



УКРАЇНА

(19) UA (11) 91920 (13) C2  
(51) МПК (2009)  
G07C 13/00

МІНІСТЕРСТВО ОСВІТИ  
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ

## ОПИС ДО ПАТЕНТУ НА ВІНАХІД

### (54) СПОСІБ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

1

(21) а200900175

(22) 10.01.2009

(24) 10.09.2010

(46) 10.09.2010, Бюл.№ 17, 2010 р.

(72) СЕРГІЄНКО ІВАН ВАСИЛЬОВИЧ, БОЮН ВІТАЛІЙ ПЕТРОВИЧ, САБЕЛЬНИКОВ ЮРІЙ АНДРІЙОВИЧ

(73) ІНСТИТУТ КІБЕРНЕТИКИ ІМ. В.М. ГЛУШКОВА НАН УКРАЇНИ

(56) RU 2298229 C2; 10.06.2006

RU 2212056 C1; 10.09.2003

UA 68459 C2; 15.08.2004

US 2006/0229991 A1; 12.10.2006

GB 2417352 A; 22.02.2006

JP 2003067801 A; 07.03.2003

DE 10325491 A1; 30.12.2004

US 7461787 B2; 09.12.2008

(57) 1. Спосіб електронного голосування, що включає активізацію в процесі голосування в зазначений час електронної системи, генерування одноразових кодів доступу до системи, ідентифікацію суб'єкта волевиявлення (виборця) та отримання ним одноразового коду доступу до системи, який **відрізняється** тим, що до початку голосування за допомогою інформаційно-обчислювальної техніки генерують шифруючі та дешифруючі ключі, зберігають їх з обмеженням правом доступу, записують ці ключі в керуючі шифрувальні пристрої, передають керуючі шифрувальні пристрої до виборчих дільниць і підключають їх до електронних систем голосування, потім в процесі голосування суб'єкт волевиявлення (виборець) в кабіні для голосування на почергові мовні чи індикаційні повідомлення системи вводить в систему код доступу та вводить послідовно номери за списками, на основі цих даних формують результат голосування і повідомляють його суб'єкту волевиявлення (виборцеві) для підтвердження результатів, при непогодженні процес голосування повторюють, а при погодженні цей результат шифрують у вигляді унікального коду, в якому зашифровані дані номери і додаткова інформація, друкують цей результат на паперовому носії у вигляді відкритого рядка введених номерів за списками і зашифрованого коду і знайомлять з цим результатом суб'єкта волевиявлення (виборця), після чого друкований результат голосування приховують для неможливості ознайомлення з ним інших су-

2

б'єктів і зберігають одночасно результат за кожним голосуванням у вигляді відкритого рядка введених номерів за списками і зашифрованих унікальних кодів в електронному вигляді в керуючому шифрувальному пристрої, а код доступу до системи цього суб'єкта волевиявлення (виборця) анулюють, після завершення виборів результати голосування автоматично обраховують, додатково шифрують і передають у центральний виборчий орган.

2. Спосіб за п. 1, який **відрізняється** тим, що перевірку центральним виборчим органом електронних результатів на фальсифікацію голосування виконують автоматично дешифруванням кожного зашифрованого коду, результатом якого є рядок номерів за списками і додаткова інформація, при тотожності дешифрованого і відкритого рядків роблять висновок про відсутність фальсифікації.

3. Спосіб за п. 1, який **відрізняється** тим, що в процесі голосування результат вибору за кожним списком надають в мовному або індикаційному вигляді виборцю, який має можливість відмінити вказаний результат і переголосувати або підтвердити його і продовжити голосування за іншими списками.

4. Спосіб за п. 1, який **відрізняється** тим, що при необхідності перерахунку голосів за паперовими даними, які бачив і підтвердив виборець, за допомогою додаткового сканування здійснюють зчитування результатів голосування, перевірку їх на наявність фальсифікації та перерахунок результатів.

5. Спосіб за п. 1 або 2, який **відрізняється** тим, що перевірку результатів голосування для виявлення фальсифікації на виборчій дільниці виконують шляхом порівняння результатів електронного підрахунку або сканування паперових стрічок з результатами, врахованими центральним виборчим органом.

6. Спосіб за п. 1 або 2, який **відрізняється** тим, що перевірку результатів голосування для виявлення фальсифікації голосування за партію виконують шляхом порівняння результатів електронного підрахунку або сканування паперових стрічок з результатами, врахованими центральним виборчим органом.

7. Спосіб за п. 1 або 2, який **відрізняється** тим, що достовірність голосування кожного виборця виконують порівнянням його сканованого зашиф-

(13) C2

(11) 91920

(19) UA

рованого коду, отриманого ним на виборчій дільниці, з результатами на сайті центрального вибор-

чого органу, де розміщені результати голосування.

Даний винахід належить до інформаційно-обчислювальної техніки і може бути використаний для проведення електронного голосування, електронних виборів, референдумів. Технічним результатом є розширення функціональних можливостей, значне прискорення підрахунку результатів голосування та підвищення надійності, а саме, практично виявити будь-яке несанкціоноване втручання в процес голосування на всіх його етапах.

Відомий спосіб голосування з використанням паперових бюлетенів (див. патент РФ "Способ тайного голосования избирательными бюллетенями" №2153192, 12.11.1999г.) Спосіб пов'язаний з завчасним виготовленням паперових бюлетенів, їх зберіганням, розподілом, доставкою, як документів суворой звітності. Спосіб базується на ручних операціях вводу в паперові бюлетені інформації про волевиявлення шляхом нанесення знаку в одному з визначених місць (квадрату), що відноситься до того з варіантів волевиявлення, по відношенню до якого зроблено вибір.

Основним недоліком способу голосування з використанням паперових бюлетенів є великі часові, організаційні та матеріальні затрати на підготовку та проведення виборів, можливість невірної заповнення суб'єктом волевиявлення паперового бюлетеню для голосування і визнання його волевиявлення дійсним, неможливість виправлення випадкової помилки в процесі голосування, невисока степінь захисту результатів голосування від фальсифікації.

Відомі також способи для таємного голосування (див. патенти РФ "Способ тайного голосования" №2178586, 01.12.1999г., "Способ тайного голосования избирательными бюллетенями" №2178203, 28.04.2001г.). Способи забезпечують прозорість підрахунку голосів та врахування волевиявлення виборців. Але вказані способи мають такі ж недоліки: використання паперових бюлетенів, великі часові, організаційні та матеріальні затрати на підготовку і проведення виборів. До того ж, вказані способи не забезпечують захист від компрометації результатів голосування, більш того дають реальну можливість для компрометації результатів голосування. Крім того, способи не забезпечують автоматизацію підрахунку голосів.

Найбільш близьким до запропонованого способу по технічній сутності і задачі є спосіб електронного голосування (див. патент РФ "Способ электронного голосования, обработка результатов", №2298229, 15.12.2004, опублікований 27.04.2007, бюл. №12). В способі виконують ідентифікацію і реєстрацію суб'єкта волевиявлення, видають електронний засіб ідентифікації, який містить унікальний ідентифікаційний код, вводять указаний засіб ідентифікації в пристрій для голосування, активізують програму голосування, виконують процедуру контрольної перевірки ідентифікаційного коду, при негативному результаті перевірки видають

повідомлення про відмову в голосуванні, при позитивному результаті виконують вибір на зображенні електронного бюлетеня на сенсорному екрані монітора, фіксують результат голосування і засвідчують його електронним цифровим підписом, знищують унікальний код з вказаного засобу ідентифікації і здають його комісії, формують підсумковий протокол, який засвідчують електронним цифровим підписом.

Але цей відомий спосіб теж має недоліки. Спосіб не виключає можливості несанкціонованого втручання в результати голосування, а також виникнення помилок при виконанні перевірки. Це обумовлено наявністю в процесі голосування контакту з електронним бюлетенем при виборі на зображенні електронного бюлетеня на сенсорному екрані монітора при виконанні перевірки.

В основу винаходу, який пропонується, покладена технічна задача створення способу, що дозволить автоматизувати процес голосування для формування і збереження захищених первинних результатів голосування, як в електронному так і в паперовому вигляді з можливістю подальшої (при необхідності) перевірки і перерахунку голосів по первинним документам, виключення або зниження вірогідності можливих фальсифікацій результатів виробів, формування результатів голосування без втручання членів комісії виборчої дільниці.

Поставлена технічна задача вирішується способом електронного голосування, що передбачає при підготовці до голосування за допомогою інформаційно-обчислювальної техніки генерацію шифруючих і дешифруючих ключів, зберігання їх, як документів суворой звітності з обмеженням правом доступу, відповідною службою, запис цих ключів в управляючі шифрувальні пристрої, які не дозволяють зовні ці ключі прочитати, передачу управляючих шифрувальних пристроїв до виборчих дільниць і підключення їх до електронних систем голосування, потім в процесі голосування, в зазначений час, активізацію системи, генерування одноразових кодів доступу до системи, ідентифікацію суб'єкта волевиявлення (виборця) та отримання ним одноразового коду доступу до системи, при цьому суб'єкт волевиявлення (виборець) в кабіні для голосування на почергові мовні чи індикаційні повідомлення вводить код доступу до системи, послідовно номери за списками, на основі цих даних формується результат голосування і повідомляється суб'єкту волевиявлення (виборцеві) для підтвердження результатів, при непогодженні процес голосування повторюється, а при погодженні цей результат шифрується у вигляді унікального коду, в якому зашифровані дані номери і додаткова інформація, друкується на паперовому носії у вигляді відкритого рядка введених номерів за списками і зашифрованого коду, і знайомлять з цим результатом суб'єкта волевиявлення (виборця), після чого друкований результат голосування скривається для неможливості озна-

йомлення з ним інших суб'єктів і зберігається, одночасно результат по кожному голосуванню у вигляді відкритого рядка введених номерів за списками і зашифрованих унікальних кодів зберігається в електронному вигляді в управляючому шифрувальному пристрої, а код доступу до системи цього суб'єкта волевиявлення (виборця) анулюється, після завершення виборів результати голосування автоматично обраховуються, додатково шифруються і відправляються у центральний виборчий орган.

Для ілюстрації запропонованого способу на фіг. 1 приведена блок-схема системи електронного голосування. Система містить персональний комп'ютер 1, зв'язний з одним із входів управляючого шифрувального пристрою 2, другий вхід якого зв'язаний з автоматами 3 для голосування, кожен з яких містить цифрову клавіатуру 4, слухавку 5, блок 6 індикації повідомлень, друкувальний пристрій 7 з вікном 8 перегляду виборцем надрукованого результату голосування, який розташований в закритому і опломбованому контейнері 9 для збереження надрукованих результатів голосування.

Цифрова клавіатура 4 і слухавка 5 може бути виконана на базі телефонного апарату, за допомогою клавіатури якого можна виконувати ввід інформації і надавати мовні інформаційні повідомлення виборцю завдяки наявності телефонного динаміка. Друкувальний пристрій 7 може бути виконаний подібним друкувальним апаратам, що є в мобільних касових апаратах. Це все дозволить скоротити витрати на виготовлення автомату 3 для голосування і зробити його найбільш зрозумілим для виборців. Управляючий шифрувальний пристрій 2 за попередніми оцінками розробників буде недорогим, з малими габаритними розмірами і буде мати можливість перепрограмування для послідовних виборів.

Ключі для шифрування і дешифрування можуть бути індивідуальними для кожної виборчої дільниці. Для підвищення ступеня захисту результату голосування можуть бути додатково зашифровані в цілому.

Слід зазначити, що при реалізації управляючого шифрувального пристрою 2 програмно на персональному комп'ютері 1 залишається загроза зламу програми і розкриття ключа для шифрування, що відкриває шлях до можливих фальсифікацій. При реалізації управляючого шифрувального пристрою 2 у вигляді спеціалізованого пристрою можна забезпечити неможливість розкриття ключів для шифрування і дешифрування.

Електронне голосування відбувається наступним чином.

Член виборчої комісії проводить ідентифікацію виборця по паспортним даним і видає йому код доступу до системи. В системі можна передбачити час дії коду доступу після його видачі. Виборець заходить в кабінку для голосування, де знаходиться автомат 3 для голосування, списки кандидатів (партій) з їх номерами і інформаційним матеріалом, з розрахунку один комплект на кожну кабінку. Виборець піднімає слухавку 5 і прослуховує повідомлення, або слідкує за інформацією на блоку 6 індикації повідомлень. Йому по черзі пропонується

ввести код доступу, номери за списками, а потім повідомляється та показується на блоку індикації повідомлень результат голосування. При помилці результат може бути відмінений і процедура голосування повторюється.

При погодженні, результати голосування друкуються друкувальним пристроєм 7 і виборець їх бачить через вікно 8 у вигляді віддрукованого відкритого рядка введених номерів по спискам і унікального коду, в котрому зашифровані дані номери і додаткова інформація.

У випадку неспівпадіння кодів на блоку індикації і друкувальному пристрої викликається член виборчої комісії, який може впевнитись у збої системи і скласти відповідний протокол.

Після того, як виборець покладе слухавку 5, друкувальний пристрій 7 протягне папір і закрий чергові результати голосування за рамками вікна 8 перегляду, при цьому код доступу виборця до системи анулюється. Опломбований контейнер 9, де розташований друкувальний пристрій 7, виконує роль урни для голосування з вікном 8 для перегляду чергового результату.

Таким чином, результати по кожному голосуванню у вигляді віддрукованого відкритого рядка введених номерів за списками і зашифрованих унікальних кодів зберігаються в електронному вигляді в центральному управляючому шифрувальному пристрої і на паперовому носії.

При закінченні голосування системі дається команда "зачинення", після чого в управляючий шифрувальний пристрій неможливо ввести додатково ніяких результатів, а тільки зчитати в персональний комп'ютер ті, що маютьсся.

Результати голосування в електронному вигляді засобами персонального комп'ютера можуть бути перевірені на предмет фальсифікації відповідними службами, які мають ключі дешифрування. В результаті дешифрування кожного зашифрованого коду повинен бути отриманий рядок номерів за списками і додаткова інформація, яка є в зашифрованому коді для перевірки його на коректність. При не тотожності дешифрованих номерів з відкритими номерами або отриманні не коректної додаткової інформації даний результат зараховується як спотворений.

Результати голосування в електронному вигляді можуть бути розміщені на сайті центрального виборчого органу, що проводить голосування і доступні для перевірки членами комісії виборчих дільниць і спостерігачами, які мають копії первинних результатів голосування в електронному і паперовому вигляді, а також виборцем, який зберіг зашифрований код результатів свого голосування.

Підбір зашифрованого коду по заданому рядку номерів без знання ключа шифрування і дешифрування за обмежений час практично неможливий.

При необхідності додаткової перевірки можливе отримання копії електронного варіанта за рахунок сканування результатів з первинного паперового носія, записи в котрому бачив і підтвердив виборець.

Методи шифрування і дешифрування, котрі пропонується застосувати, є відкритими і достатньо добре у світовій практиці досліджені і відпра-

цьовані. Застосовуються в таких областях як електронний підпис.

При впровадженні такого способу і системи електронного голосування відпадає необхідність у виготовленні захищених бюлетенів для голосування, що дасть економію коштів, котра в деякій мірі компенсує витрати по розробці і впровадженню системи, а багаторазове її використання на виборах різного рівня швидко окупить всі витрати.

Світовий ринок таких систем становить сотні мільярдів доларів, що дає гарні перспективи для України при входженні в нього.

Голосування на будь-якій виборчій дільниці без відкріпних талонів забезпечується за рахунок перевірки прізвища в Державному Реєстрі виборців і виключення його із списків для унеможливлення повторного голосування.

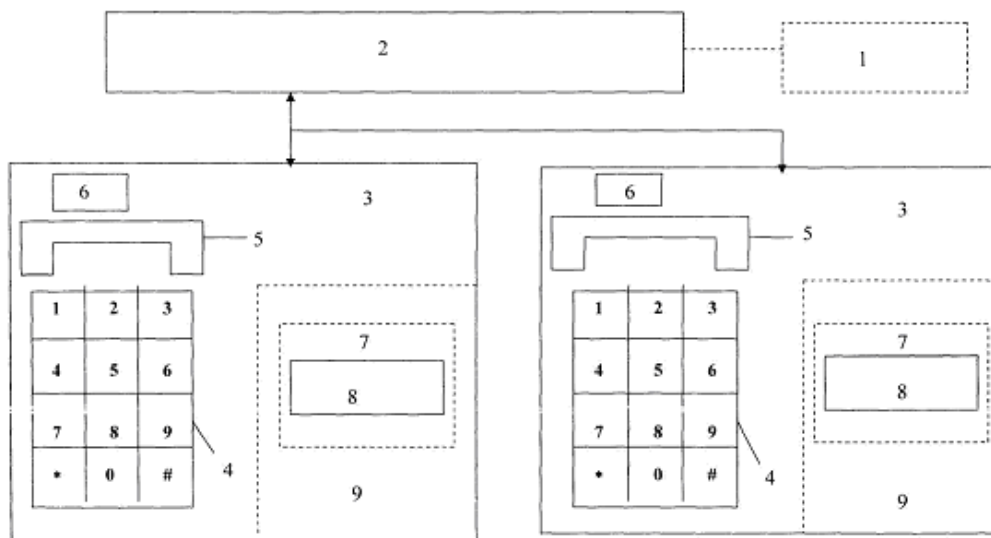


Fig. 1