вона обмежена групами, в яких є функція складання пари.

Схема № 12 - Схема GMR (Goldwasser-Micali-Rivest). Запропоновано в 1984 році Шафи Гольдвассер, Сільвіо Мікалі і Рональдом Рівестом.

У деяких спеціальних інформаційних технологіях, наприклад, в системах електронних грошей, одним з важливих вимог є забезпечення невідслідковуваності (анонімності) користувачів. Для вирішення цього завдання був запропонований механізм формування ЕЦП «наосліп», що реалізується за допомогою протоколів сліпого підпису. У протоколах даного типу беруть участь два суб'єкти:

- 1) клієнт, який формує електронний документ і хто хоче отримати справжній підпис іншої особи до цього документа, і
- 2) підписант, що обчислює деякі параметри (елементи сліпого підпису) і передає їх значення клієнту, а потім останній обчислює справжню ЕЦП. Перевірка справжності підпису, отриманого клієнтом, здійснюється за тим же

алгоритмом, як і перевірка звичайного підпису. При цьому за даними, використаним в ході протоколу сліпого підпису, клієнт не може отримати інформацію про особистий секретний ключ підписанта, а підписант не може однозначно встановити зв'язок деякого виконаного протоколу сліпого підпису з деяким електронним документом і доданою до нього справжнім ЕЦП (передбачається, що підписант багаторазово виконував підписування документів «наосліп»). Останній момент називається вимогою забезпечення невідслідковуваності користувачів, яка пред'являється до протоколів сліпого підпису. Перший протокол сліпого ЕЦП був реалізований на основі схеми підпису RSA, заснованого на обчислювальній складності задачі факторизації. Надалі були розроблені протоколи сліпих ЕЦП, засновані на обчислювальній складності диференційного логарифмування. В обох випадках анонімність клієнта забезпечується механізмом внесення в сліпий підпис одного або двох випадкових засліплюючих множників. Після отримання сліпого підпису від підписанта клієнт видаляє засліплюючі множники, в результаті чого отримує справжній підпис. Протоколи сліпого підпису можуть бути реалізовані на основі ряду відомих схем ЕЦП, наприклад, на основі RSA , схеми Шнорра, BLS, ГОСТ Р 34.10-94 і ГОСТ Р 34.10-2001.

### **Сліпий підпис [29].**

Припустимо, що Аліса - директор, а Боб - секретар. Боб хоче подати документ на підпис Алісі так, щоб вона не дізналася нічого про вміст документа; при цьому потрібно, щоб Боб не зміг підробити підпис Аліси (В криптографічних термінах, не отримав її секретного ключа). Протокол обміну повідомленнями між Алісою і Бобом, в результаті якого Боб отримає підпис Аліси на потрібному йому документі, а Аліса не дізнається, що вона підписала, називається протоколом сліпого підпису. Підпис – це щось, що посвідчує документ. Він не вбудовується в документ, а прикріплюється до нього. Підпис залежить і від людини, яка підписала документ, і від вмісту документа, що підписаний. Підпис задається незмінним для нього алгоритмом (параметрами

якого є текст документа та приватний ключ людини, що підписує) [33]. При необхідності підпис можна перевірити:

1. що підпис належить саме тій людині, яка про це заявляє;
2. що підпис був поставлений саме на цей документ (що в документ не були внесені зміни або ні підкладений інший документ).

Найпростіша фізична реалізація сліпого підпису така: в конверт з документом ми кладемо копірку, людина розписується на конверті, завдяки копірці (яку ми після цього виймаємо) підпис з'являється на документі. Протоколи сліпого підпису були розроблені близько 20 років тому. Вони засновані на різних математичних алгоритмах: гомоморфному шифруванні з використанням дискретних логарифмів (в тім числі виконаних на еліптичних кривих), білінійному спарюванні на спеціальних еліптичних кривих та ін.

### **3.2. Етапи таємного голосування.**

Протоколи таємного голосування ґрунтуються на широко відомих і перевірених алгоритмах шифрування, хешування, цифрового підпису [35]. Але для втілення їх в життя необхідно врахувати безліч вимог і чинників. Реалізація будь-якої вимоги, що пред'являється до даних протоколів, може стати хорошим завданням для подальшого дослідження.

#### **Ми дещо модифікували оригінальний протокол He-Su:**

- виключили забезпечення непідтвердженості голосу. В запропонованому нами варіанті протоколу забезпечується можливість перевірки факту врахування свого конкретного голосу кожним учасником голосування. Таким чином, повністю виключається можливість прямого шахрайства з боку рахівника.

- виключили можливість переголосування до моменту розкриття голосу. Ця можливість в деякій мірі перешкоджала продажі голосу (виборець міг змінити «проданий» голос). В нашому випадку натомість забезпечується можливість надати учасником голосування беззаперечні докази шахрайства з

боку рахівника (самовільної зміни його голосу при підрахунку), що на наш погляд, більш важливо з урахуванням особливостей моделі загроз щодо виборів в Україні.

Для реалізації протоколу таємного голосування ми використали сучасні криптографічні примітиви, стійкість яких формально доведена авторами в фахових публікаціях.

Для забезпечення персональної аутентифікації з використанням паролю був використаний протокол SPEKE (аналог відомого криптографічного протоколу соціаліста-мільйонера). Цей протокол має нульове розголошення паролю, що запобігає можливості підбору паролю методом перебору без активного підключення до сервера, використовуючи лише інформацію, отриману з декількох спроб аутентифікації. Таким чином, для перевірки кожного можливого паролю потрібна повна процедура мережевої взаємодії з сервером, що дуже ускладнює процес підбору. Таким чином, мається можливість безпечно використовувати навіть короткі паролі (наприклад, PIN-коди). Даний протокол реалізований на еліптичній кривій X25519, що забезпечує близько 128 біт захисту. Необхідне для протоколу хешування на еліптичну криву реалізоване з використанням алгоритму Elligator2, що гарантує відсутність витоку біту інформації про пароль через дані про належність точки кривій чи її твісту. Фактично даний протокол реалізує Diffie-Hellman обмін сесійними ключами з особливістю: у якості базової точки використовується не стандартна загальновідома точка  $G$ , а точка, що являється результатом хешування пароля на еліптичну криву.

Реалізація сліпого підпису виконана на основі BLS-підпису. Цей підпис перевіряється методом білінійного спарювання (в нашому випадку це АТЕ-спарювання) на спеціальній еліптичній кривій BN254. З урахуванням атак, відкритих в останні роки, ця еліптична крива забезпечує близько 100 біт захисту, що достатньо з урахуванням обмеженого тривання виборів та стану

обчислювальних потужностей, доступних сьогодні (принаймні до створення квантового комп'ютера).

Симетричне аутентифіковане шифрування реалізоване з використанням алгоритму Кессак-800, що працює у Duplex-режимі та використовує доповнення, стандартизовані для сімейства функцій з розширюванням виходу Shake (частина стандарту хеш - функції SHA3, яка рекомендована NIST для заміни застарілих хеш - функцій сімейства SHA). Ця ж функція використовується для хешування, аутентифікації (MAC) та в послідовному циклі для обробки паролів (PKDF).

В якості генератора псевдовипадкових чисел використовується генератор з використанням цього ж перетворення Кессак-800 за алгоритмом, рекомендованим авторами Кессак. Для ініціалізації генератора використовується ентропія, отримана за допомогою системних викликів та додатково за допомогою алгоритму HAVEGE, який отримує ентропію за рахунок неоднозначної взаємодії різних потоків у мультизадачних операційних системах, за рахунок чого час виконання заданого коду буде дещо різнитися.

38

На рівні протоколу процедура голосування за запропонованим нами протоколом має такі етапи:

1. Підготовка персональної бази даних виборців. В цю базу додаються всі допущені до голосування виборці: їх прізвища та ідентифікаційні коди (в якості унікального ідентифікатора). Також кожному виборцю надається персональний пароль, який саме забезпечує доступ до виборів. Для кожного користувача формується запрошення у вигляді QR-коду, що містить порядковий номер виборця у базі даних, його персональний пароль та веб - адресу сервера, що буде забезпечувати вибори. Даний QR-код містить конфіденційну інформацію (фактично є самодостатньою «перепусткою» на вибори), тому повинен бути вручений виборцю особисто у світлонепроникному конверті (по аналогії з PIN-кодом банківської карти).

2. Сервер публікує загальну інформацію про виборців на веб - сторінці, яка доступна виборцям та волонтерам. Доступ до сервера забезпечується анонімізатором Tor, який при першому старті генерує onion-адресу сервера.

Для забезпечення мережевої анонімності веб - сторінки та інтерфейсу протоколу голосування сервера доступний в мережі DarkNet з використанням анонімізатора Tor у складі клієнтського додатку для голосування або Tor-браузера для перегляду веб - сторінки сервера. Альтернативою для доступу до веб - сторінки є використання шлюзів, що забезпечують доступ до DarkNet зі звичайного браузера. Також при першому старті сервера створюються ключі реєстратора та рахівника, що залишаються незмінними на протязі виборів.

3. Учасники виборів встановлюють клієнтський додаток, що забезпечують всі кроки процедури голосування. Нами розроблені додатки для операційних систем Windows та Android. В момент першого старту після встановлення додаток генерує індивідуальний ключ клієнта, який буде в подальшому використовуватися на всіх етапах виборів та не може бути змінений. Наступним кроком є сканування QR-коду отриманого запрошення, в якому містяться персональні данні учасника голосування (його порядковий номер у списку та пароль), а також веб - адреса сервера в DarkNet (так звана onion-адреса).

4. Далі клієнт анонімно підключається до сервера, використовуючи відому йому з запрошення onion-адресу, та отримує публічні ключі реєстратора та рахівника. Анонімність клієнта виключає можливість надання окремим клієнтам (які передбачувано невігідні організаторам голосування) різних ключів за метою подальшого шахрайства. Onion-маршрутизація, що забезпечується анонімізатором Tor, гарантує доступ саме до сервера, onion-адреса якого (фактично це є хеш від публічного ключа Tor на боці сервера) вказана в QR-коді запрошення. Захищений канал зв'язку, що формується Tor, запобігає спотворенню інформації активним зловмисником. Після отримання

публічних ключів реєстратора та рахівника клієнт може перевіряти їх підписи та буде готовий до наступних етапів голосування.

5. Етап персональної реєстрації триває деякий час (декілька тижнів) перед днем виборів. Він не потребує мережевої анонімності. Клієнт вказує свій номер в базі даних та аутентифікує себе на сервері з використанням паролю, вказаного в QR-коді запрошення. Протокол пароліної аутентифікації, що використовується в запропонованому нами програмному забезпеченні – SPEKE, що гарантує підвищену стійкість навіть коротких паролів. У нашому випадку використовуються паролі, що містять 15 символів з набору base64, що еквівалентно 75-бітному паролю. Цього достатньо для забезпечення високого ступеню захисту аутентифікації клієнта, враховуючи, що пароль потрібен лише для первинної реєстрації клієнта та в подальшому більше не використовується та може бути розголошений. Після аутентифікації клієнт на основі свого публічного ключа та згенерованого випадкового «осліплювача» створює код та надсилає його Реєстратору. Реєстратор перевіряє, що даний клієнт раніше не реєструвався, накладає на отриманий код сліпий підпис та робить в базі даних відмітку, що цей клієнт був зареєстрований. При спробах повторної реєстрації клієнту буде завжди надаватися підпис, зроблений Реєстратором при першій реєстрації. Клієнт, отримавши від сервера сліпий підпис, знімає з нього осліплення, знову використовуючи запам'ятоване число, що було використане раніше для осліплення. В результаті клієнт фактично отримує підпис Реєстратором свого публічного ключа. При цьому сам публічний ключ залишається невідомим Реєстратору, і Реєстратор не може зіпівставити цей ключ з персональними даними клієнта. Таким чином, клієнт в подальшому може використовувати свій публічний ключ у якості псевдоніма, а підпис Реєстратора засвідчуватиме легітимність клієнта та гарантуватиме, що кожен клієнт має тільки один псевдонім. Кожен клієнт та волонтери можуть бачити персональний список виборців з відміткою про реєстрацію. Таким чином, на момент закінчення реєстрації відома кількість виборців, що зареєструвалися.



Природно, що кількість виборців, що проголосували на момент закінчення виборів, не повинна бути більшою від кількості зареєстрованих виборців.

6. Етап саме виборів звичайно відбувається у день виборів. Для доступу до сервера (а саме рахівника) використовується анонімне з'єднання через мережу DarkNet. Важливо перезапустити клієнтський додаток для зміни мережевої ідентичності та почекати деякий час після персональної реєстрації. Це запобігає проведенню деанонізації клієнтів шляхом кореляційної атаки, порівнюючи моменти персональної реєстрації та голосування. Відокремлення процедури реєстрації (перед виборами) від процедури голосування (у день виборів) забезпечує цю вимогу. Єдиним недоліком такого рознесення в часі є необхідність зберігати додаток для голосування на пристрої, адже втрата чи пошкодження пристрою та перевстановлення додатку призведе до генерації нового ключа клієнта, але повторна персональна реєстрація цього ж клієнта буде неможлива.

При голосуванні клієнт спершу надсилає Рахівнику свій публічний ключ та підпис Реєстратора. Рахівник перевіряє підпис, впевнюючись, що це легітимний клієнт. Також Рахівник перевіряє відсутність цього ключа в своїй базі даних та впевнюється, що даний клієнт ще не отримувал бюлетень. Перевіривши вказані умови, Рахівник надсилає клієнту бюлетень з вказаними прізвищами кандидатів. Цей бюлетень Рахівник підписує, що дає можливість клієнту довести факт видачі бюлетеню у випадку підозри на шахрайство з боку Рахівника.

Клієнт заповнює бюлетень (робить відмітку про свій вибір) та шифрує цю інформацію випадковим ключем, який зберігає до моменту відкриття голосу. Клієнт підписує зашифрований бюлетень своїм ключем та надсилає назад Рахівнику.

Рахівник за номером бюлетеня визначає псевдонім (публічний ключ) учасника голосування та перевіряє його підпис. Далі Рахівник зберігає зашифрований бюлетень в базі даних та надає клієнту квитанцію: свій підпис

отриманого зашифрованого бюлетеня. Ця квитанція зберігається клієнтом та може бути використана ним в подальшому при підозрі шахрайства з боку Рахівника.

7. Етап розкриття голосу звичайно розпочинається на наступний день після виборів та триває декілька днів. На цьому етапі кожен учасник виборів, що проголосував, надсилає рахівнику номер свого бюлетеня та ключ шифрування, що був використаний для приховування свого голосу. Рахівник знаходить в базі даних вказаний бюлетень, розшифровує інформацію про вибір клієнта та перевіряє контрольну суму (MAC). Рахівник вносить відкритий голос клієнта у базу даних та надсилає клієнту квитанцію (електронний підпис) з відкритим голосом, підтверджуючи, що голос врахований. Ця квитанція зберігається клієнтом та може бути використана ним в подальшому при підозрі на шахрайство з боку Рахівника.

На етапах голосування та розкриття голосів Рахівник забезпечує доступ до бази даних бюлетенів: номера виданого бюлетеня, відмітки про прийняття голосу та його розкриття з вказуванням вибору клієнта. Таким чином, клієнт за номером свого бюлетеня може перевірити його стан, що відображується, контролюючи дії Рахівника. У випадку шахрайства клієнт використовує отримані від Рахівника квитанції з його електронними підписами як докази, що є основою для анулювання результатів виборів з вини Рахівника. Волонтери можуть контролювати загальну статистику бюлетенів, а саме:

- кількість виданих реєстратором бюлетенів повинна бути не більша, ніж кількість зареєстрованих учасників виборів;
- кількість прийнятих бюлетенів повинна бути не більша від кількості виданих;
- кількість відкритих (врахованих) бюлетенів повинна бути не більша, ніж кількість прийнятих.

Крім того, волонтери можуть відслідковувати активність персональної реєстрації: масові дії в останні моменти реєстрації можуть свідчити про

фальсифікації (наприклад, використання так званих «мертвих душ»), що є приводом для вибіркового добровільного опитування таких виборців з метою виявлення фальсифікацій з боку реєстратора.

Формальний опис запропонованого нами протоколу таємного голосування наведено в табл. 1.



**Таблиця 1. Формальний опис запропонованого протоколу таємного голосування, розробленого на базі протоколів SPEKE та He-Su.**

| <p><i>Functions:</i></p> <p><b>H</b> is general hash-function Shake-128 based on Keccak-800 permutation</p> <p><b>H2P</b> is HashToPoint function for BN254 curve (ecfp group)</p> <p><b>Elligator</b> is HashToPoint function for X25519 curve</p> <p><b>SIGN<sub>c</sub>(M)</b> – signing message M (BN254 ecfp point in compressed format) using private key c</p> <p><b>VERIFY<sub>cc</sub>(M, SM)</b> – verifying signature SG of message M (both BN254 ecfp point in compressed format) with public key CC (BN254 ecfp2 point)</p> <p><b>BLIND<sub>f</sub>(M)</b> – blinding message M (BN254 ecfp point in compressed format) with BN254 field value f[32]</p> <p><b>UNBLIND<sub>f,R</sub>(BS)</b> – unblind blind signature BS (BN254 ecfp point in compressed format) with BN254 field value f[32] and signer's public key R (BN254 ecfp point in compressed format)</p> <p><i>Long-term keys:</i></p> <p><b>r[32], v[32], c[32]</b> are Registrator's, Voter's and Counter's private keys as random in field of BN254 curve.</p> <p><b>RR[128], VV[128], CC[128]</b> are corresponds public keys in ecfp group in uncompressed format.</p> <p><b>R[32]</b> is registrator's public key in ecfp group (compressed format).</p> <p><i>Registrator's Database (DB) fields:</i></p> <p><b>ID[4]</b> key autoincrement field is user's number as integer;</p> <p><b>FIO[64]</b> is user's not null name as Windows1251 encoded string</p> <p><b>INN[16]</b> is unique not null federal authenticator of person as string with 8-15 numbers</p> <p><b>PSW[16]</b> is password as string with 1-15 base64 chars</p> <p><b>SS[16]</b> is binary hashed SPEKE shared secret</p> <p><b>BS[32]</b> is blind signature (as BN254 ecfp point in compressed format)</p> <p><i>Counter's DB fields:</i></p> <p><b>N[4]</b> is key autoincrement ballot's number</p> <p><b>K[16]</b> is unique binary user's key</p> <p><b>E[16]</b> is binary encrypted vote</p> <p><b>M[16]</b> is binary checksum (MAC)</p> <p><b>D[16]</b> is decrypted vote as string up to 15 chars</p> <p><i>Counter's general data:</i></p> <p><b>LL[12][16]</b> is list of up to 12 names of candidates maximum 16 chars each (in Windows 1251 encoding).</p> <p><b>RS[32]</b> is Counter's signature of Registrator's public key (as BN254 BN254 ecfp point in compressed format).</p> <p><i>Other values:</i></p> <p><b>P[32]</b> is X25519 point as base in SPEKE key exchange (derived from password).</p> <p><b>x[32], X[32]; y[32], Y[32]</b> is session keypairs of voter and registrator used in SPEKE key exchange. Public keys computes using P[32] as base point.</p> <p><b>SS[16]</b> is hashes shared secret of SPEKE key exchange Diffie-Hellmann protocol.</p> <p><b>M[16]</b> is MAC checksum computed with H hash function</p> <p><b>f[32]</b> is random value in BN254 field, generate by voter for blinding.</p> <p><b>K[16]</b> is hash of voter's public key.</p> <p><b>KK[32]</b> is point on BN254 ecfp group (in compressed format) as HashToPoint of K value</p> <p><b>B[32]</b> is KK point blinded using f value (BN254 ecfp point in compressed format)</p> <p><b>BS[32]</b> is registrator's blind signature of KK value (BN254 ecfp point in compressed format)</p> <p><b>KS[32]</b> is unblinded BS value: in fact this is registrator's signature of KK value (BN254 ecfp point in compressed format)</p> <p><b>z[16]</b> is symmetric key for encryption / decryption of vote</p> <p><b>T[32]</b> is tickets: in fact this is Counter's signature of received data (BN254 ecfp point in compressed format).</p> |  |   |
|---|--|---|
| Registrator   | Voter  | Counter   |
| <p>Startup:</p> <p>have Counter's public key CC[128]</p> <p>have DB of voters:</p> <p>ID[4], FIO[64], INN[16], PSW[16], SS[16], BS[32]</p> <p>generate BN254 keypair: r[32], R[32], RR[128]</p>   | <p>Startup:</p> <p>Have server's onion address, ID[4], PASW[16] (from QR-code invite)</p> <p>generate BN254 keypair: v[32], VV[32]</p> | <p>Startup:</p> <p>have Registrators public key RR[128]</p> <p>have DB of ballots:</p> <p>N[4], K[16], E[16], M[16], D[16]</p> <p>have list of candidates LL[12][16]</p> <p>generate BN254 keypair c[32], CC[128]</p> <p>compute RS[32]=SIGN<sub>c</sub>(RR);</p> |
|   | <p>Keys request</p> <p>Connect to Counter over DarkNet (Tor authenticated link)</p> <p>using onion-adress from invite so we</p>        |   |

|  |   |  |
|--|---|--|
|  | can trust received public keys.<br><b>Keys request --&gt;</b>   |  |
|  |   | Keys presentation:<br><b>&lt;--CC[128], RS[32]</b> |
|  | Keys store:<br>save CC[128], RS[32]   |  |
|  | Identification:<br>Connect to Registrar over DarkNet<br>P[32]=Elligator(H(PSW[128]))<br>generate x[32] at random, save<br>compute X[32]=x*P<br><b>&lt;--ID[4], X[32]</b>  |  |
| Identification:<br>generate y[32] at random<br>compute SS[16]=H(y*X), save to DB<br>by ID<br>extract PSW from DB by ID<br>compute P[32]=Elligator(H(PSW))<br>compute Y[32]=y*P<br><b>Y[32], RR[128] --&gt;</b>   |   |  |
|  | Identification<br>VERIFY <sub>CC</sub> (RR, RS), abort on fail<br>save RR[128]  |  |
|  | Registration:<br>compute SS[16]=H(Y*x), save SS<br>compute K[16]=H(VV[128]), save K<br>compute KK[32]=H2P(K)<br>generate f[32] at random, save<br>B[32]=BLIND <sub>f</sub> (K);<br>M[16]=H(SS[16]  ID[4]  B[32])<br><b>&lt;-- ID[4], B[32], M[16]</b> |  |
| Registration:<br>Extract SS[16] from DB by ID, if<br>abort not exist<br>Check<br>M[16]?=H(SS[16]  ID[4]  B[32]);<br>abort fail<br>Try extract BS[32] from DB by ID,<br>skip next calculation on exist:<br>{<br>BS[32]=SIGN <sub>r</sub> (B);<br>Save BS[32] to DB by ID<br>}<br><br>Extract SS[16] from DB by ID<br>M[16]=H(ID[4]   BS[32]   R[32]  <br>SS[16] )<br><b>ID[4],BS[32],R[32],M[16] --&gt;</b> |   |  |
|  | Registration:<br>load SS[16]<br>check M[16]?=H(ID[4]   BS[32]  <br>R[32]   SS[16] ), repeat on fail<br>KS[32]=UNBLIND <sub>f,R</sub> (BS)<br>compute KK[32]=H2P(K[16])<br>VERIFY <sub>RR</sub> (KK,KS), repeat fail<br>save KS[32]                    |  |
|  | Request ballot:<br>Connect to Counter over DarkNet<br><b>K[16], KS[32] --&gt;</b>   |  |
|  |   | Issue ballot:                                      |

|  |   |  |
|--|---|--|
|  |   | search in DB by K[16],<br>skip on exist:<br>{<br>KK[32]=H2P(K)<br>VERIFY <sub>RR</sub> (KK,KS), abort fail<br>save K[16] to end of DB as new<br>entry<br>get N[4] of this entry<br>}<br><br>T[32]=SIGN <sub>v</sub> (Step[4]   N[4]  <br>L[12][16]   K[16])<br><-- N[4], LL[12][16], K[16], T[32]                              |
|  | Receive ballot:<br>VERIFY <sub>VV</sub> ( (Step[4]   N[4]  <br>LL[12][16]   K[16], T[32]), repeat on<br>fail<br>save N[4], LL[12][16], T[32]  |  |
|  | Send vote:<br>select candidate D[16] from list<br>LL[12][16]<br>generate z[16] at random, save<br>encrypt and authenticate:<br>E[16], M[16]=ENK <sub>z</sub> (D[16])<br>VS[32]=SIGN <sub>v</sub> (N[4]   Step[4]   E[16]<br>  M[16])<br><b>N[4], Step[4], E[16], M[16], VS[32],<br/> VV[128] --&gt;</b> |  |
|  |   | Process vote:<br>get K[16] from DB by N<br>check K[16] ?= H(VV[128]), abort<br>on fail<br>VERIFY <sub>VV</sub> (N[4]   Step[4]   E[16]  <br>M[16]), VS[32]), abort on fail.<br>save E[16], M[16] to DB by N<br>T[32]=SIGN <sub>c</sub> (N[4]   Step[4]   E[16]  <br>M[16])<br><-- N[4], Step[4], E[16], M[16],<br><b>T[32]</b> |
|  | Check is vote accepted:<br>VERIFY <sub>CC</sub> ((N[4]   Step[4]   E[16]  <br>M[16]), T[32]), repeat on fail<br>save T[32]  |  |
|  | Open vote:<br><b>N[4], z[16] --&gt;</b>   |  |
|  |   | Open vote:<br>Extract E[16], M[16] from DB by ID<br>D[16]=DEC <sub>z</sub> (E[16], M[16]), abort on<br>fail<br>save D[16] to DB by N<br>T[32]=SIGN <sub>c</sub> (step[4], N[4], D[16])<br><-- <b>N[4], D[16], T[32]</b>  |
|  | Check is vote opened:<br>VERIFY <sub>CC</sub> ((step[4], N[4], D[16]),<br>T[32]), repeat on fail<br>save D[16]  |  |

### **3.3. Реалізація клієнт-серверного програмного забезпечення для таємного голосування.**

При розробці програмного забезпечення для таємного голосування використовувалися підходи, притаманні криптографічному коду. Так, сервер реалізований в одному потоці, що запобігає будь-якому конкурентному доступу до криптографічних примітивів. Динамічне виділення пам'яті в реалізації крипто примітивів також не використовується. Поля даних у транспортних пакетах фіксовані та не можуть довільно інтерпретуватися залежно від їх вмісту, що запобігає атакам, пов'язаним з невірною серелізацією. Вихідний код не має зовнішніх залежностей від сторонніх бібліотек (в тім числі криптографічних) – весь необхідний функціонал включений у проект лише у вигляді вихідних кодів. При написанні С-коду використовувалася сумісність з стандартом ANSI C та зведений до мінімуму виклик системних функцій – майже всі необхідні алгоритми реалізовані у вигляді функцій - хелперів у вихідному коді. Це значно полегшує криптографічний аналіз такого коду на предмет можливих випадкових чи спеціально вкладених вразливостей. Данні в кеші знищуються в кожній функції. Час виконання криптографічних перетворень не залежить від їх аргументів, що запобігає таймінг-атакам.

#### **Компонентами програмного забезпечення є:**

1. Кросплатформенний сервер у вигляді консольного додатку для ОС Windows та Linux. Сервер включає анонізатор Tor для забезпечення анонімного доступу до веб-інтерфейсу через мережу DarkNet.
2. Графічний додаток для роботи з базою даних виборців для ОС Windows.
3. Кросплатформенний клієнтський додаток для голосування (ОС Windows та Android). Додаток містить вбудований анонізатор Tor для забезпечення мережевої анонімності та доступу до сервера через DarkNet.



---

Повний програмний код усіх компонентів програмного забезпечення доступний у персональному GitHub -репозиторії розробника за посиланням: <https://github.com/vikanmtu>

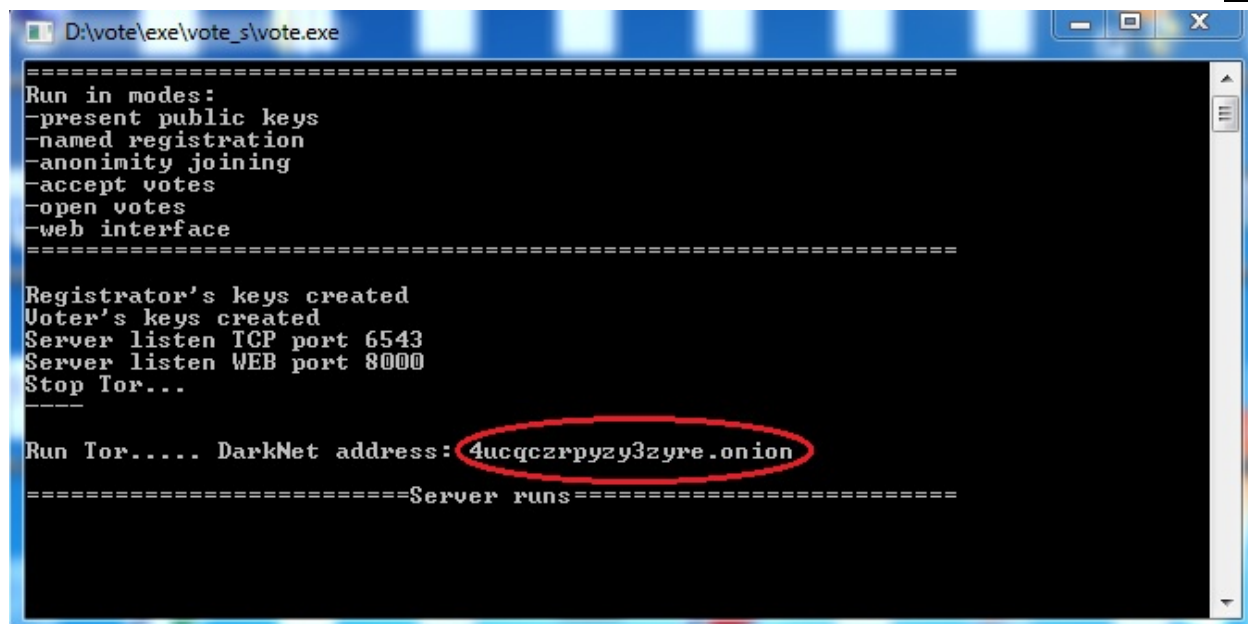
---

## I. Налаштування сервера

1. Завантажте архів з файлами сервера за посиланням: [http://torfone.org/download/vote\\_demo.zip](http://torfone.org/download/vote_demo.zip)

2. Розархівуйте папку `vote_s` на жорсткий диск вашого комп'ютера з будь-якою версією Windows (від XP 32bit до Win10 64 bit). Уникайте надто довгих шляхів та таких, що містять символи кирилиці або пробіли.

3. Зайдіть у папку та запустіть виконуючий файл сервера `vote.exe`. Буде відкрите консольне вікно сервера (рис.1), а через декілька секунд – ще одне консольне вікно анонімізатора Tor (рис.2). Дочекайтеся 100% підключення Tor до мережі. У випадку першого запуску це може зайняти до 10 хвилин. При наступних запусках підключення відбувається значно швидше (близько 1 хв.).



```
=====  
Run in modes:  
-present public keys  
-named registration  
-anonymity joining  
-accept votes  
-open votes  
-web interface  
=====
```

```
Registrator's keys created  
Voter's keys created  
Server listen TCP port 6543  
Server listen WEB port 8000  
Stop Tor...  
=====
```

```
Run Tor..... DarkNet address: 4ucqczrpyzy3zyre.onion  
=====Server runs=====
```

Рис.1. Консольне вікно сервера. Червоним виділена onion-адреса сервера, автоматично згенерована при першому старті.

Рис.2. Консольне вікно анонізатора Tor. Виділене повідомлення про стан підключення Tor до мережі Інтернет.

3. Після повного завантаження Tor тимчасово закрийте вікна сервера та Tor на час роботи з базою даних виборців (адже сервер блокує сторонній доступ до бази даних на час своєї роботи з міркувань безпеки). Запустіть графічну утиліту роботи з базою даних *manager.exe*

4. Перш за все вкажіть шлях до файлу бази даних сервера (*vote\_s/reg\_data/reg.db3*), натиснувши кнопку <...> у верхньому правому кутку форми додатку (рис.3). Відкрийте базу, натиснувши на кнопку <OpenDB>. При успішному відкритті колір поля з шляхом до файлу бази даних стане зеленим. Кодова таблиця бази даних – windows1251.

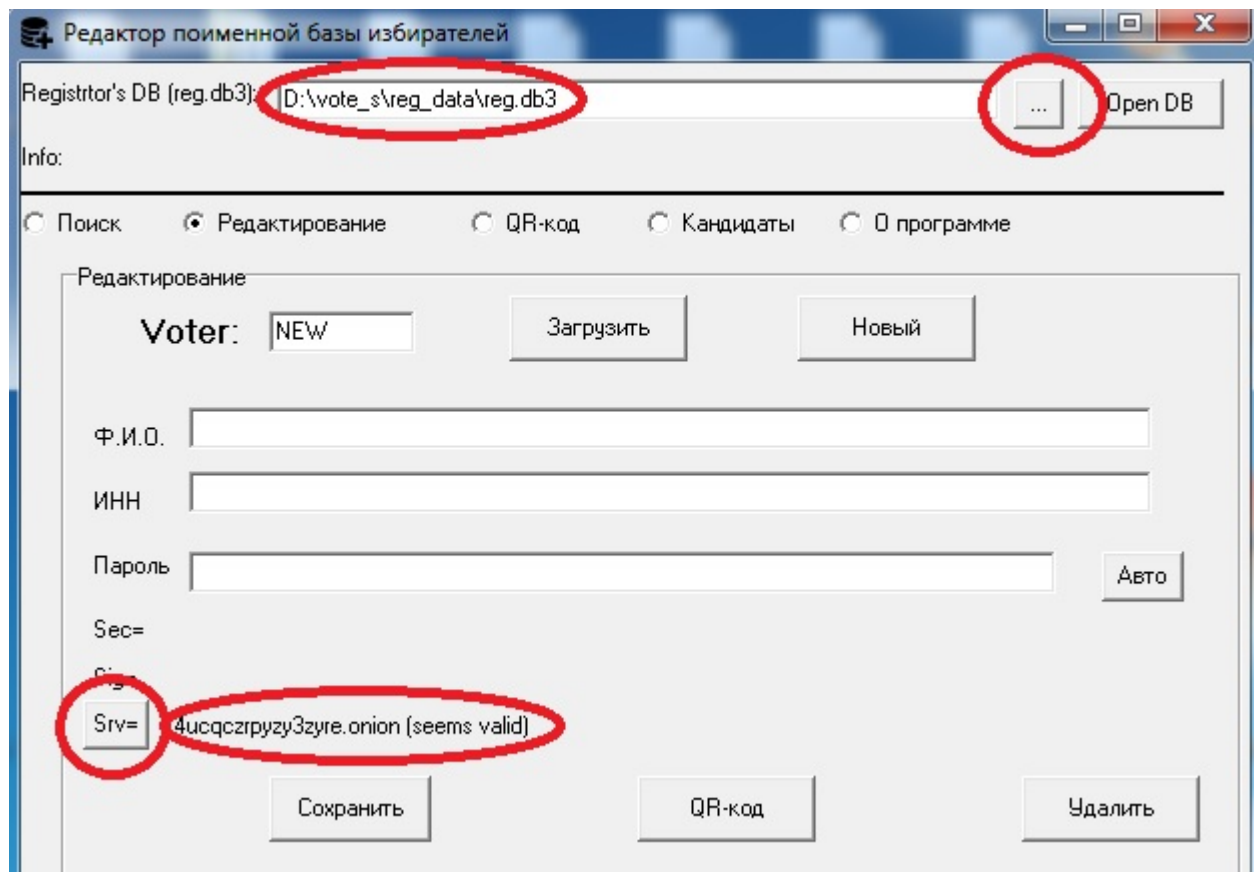


Рис.3. Додаток для роботи с базой даних. Кнопка <...> у верхньому правому кутку потрібна для вибору шляху до файлу бази даних. Кнопка <Srv=> у нижньому лівому кутку потрібна для вибору шляху до файлу з onion-адресою сервера (згенерованою Tor при першому старті).

51

5. За допомогою кнопки <Srv=> у нижньому лівому кутку форми виберіть шлях до файлу з onion-адресою сервера: *vote\_s/tor/hidden\_service/hostname*, згенерованою Tor при першому старті. Відповідна адреса буде відображена справа від кнопки.

6. Перейдіть на вкладку **‘Кандидаты’** та вкажіть шлях до файлу зі списком кандидатів (*vote\_s/vot\_data/vot.txt*), за яких будуть голосувати виборці (рис.4). Додайте від 2 до 12 прізвищ кандидатів до списку та натисніть кнопку **‘Сохранить’** для збереження списку у файлі. Можна використовувати латиницю та кирилицю, кодова таблиця файлу – windows1251.

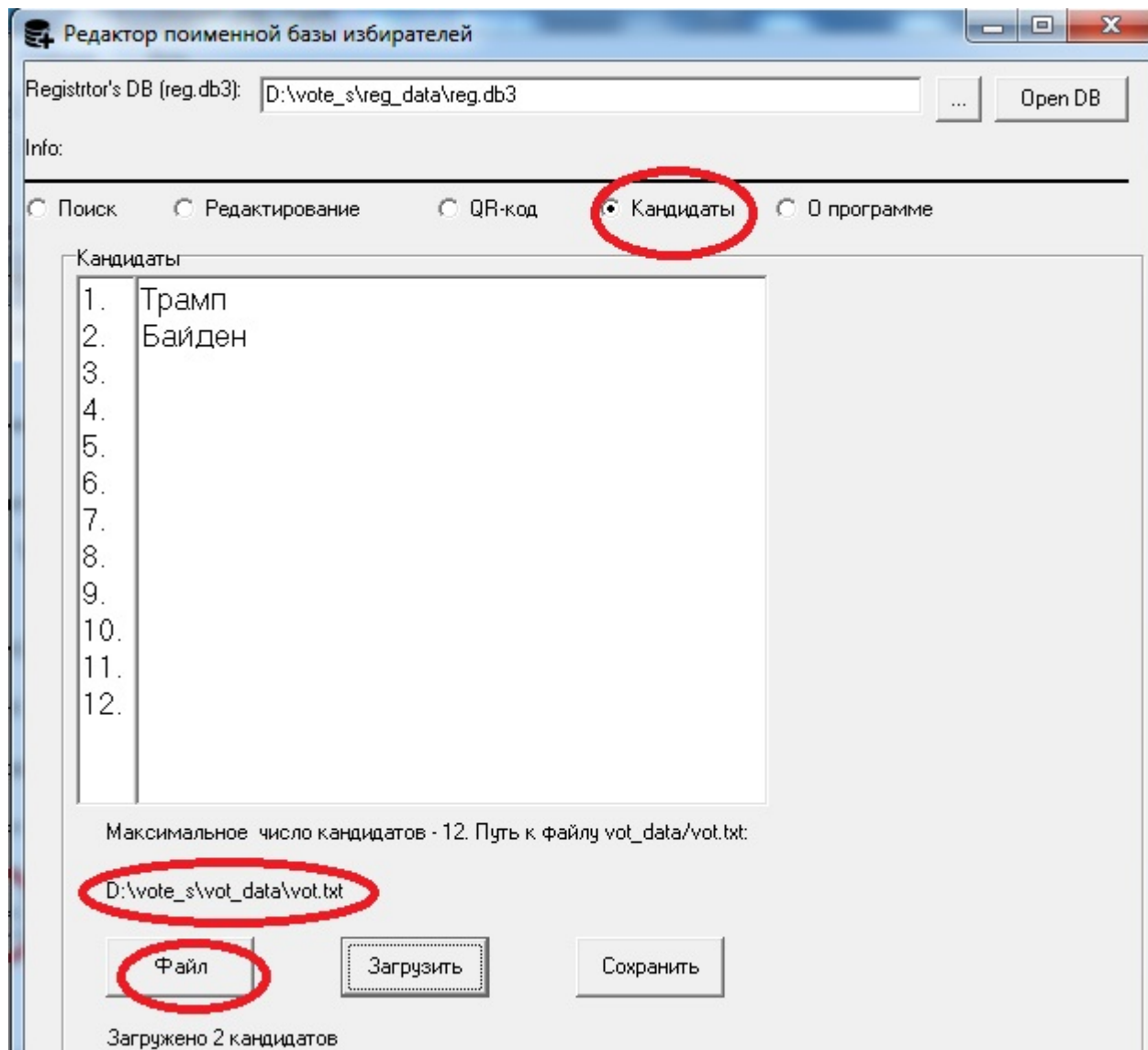


Рис.4. Вкладка для додавання кандидатів голосування.

7. Перейдіть на вкладку **‘Редактирование’** (рис.5) для формування списку виборців.

- натисніть кнопку **«Новий»**
- введіть прізвище та ідентифікаційний код виборця у відповідні поля (можна використовувати латиницю та кирилицю)
- натисніть кнопку **«Авто»** для генерування пароля виборця
- натисніть кнопку **«Сохранить»** для збереження інформації у базі даних
- натисніть кнопку **«QR-код»** для створення персонального запрошення на вибори

- на вкладці «QR-код», що відкриється (рис. 6), натисніть кнопку «Сохранить».

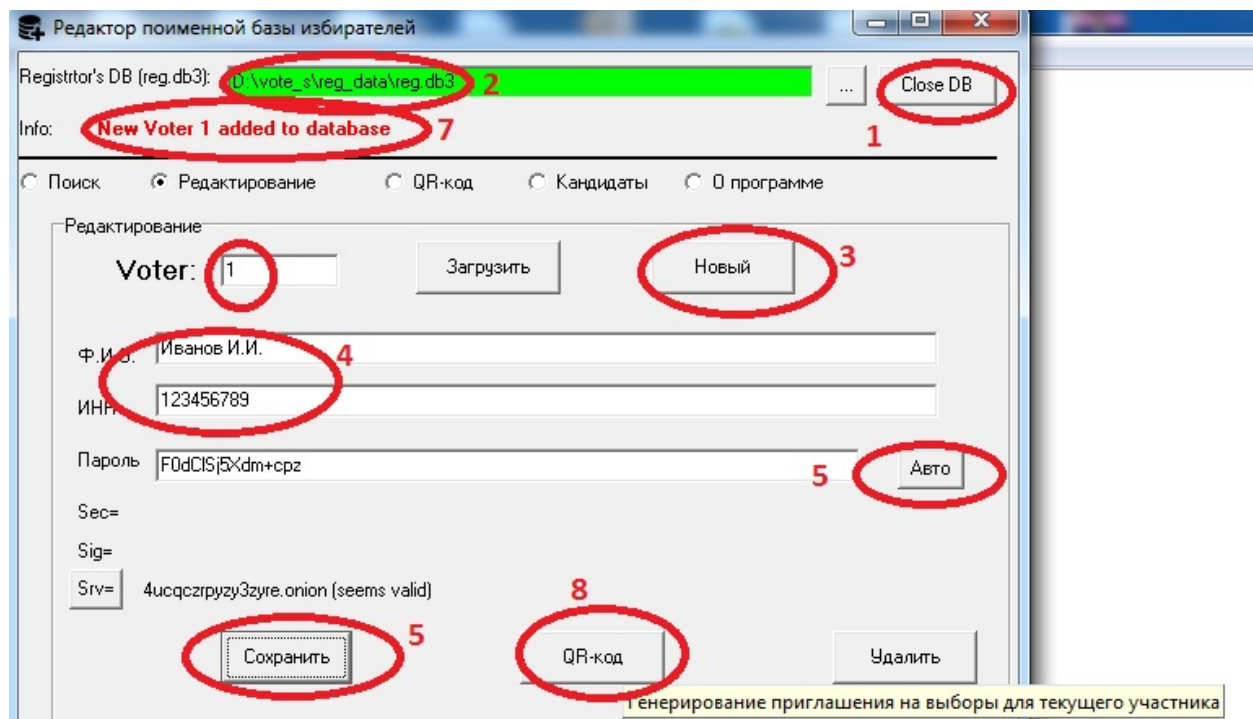


Рис. 5. Додання виборця до списку: 1 – кнопка відкривання бази даних, 2 – зелений колір свідчить про те, що база даних відкрита, 3 – кнопка додавання нового виборця, 4 – поля ПІБ та ІНН, 5 – кнопка автоматичного генерування унікального паролю виборця, кнопка збереження персональних даних у базі, 8 – кнопка генерації QR-коду персонального запрошення на вибори.

8. Повторюючи дії, вказані в пункті 7, додайте потрібну кількість виборців до бази даних. Кількість виборців практично необмежена, для тестування достатньо додати близько 16 осіб.

9. Вийдіть з додатку та роздрукуйте запрошення, що знаходяться у вигляді малюнків (*jpeg*-файлів) у папці *vote\_s/qrcode*. Файл запрошення починається з літери *q\_* та містить номер запису у базі даних. Зручно розмістити 16 запрошень (4 \* 4) на одному аркуші А4 в альбомній орієнтації. Також у цій папці знаходяться запрошення у вигляді файлів даних, які розпочинаються з літери *d\_* та мають розширення *.dat*. Ці файли також можуть бути використані учасниками виборів для отримання доступу у випадку

відсутності можливості відсканувати QR-код (наприклад, при відсутності камери на комп'ютері).

Увага: запрошення містять індивідуальний пароль та дають право участі у виборах. Витік даних про вміст запрошення може призвести до неправомірного використання зловмисником виборчого права. Тому передавайте запрошення виборцям у закритому світлонепроникному конверті (по аналогії з пін-кодом банківських карт).

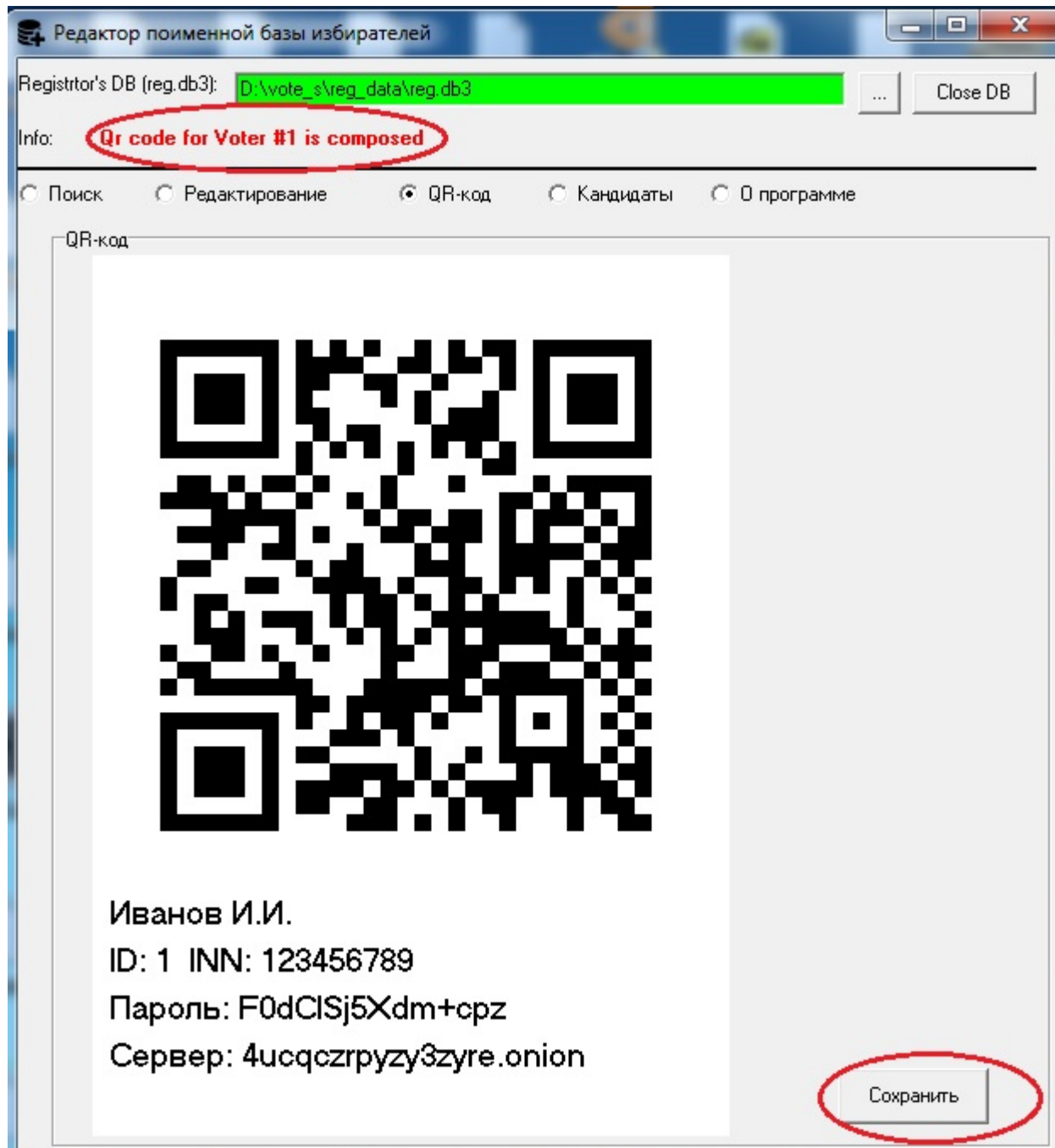


Рис. 6. Створення персонального запрошення на вибори.



10. Після підготовки бази даних знову запустіть сервер та дочекайтеся 100% завантаження Tor (див. п.3). Почекайте ще 1-2 хвилини, потрібні на публікацію сервером своєї onion-адреси в мережі DarkNet. Тепер сервер готовий до голосування.

## II. Налаштування клієнта

1. Для використання клієнтського додатку на Windows-комп'ютері чи ноутбуків завантажте архів за посиланням: <http://torfone.org/download/vote.zip> та розархівуйте папку *vote* на жорсткий диск вашого комп'ютера з будь-якою версією Windows (від XP 32bit до Win10 64 bit). Уникайте надто довгих шляхів та таких, що містять символи кирилиці або пробіли. Зайдіть у папку та запустіть виконуючий файл клієнта *Vote.exe*. За замовчуванням, крім графічного інтерфейсу додатку буде відкрите консольне вікно анонімізатора Tor. Дочекайтеся 100% завантаження Tor (аналогічно як при налаштуванні серверу, це може тривати до 10 хв, при наступних запусках – до 1 хв). Для того, щоб надалі не показувати вікно Tor, видаліть файл *vote/wintor/show.txt*

2. Для використання клієнтського додатку на Android-телефоні чи планшеті завантажте додаток за посиланням: <http://torfone.org/download/vote.apk> Для встановлення додатку на телефоні дозвольте встановлення з невідомих джерел та дозвольте доступ до Інтернету, камери та сховища (SD-карти). Після першого запуску додатку залиште його включеним та почекайте 10 хв для 100% підключення вбудованого анонімізатора Tor до мережі. При наступних запусках чекайте близько хвилини після відкриття додатку.

3. У верхній частині додатку (рис. 7) знаходяться кнопка ‘?’ для переходу до вікна з інформацією про програму та її автора та кнопка ‘i’ для переходу до вікна з персональною інформацією та станом виборця. У середній частині знаходяться кнопки дій користувача відповідно до кроків процедури

голосування. Першим кроком є сканування QR-коду запрошення на вибори. Натисніть кнопку «Сканировать» для переходу на вкладку сканування.

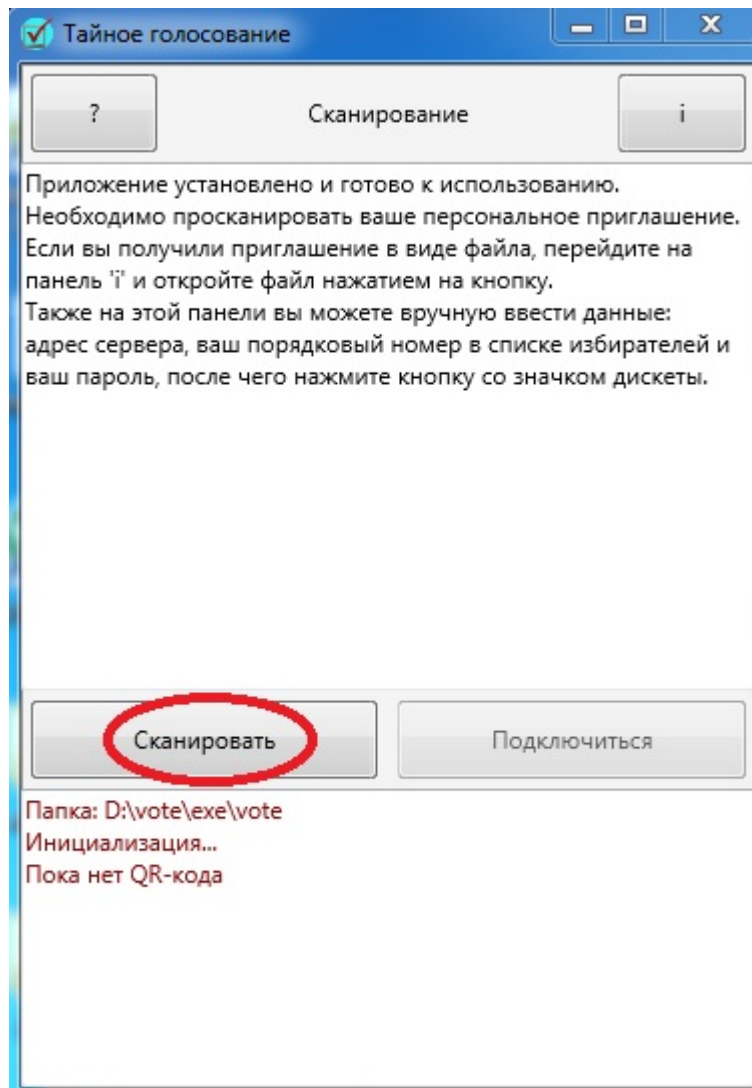


Рис. 7. Вигляд клієнтського додатку після встановлення.

4. Для сканування запрошення розмістіть його перед камерою та тримайте нерухомо декілька секунд. На мобільних пристроях ви можете вибрати основну чи фронтальну камеру та включити освітлення (рис. 8). Також при необхідності можна змінити роздільну здатність камери. Після успішного сканування виводиться повідомлення та червоний надпис на кнопці «ОК». натисніть на неї для переходу до наступного кроку.





Рис.8. Сканування персонального запрошення на вибори.

5. Після сканування запрошення потрібно пройти наступні кроки, натискаючи на відповідні кнопки: «Подключение», «Идентификация» и «Регистрация» (рис.9, 10, 11).

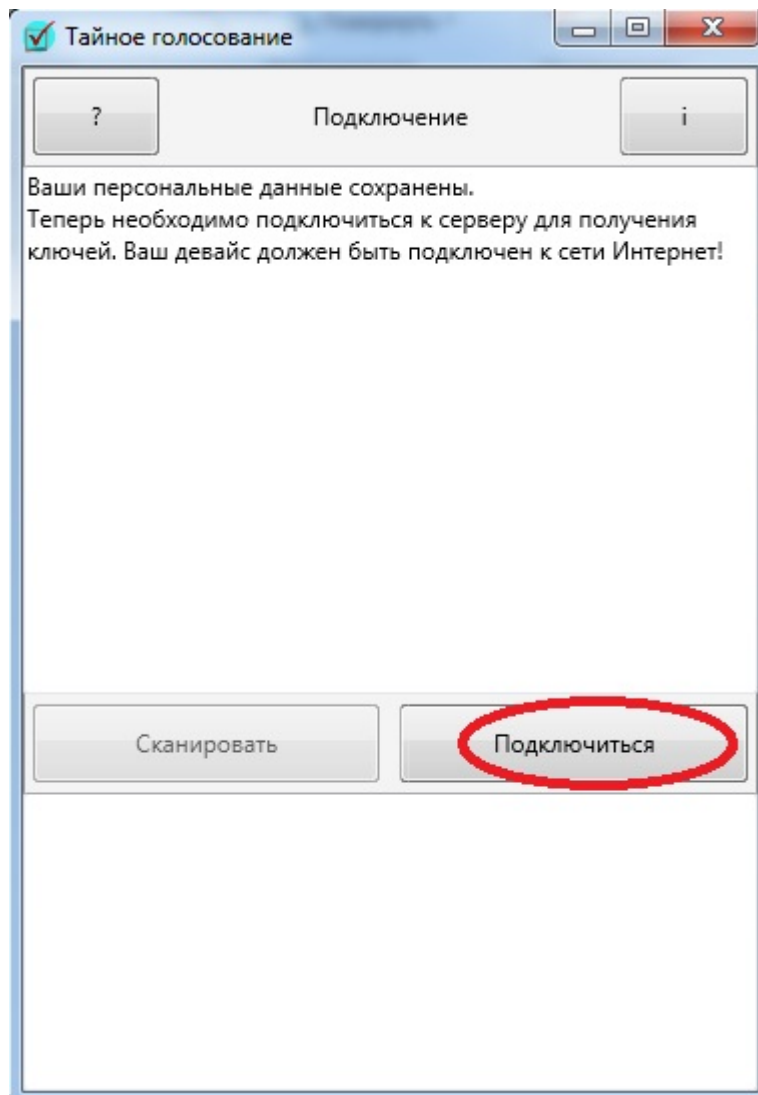


Рис. 9. Стадія підключення до серверу.

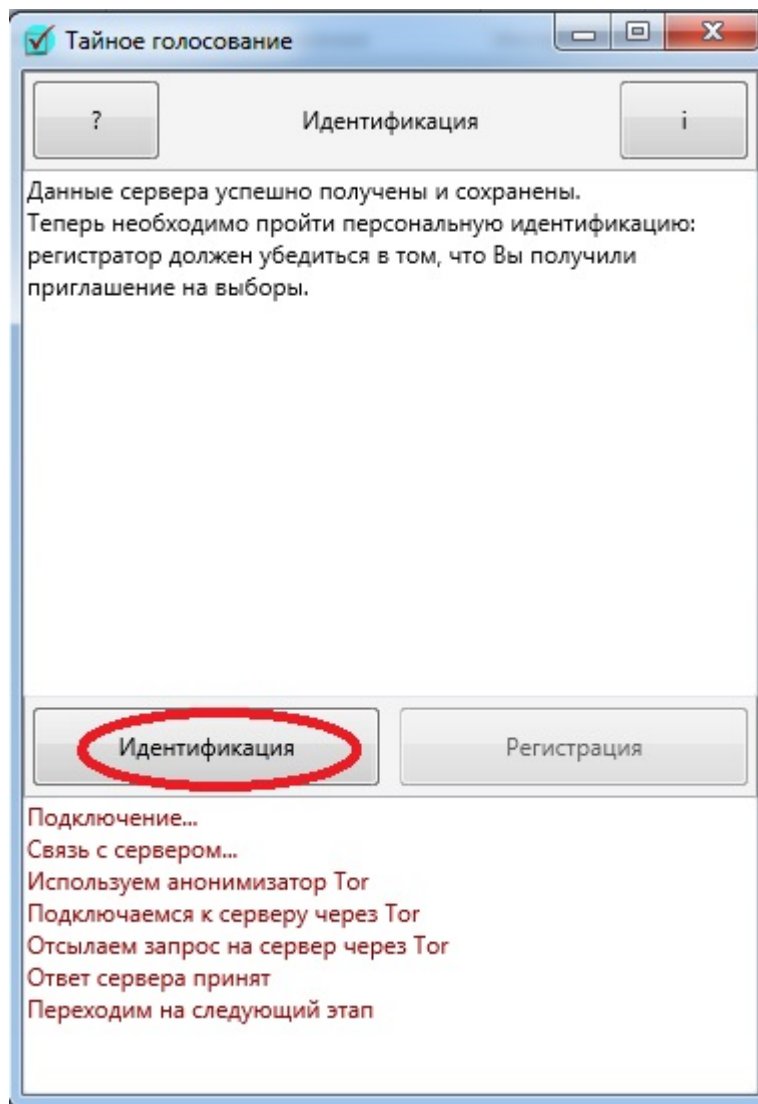


Рис. 10. Стадія ідентифікації користувача.

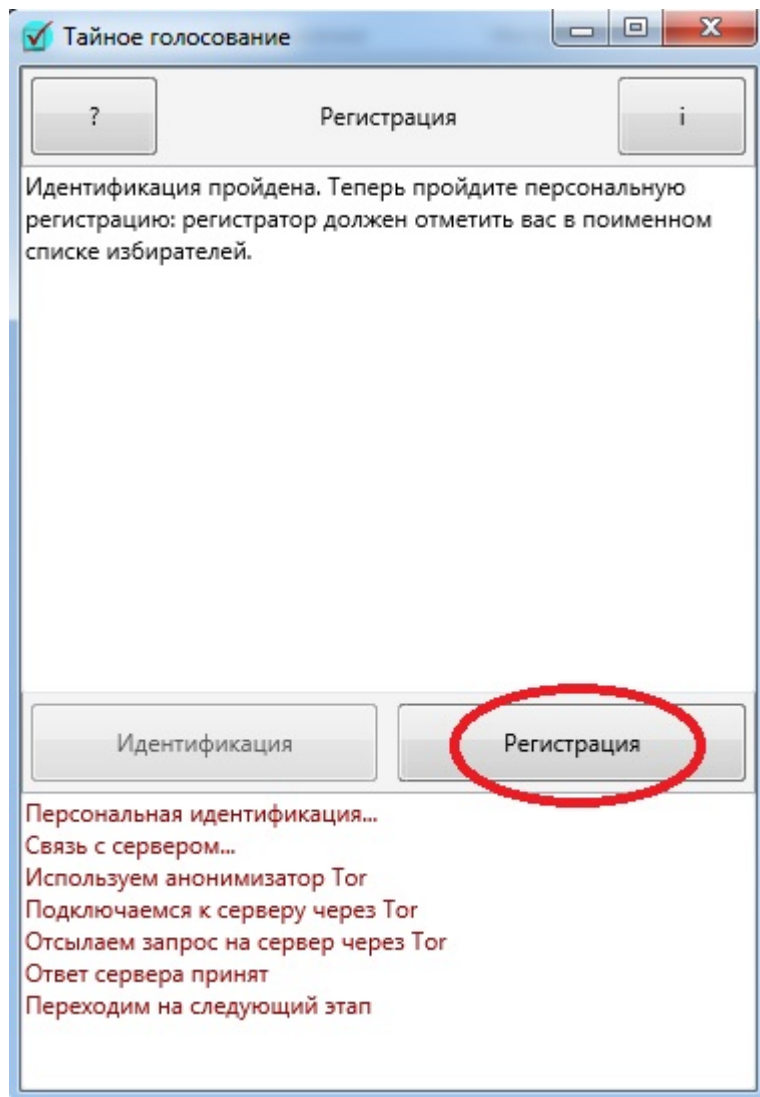


Рис. 11. Стадія персональної реєстрації.

6. Після успішної реєстрації необхідно перезапустити додаток, щоб змінити мережеву ідентичність при переході до анонімної стадії голосування. Натисніть кнопку «**Перезапуск**» (рис. 12) для виходу з додатку. зачекайте деякий час: це захистить від можливості співставлення часу персональної реєстрації та анонімного отримання бюлетеня, що може привести до деанонімізації користувача.

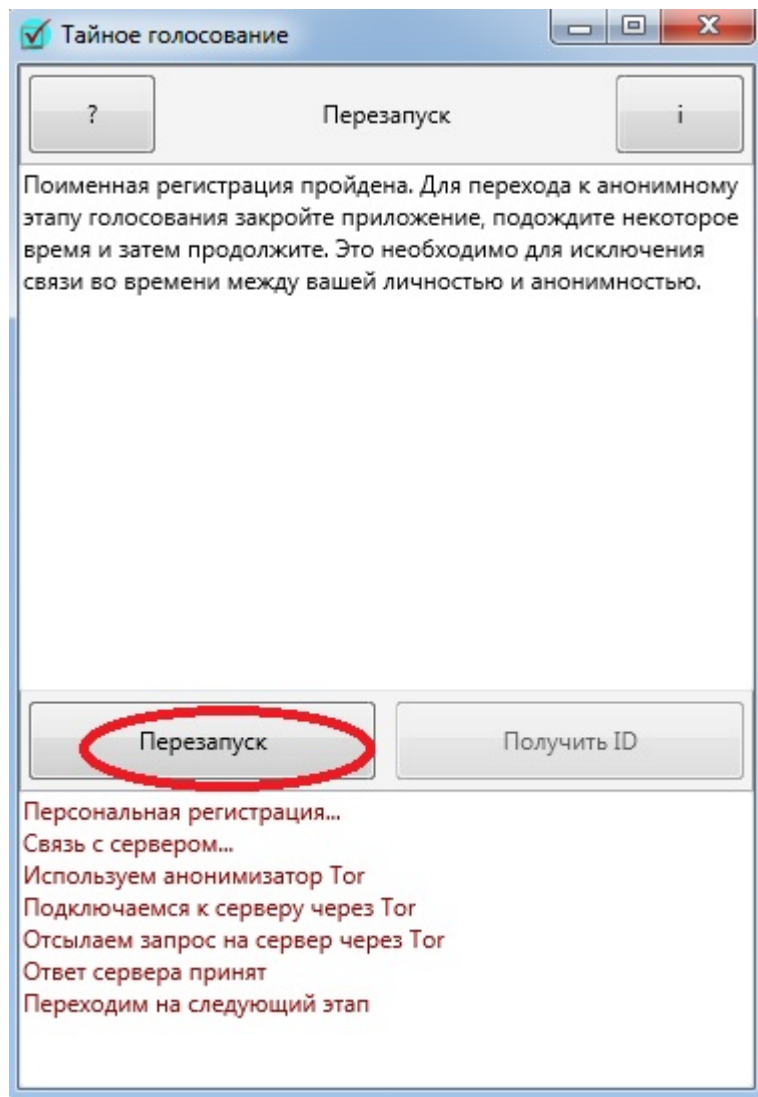


Рис.12. Стадія перезапуску додатку при переході від персональної до анонімної стадії голосування.

7. Після повторного запуску додатку зачекайте хвилину та можете отримати бюлетень (рис. 13).

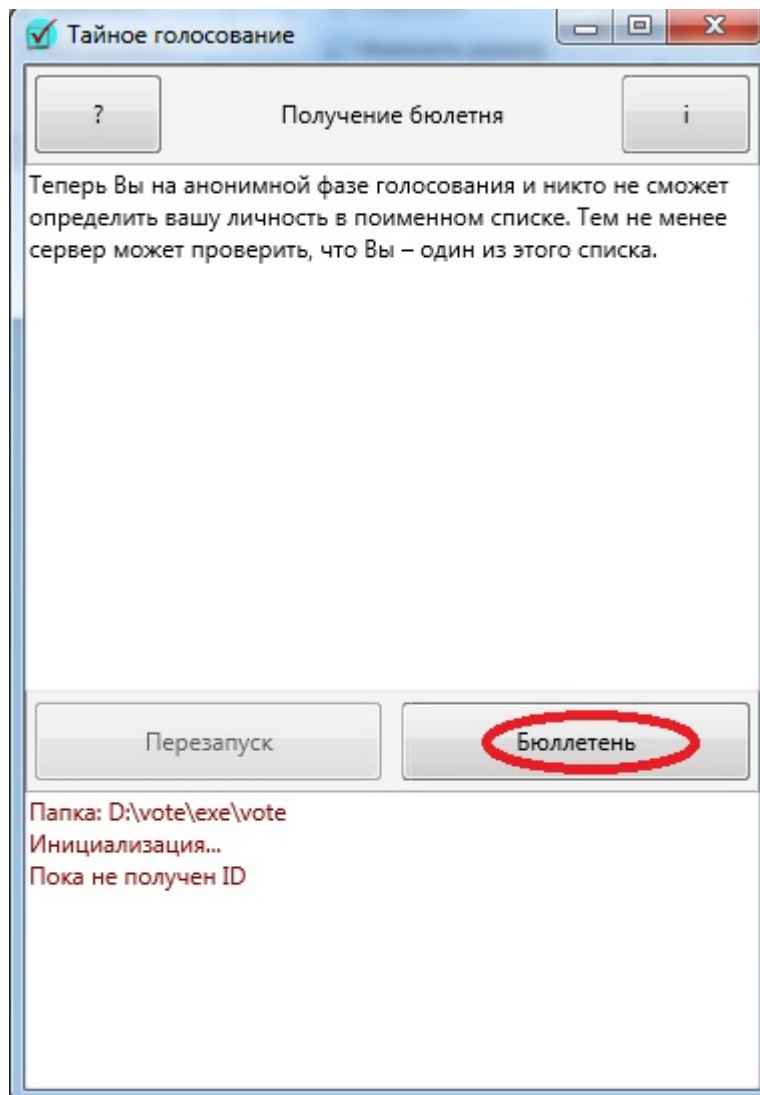


Рис.13. Отримання анонімного бюлетеня.

8. Після отримання бюлетеня можлива власне процедура голосування: (рис. 14, 15).

Натисніть кнопку **«Голосувати»**, відкриється вкладка вибору голосу. Натисніть на випадаючий список у верхній частині вікна додатку та виберіть вашого кандидата.

Підтвердіть свій вибір, натиснувши на кнопку **«ОК»**.

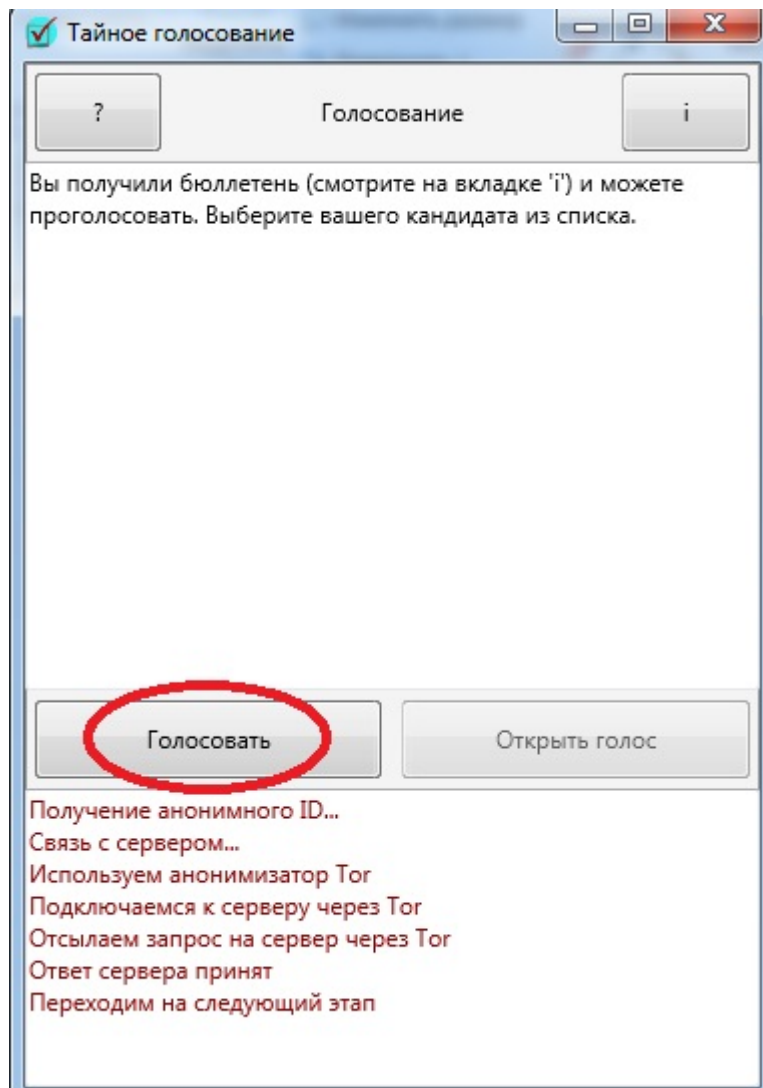


Рис.14. Перехід до процедури вибору голосу.

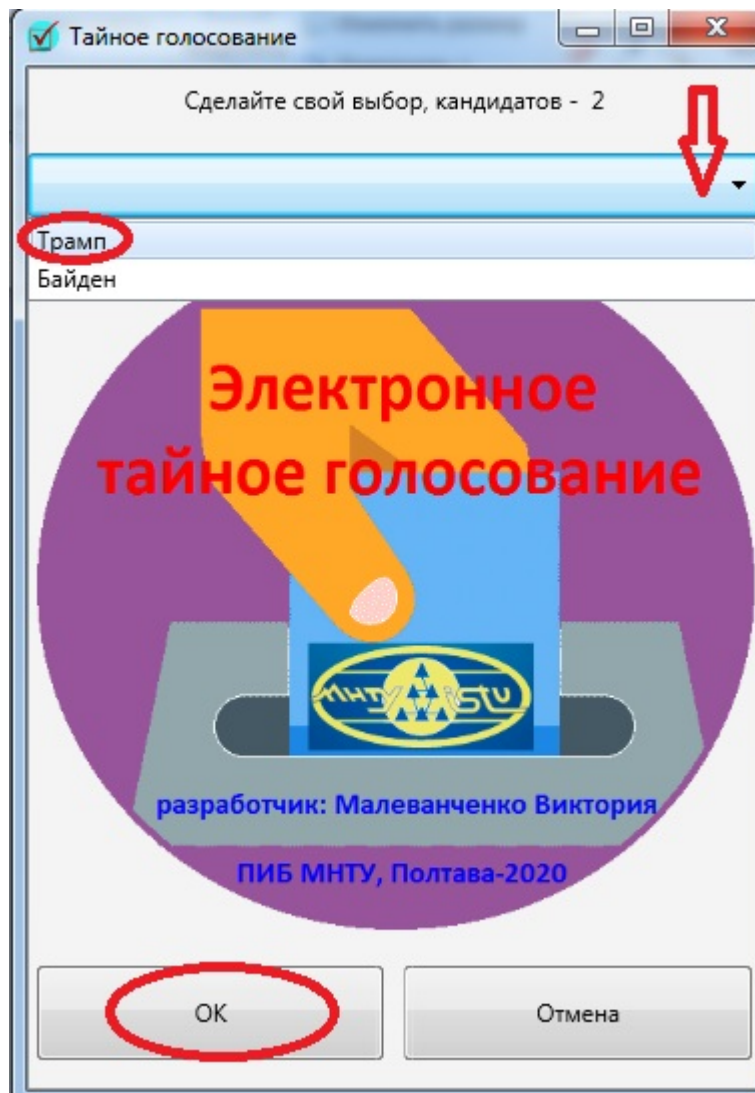


Рис.15. Вибір кандидата.

9. Після голосування необхідно відкрити свій голос. Натисніть кнопку «Открыть» для завершення процедури голосування (рис. 16):



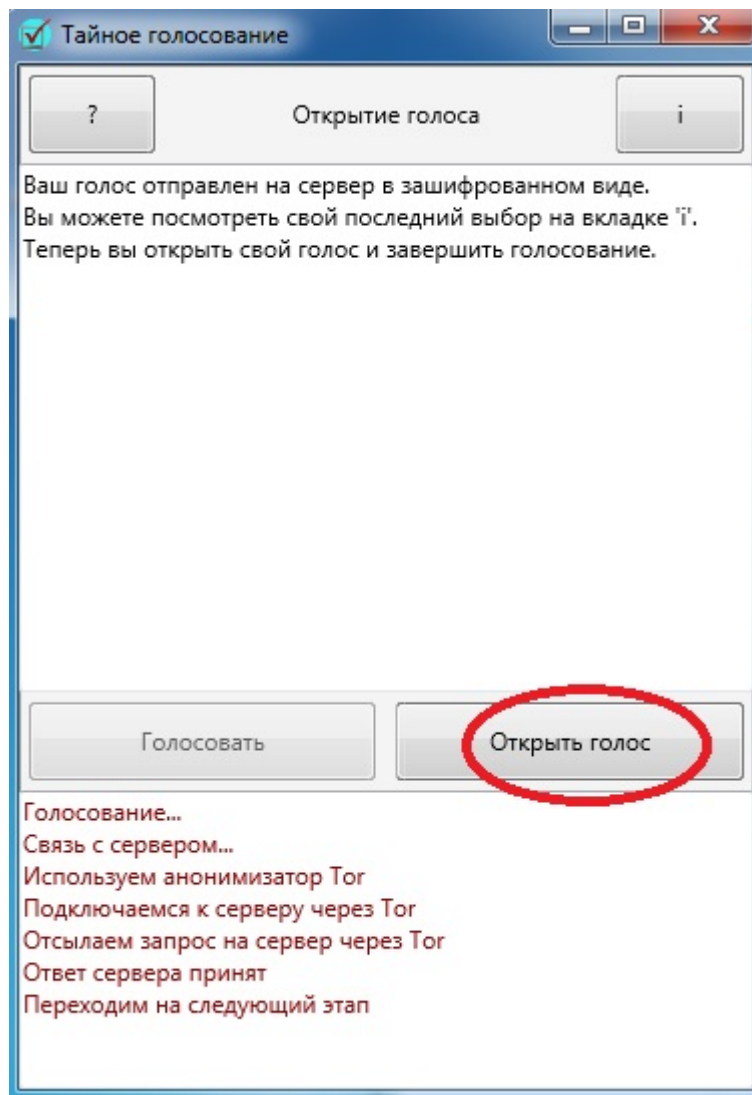


Рис. 16. Відкриття голосу.

10. Ваші персональні дані та результати голосування можна переглянути на вкладці «і» (рис.17). Наводяться дані, отримані в особистому запрошенні на вибори (onion-адреса сервера, номер виборця у списку та його пароль), а також номер отриманого анонімного бюлетеня та ваш голос. Ці дані можуть бути використані для індивідуального контролю за виборами через web-інтерфейс сервера. Крім того, у папці *vote/pub* Windows-додатку або у папці *Документи/vote* на внутрішньому диску Android-пристрою зберігаються так звані квитанції з електронними підписами сервера, що підтверджують персональну реєстрацію, видачу анонімного бюлетеня, прийняття голосу та його відкриття. Ці квитанції можуть бути використані як докази шахрайства з

боку сервера у випадку, коли користувач виявив невідповідність свого голосу з відображеним у веб-інтерфейсі сервера.

Тайное голосование

Onion-адрес сервера:  
4ucqczrpyzy3zyre.onion

Ваш номер в списке:  
12

Ваш пароль:  
0Ptn7iz4F/mW6i+

Ваш анонимный код:  
1

Ваш голос:  
Трамп

Этап голосования:  
Завершено

Голос был успешно открыт

Выйти

Рис.17. Вкладка 'i' с персональной информацией избирателя.

### III. Контроль за голосованием.

1. Контроль за выборами проводится каждым избирателем и активистами для выявления фактов шатраства з боку сервера (Регистратора та Рахувника голосів). Для цього використовується Web-інтерфейс сервера, доступний у мережі DarkNet. Адреса сервера відображається у консольному вікні самого сервера (див. рис. 1), у персональному запрошенні на вибори (див. рис. 6) та у клієнтському додатку (див. рис. 17). Для доступу до сервера

найбільш надійним є використання Тор-браузера, доступного за посиланням:  
<https://www.torproject.org/ru/download/>

Також є можливість використання так званих шлюзів, які забезпечують доступ у DarkNet зі звичайної мережі Інтернет з використанням будь-якого браузера, наприклад, Google Chrome. Такі шлюзи утримуються волонтерами та мають обмежений термін життя, так як дають доступ звичайним користувачам до нецензурованої і часто протизаконної інформації у мережі DarkNet. На момент написання цієї інструкції функціонує шлюз *sh*. Додайте до onion-адреси вашого сервера суфікс *.sh* та відкрийте посилання у звичайному браузері (рис. 18). Сучасні браузери прагнуть використовувати захищене з'єднання *https*, тоді як наше посилання є звичайним *http*. Тому браузер може показати сторінку попередження про недостовірне з'єднання. Дозвольте перегляд, натиснувши надпис «Додатково» та «перейти на сторінку - небезпечно». У різних браузерах алгоритм дозволу може відрізнятись. Натисніть посилання «**На русском**» внизу головної сторінки для подальшого перегляду інформації на російській мові.

67

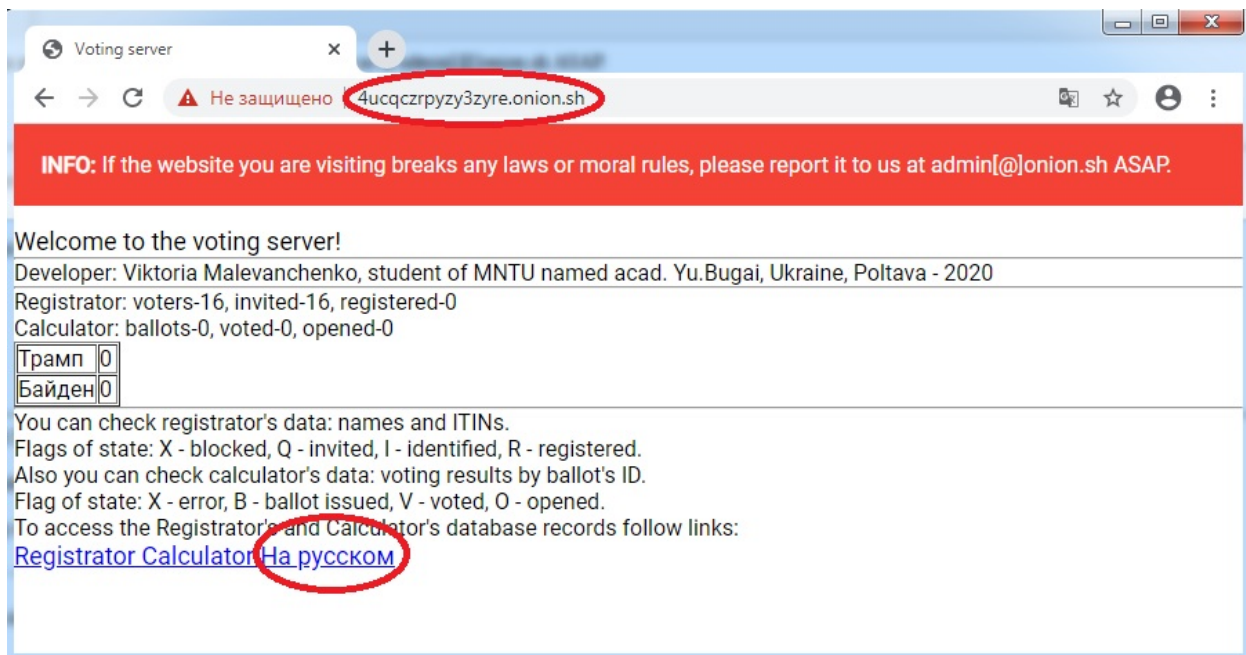


Рис.18. Головна англomовна сторінка web-інтерфейсу сервера для голосування в DarkNet, відкрита в звичайному браузері за допомогою шлюзу *sh*.

2. На головній сторінці сервера відображається загальна статистика виборів: кількість виборців у списку, кількість виданих запрошень, кількість виборців, що пройшли персональну реєстрацію, кількість виданих бюлетенів, кількість бюлетенів, що проголосували та кількість відкритих голосів. Також в таблиці відображається кількість голосів, відданих за кожного з кандидатів (рис. 19).

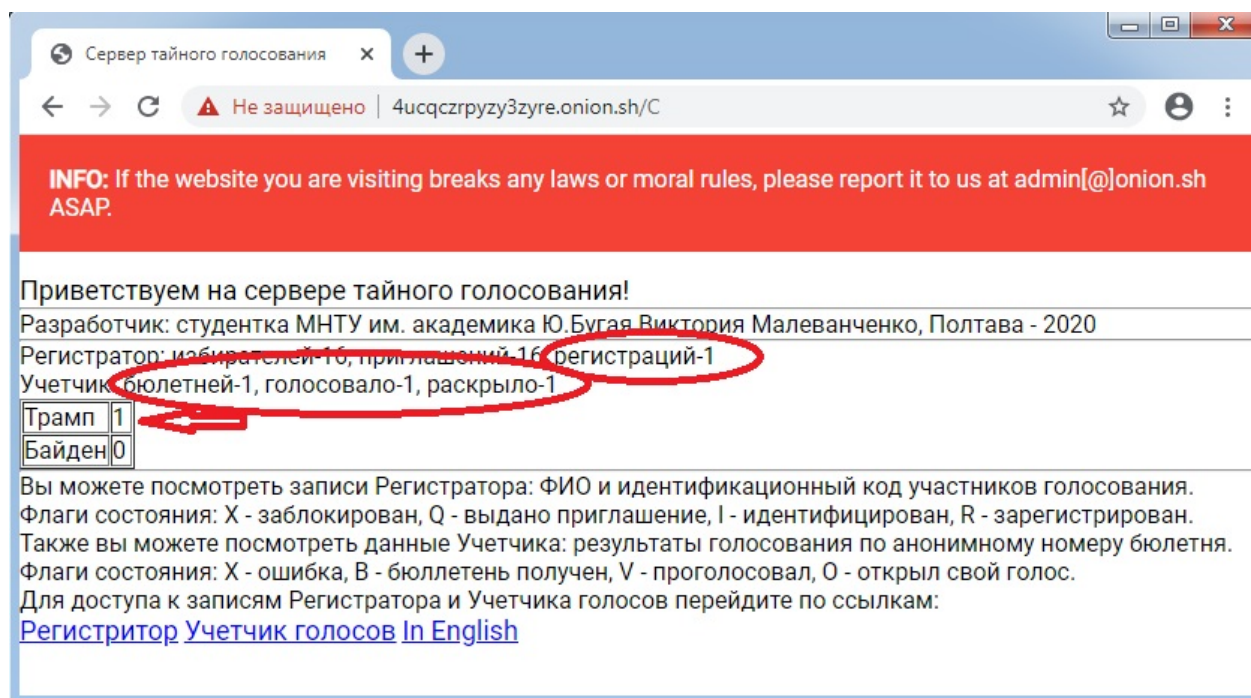
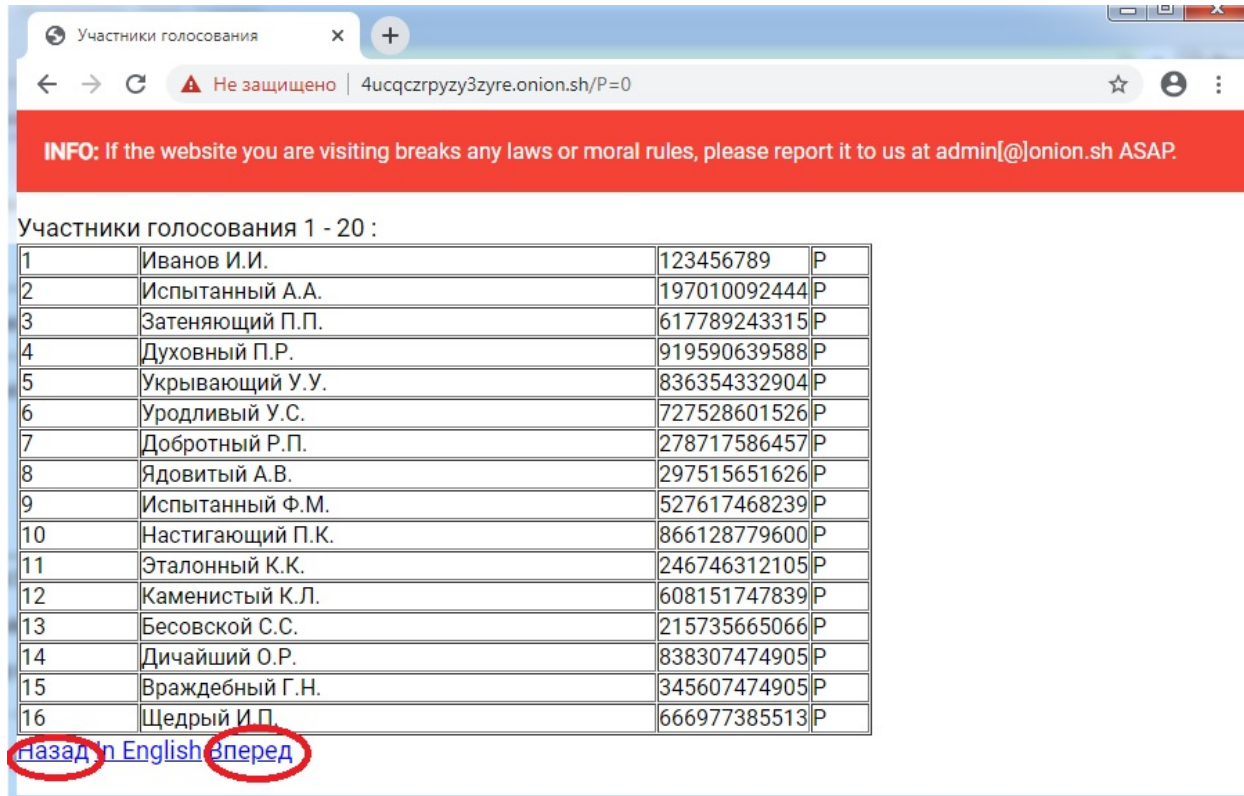


Рис. 19. Головна російськомовна web-сторінка сервера таємного голосування.

3. Для перегляду власних даних скористайтесь інформацією про ваш номер у персональному списку виборців та про номер вашого анонімного бюлетеня. Перейдіть відповідно на сторінки Реєстратора (рис.20) та Рахівника (рис.21) для перегляду відповідного запису у їх базах даних. Інформація

видається у вигляді таблиці по 20 записів. Використовуйте посилання «Вперед» та «Назад» для навігації по таблицях і для перегляду власних персональних даних та отриманого бюлетеня відповідно за номером у списку виборців та номером бюлетеня.



Участники голосования 1 - 20 :

|    |                  |              |   |
|----|------------------|--------------|---|
| 1  | Иванов И.И.      | 123456789    | P |
| 2  | Испытанный А.А.  | 197010092444 | P |
| 3  | Затеняющий П.П.  | 617789243315 | P |
| 4  | Духовный П.Р.    | 919590639588 | P |
| 5  | Укрывающий У.У.  | 836354332904 | P |
| 6  | Уродливый У.С.   | 727528601526 | P |
| 7  | Добротный Р.П.   | 278717586457 | P |
| 8  | Ядовитый А.В.    | 297515651626 | P |
| 9  | Испытанный Ф.М.  | 527617468239 | P |
| 10 | Настигающий П.К. | 866128779600 | P |
| 11 | Эталонный К.К.   | 246746312105 | P |
| 12 | Каменистый К.Л.  | 608151747839 | P |
| 13 | Бесовской С.С.   | 215735665066 | P |
| 14 | Дичайший О.Р.    | 838307474905 | P |
| 15 | Враждебный Г.Н.  | 345607474905 | P |
| 16 | Щедрый И.П.      | 666977385513 | P |

Назад In English Вперед

Рис. 20. Персональний список виборців (ПІБ та ПІН). Стан: Р-отримав запрошення, І-ідентифікувався, Р-зареєструвався.

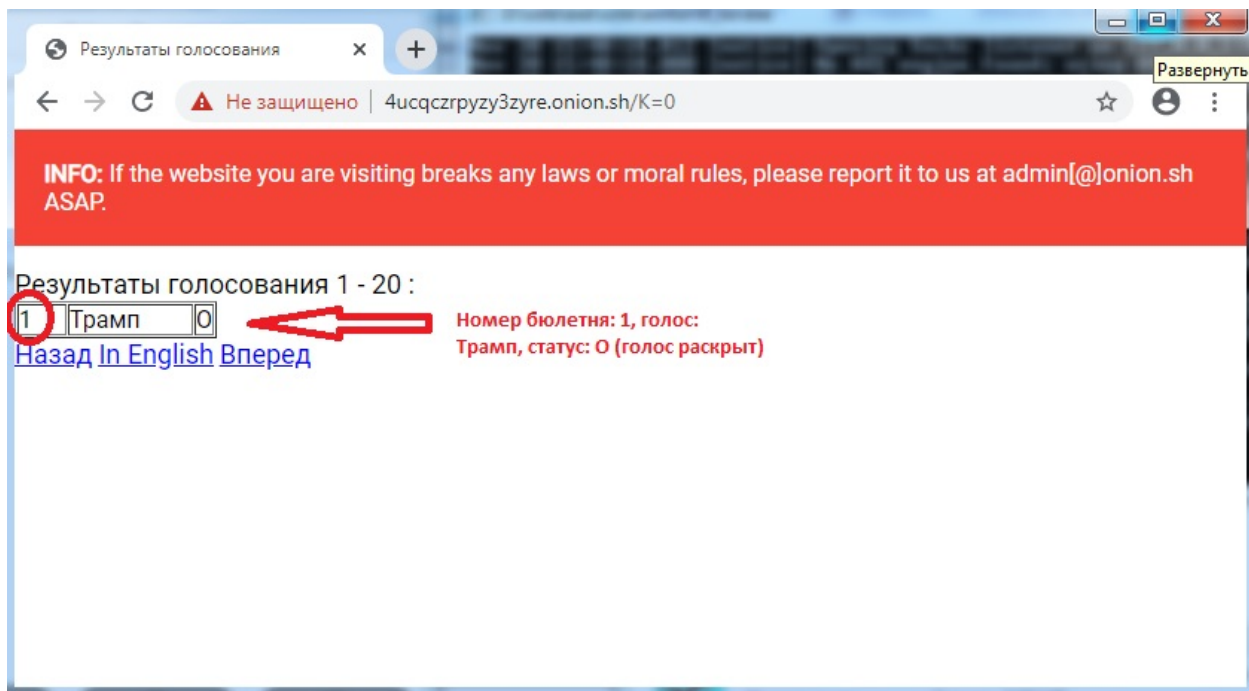


Рис. 21. Список бюлетенів. Відображується номер анонімного бюлетеня та голос (у випадку, якщо вже відкритий). Стан: J-бюлетень виданий, V-проголосував, O-відкрив свій голос.

## ВИСНОВКИ

1. Сучасний виборчий процес може бути реалізований шляхом електронного голосування. Це забезпечить більший захист від втручання у вибори порівняно з класичними виборами з паперовими бюлетенями.

2. Національними особливостями вибрів є значно вищий рівень загроз, пов'язаних з фальсифікаціями з боку організаторів виборів (використання «мертвих душ», вибраковка бюлетенів та невірний підрахунок) порівняно з іншими загрозами, наприклад, підкупом чи примусом виборців.

3. Найбільш оптимальним для реалізації таємного голосування є протокол He-Su, модифікований для забезпечення можливості підтвердження фактів фальсифікації організаторів виборів. Така модифікація конкурує з можливістю забезпечення зміни голосу під час голосування, що не є актуальним в національних умовах.

4. Для таємного голосування доцільно використовувати клієнтські додатки для мобільних телефонів та комп'ютерів, розроблені під найбільш поширені операційні системи: Windows, Android, iOS та Linux. Відкритий вихідний код є необхідною умовою прозорості виборів. Використання web-інтерфейсу не рекомендується через низький рівень захисту сучасних web-браузерів та web-протоколів.

5. Інтерфейс користувача повинен бути максимально простим та інтуїтивно зрозумілим, включати тільки необхідні для голосування елементи без необхідності додаткових налаштувань.



## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Основополагающие документы Венецианской комиссии в области избирательного права и политических партий [Electronic source] – URL:[http://www.venice.coe.int/images/SITE%20IMAGES/Publications/ElectionsandPP\\_RUS.pdf](http://www.venice.coe.int/images/SITE%20IMAGES/Publications/ElectionsandPP_RUS.pdf)
2. Кодекс належної практики у виборчих справах. Керівні принципи та Пояснювальна доповідь (CDL-AD(2002)23rev) // Європейський демократичний доробок у галузі виборчого права: Матеріали Венеціанської Комісії : в 2 ч. : пер. з англ. / за ред. Ю. Ключковського. – Вид. 3-тє, випр. і доповн. – Ч. 1. – К. : Логос, 2016. – С. 143–176.
3. Марцеляк О. В. Вибори народних депутатів України: історія, теорія, практика : навч. посібник / О. В. Марцеляк. – Харків : Прометей-Прес, 2008. – 636 с.
4. Ключковський Ю. Принцип чесних виборів у виборчому праві України / Ю. Ключковський // Право України. – 2013. – № 5. – С. 165–174.
5. Бондарь Н. С. Предвыборная агитация: теория и практика / Н. С. Бондарь, А. А. Джагарян, Н. В. Хачатуров ; отв. ред. Н. С. Бондарь. – М. : Формула права, 2004. – 220 с.
6. Шведа Ю. Вибори та виборчі системи. Європейські стандарти та досвід для утвердження демократії в Україні / Ю. Шведа. – Львів, 2010. – 462 с.
7. Gritzalis D., Principles and requirements for a secure e-voting system. / Gritzalis D. — Computers Security, Vol. 21(6), 2002 — С. 539- 556, [Електронний ресурс]. — Режим доступу: [http://www.instore.gr/evote/evote\\_end/htm/3public/doc3/public/aegean/paper7.pdf](http://www.instore.gr/evote/evote_end/htm/3public/doc3/public/aegean/paper7.pdf).
8. Aditya Riza. Secure electronic voting with flexible ballot structure. / Aditya Riza — PhD thesis, Queensland University of Technology, 2005 — 200 с. [Електронний ресурс]. — Режим доступу: [http://eprints.qut.edu.au/16156/1/Riza\\_Aditya\\_Thesis.pdf](http://eprints.qut.edu.au/16156/1/Riza_Aditya_Thesis.pdf).
9. Evaluating e-voting: theory and practice / Manon de Vries and Wouter Bokslag — Department of Information Security Technology Technical University of Eindhoven, 2016. [Електронний ресурс]. — Режим доступу: <https://arxiv.org/pdf/1602.02509.pdf>.



10. Survey on Remote Electronic Voting / Alexander Schneider. — Christian Meter Philipp Hagemester, 2017. [Электронный ресурс]. — Режим доступа: <https://arxiv.org/pdf/1702.02798.pdf>.
11. Chaum D.L. Secret-Ballot Receipts: True Voter-Verifiable Elections / Chaum D.L. — IEEE Security Privacy Magazine, Feb 2004.
12. Schneier B. What's Wrong With Electronic Voting Machines? [Electronic source] — URL: [https://www.schneier.com/essays/archives/2004/11/whats\\_wrong\\_with\\_ele.html](https://www.schneier.com/essays/archives/2004/11/whats_wrong_with_ele.html)
13. The electronic voting in Estonia. [Electronic source]. — URL: [http://ru.wikipedia.org/wiki/Электронное\\_голосование\\_в\\_Эстонии](http://ru.wikipedia.org/wiki/Электронное_голосование_в_Эстонии)
14. Мачалін І. О. Технологія автентифікації виборців у відкритій системі Інтернет голосування / І. О. Мачалін, В. М. Вишняков, О. О. Комарницький // Радіoeлектроніка та інформатика. 2018. — № 2. — С. 55–62.
15. Чуприн В. М., Вишняков В. М., Пригара М. П. Метод протидії незаконному впливу на виборців у системі Інтернет голосування. Безпека інформації. 2017. — Том 23. — № 1. — С. 7–14.
16. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.: Триумф, 2002. — 816 с.
17. Введение в криптографию / Под общ. ред. В. В. Ященко. - 4-е изд., доп. М.: МЦНМО, 2012. - 348 с.
18. Ключев А. Электронное голосование [Электронный ресурс] // Gosbook.ru. — URL: <http://www.gosbook.ru/node/28337> (дата обращения: 13.06.2016).
19. Fudjioka A., Okamoto T., Ohta K. A Practical Secret Voting Scheme for Large Scale Elections [Электронный ресурс] // Csail.mit.edu. — URL: <https://people.csail.mit.edu/rivest/voting/papers/FujiokaOkamotoOhta-APracticalSecretVotingSchemeForLargeScaleElections.pdf> (дата обращения: 17.06.2016).
20. He Q., Su Z. A New Practical Secure e-Voting Scheme [Электронный ресурс] // Cs.cmu.edu. — URL: [http://www.cs.cmu.edu/~qihe/paper/e\\_voting](http://www.cs.cmu.edu/~qihe/paper/e_voting) (дата обращения: 17.06.2016).
21. Реализация протоколов тайного электронного голосования [Электронный ресурс]. URL: <https://sibac.info/studconf/tech/xxxii/42180> (дата обращения: 1.12.2018). Загл. с экрана. Яз. рус.
22. Cramer R. Multi-Authority Secret-Ballot Elections with Linear Work / R. Cramer, M. Franklin, B. Shoenmakers, M. Yung // Proc. EUROCRYPT'96, Lect. Notes in Comput. Sci. 1996. Vol. 1070. P. 72–83.

23. Рацеев С.М. О протоколах электронного голосования / С.М. Рацеев, О.И. Череватенко 8 с. / Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. 2018. Т. 18, вып. 1. С. 62-67.
24. Chaum D. Wallet databases with observers / D. Chaum, T. P. Pedersen // Proc. Crypto'92, Lect. Notes in Comput. Sci. 1993. Vol. 740. P. 89–105.
25. Протоколы электронного голосования [Электронный ресурс]. URL: <https://studfiles.net/preview/4483753/page:15/> (дата обращения: 1.12.2018). Загл. с экрана. Яз. рус.
26. Cramer R. A secure and optimally efficient multi-authority election scheme / R. Cramer, R. Gennaro, B. Schoenmakers // Proc. EUROCRYPT'97, Lect. Notes in Comput. Sci. 1997. Vol. 1233. P.103–118.
27. Мао В. Современная криптография. Теория и практика / В. Мао. – Москва : Вильямс, 2005. – 763 с. CASPIAN JOURNAL: Control and High Technologies, 2019,
28. Fujioka A. A practical secret voting scheme for large scale election / A. Fujioka, T. Okamoto and K. Ohta // Advances in Cryptology-Auscrypt'92, LNCS 718. – Springer-Verlag, 1992. – P. 244 – 260.
29. Chaum D. Blind signatures for untraceable payments / D. Chaum // Proceedings of Crypto 82. – New York : Plenum Press, 1983. – P. 199 – 203.
30. Nurmi H. Secret ballot elections in computer networks / H. Nurmi, A. Salomaa, L. Santeau // Computers and Security. – 1991. – Vol. 36, № 10. – P. 553 – 560.
31. Rivest R. L. A Method for Obtaining Digital Signatures and Public Key Cryptosystems / R. L. Rivest, A. Shamir, L. M. Adleman Communications of the ACM. – 1978. – Vol. 21, № 2. – P. 120 – 126.
32. Chaum D. Security without identification: Transaction systems to make big brother obsolete. Communication of the ACM, Oct. 1985, vol. 28, no. 10, pp. 1030–1044.
33. Молдовян Н. А. Протоколы слепой коллективной подписи на основе стандартов цифровой подписи. Вопросы защиты информации, 2010, № 1, с. 2–6.
34. Молдовян Н. А. Введение в криптосистемы с открытым ключом. / Молдовян Николай Андреевич — Петербург, 288 С, 2005. — С. 195-199.
35. 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.