УДК 004.75

[1]**Вишняков Володимир Михайлович**
Кандидат технічних наук, доцент, доцент кафедри інформаційних технологій
[1]**Пригара Михайло Петрович**
Асистент кафедри інформаційних технологій
[2]**Воронін Олексій Володимирович**
Розробник програмного забезпечення

[1]*Київський національний університет будівництва і архітектури, Київ*
[2]*Самсунг Електронікс Україна, ТОВ*

ВІДКРИТА СИСТЕМА ТАЄМНОГО ГОЛОСУВАННЯ

Анотація. *Проаналізовано міжнародний досвід розробки електронних систем дистанційного голосування з використанням мережі Інтернет. Запропоновано, обґрунтовано та експериментально перевірено основні технічні рішення щодо побудови системи дистанційного голосування в Україні з врахуванням міжнародних вимог та існуючої технології проведення виборів.*

Ключові слова: дистанційне голосування; Інтернет-технології; криптографічні алгоритми

Аннотация. *Проанализирован международный опыт создания электронных систем дистанционного голосования с использованием сети Интернет. Предложены, обоснованы и экспериментально проверены основные технические решения для системы дистанционного голосования в Украине с учетом международных требований и существующей технологии проведения выборов.*

Ключевые слова: дистанционное голосование; Интернет-технологии; криптографические алгоритмы

Abstract. *Existing developments, proposals and requirements of public network direct-recording electronic voting systems were analyzed. There are proposals for the creation of public network direct-recording electronic voting systems including the features of Ukrainian's voting system in this article. The purpose of this creation of this system is the giving more comfortable voting procedure to voters, although while keeping required international conditions for voting. There are presented results of choosing the algorithms and proofs of reliabilities cryptographic techniques. By listening all of the messages on the connection channel almost impossible to figure out who and how was voting. The creation of this system doesn't need any inputs of remarkable objects of financing by getting economical effects from the shortening the quantity of the printed ballots. In created by its authors computer programs for the ensuring the secret of voting were used opened algorithms. It's not needed to keep in a secret the software source. These sources can be totally opened for checks by professionals of cryptography.*

Keywords: Public network direct-recording electronic voting; Internet technologies; Cryptographic algorithms

Постановка проблеми

Завдяки науковим досягненням останніх десятиріч у галузі інформаційних технологій та захисту інформації з'явились можливості для суттєвого вдосконалення систем голосування.

Це вдосконалення може значною мірою підвищити якість зворотного зв'язку в системах державного управління, що являє собою важливу проблему в умовах розвитку демократичного суспільства.

В Україні на дострокових виборах Президента 25 травня 2014 року, майже кожен виборець відчув на собі чимало труднощів під час голосування. Траплялися випадки унеможливлення голосування через довжелезні черги. У східних регіонах через дії терористів багато дільниць навіть не відкрилися. Українські громадяни Криму були вимушені їхати для волевиявлення в сусідню область.

Усі ці труднощі можна подолати шляхом впровадження дистанційного голосування (ДГ), яке не потребує прибуття виборця до дільниці, а для волевиявлення достатньо мати мобільний телефон та доступ до мережі Інтернет.

У даній роботі розглядаються принципи побудови такої системи в Україні.

Слід зауважити, що результати цієї роботи можуть бути корисні не тільки в Україні, бо ця проблема піднімається в багатьох країнах світу.

Аналіз останніх публікацій

Перше легальне голосування за допомогою мережі Інтернет відбулося в Естонії в жовтні 2005 року. Тоді близько одного відсотку виборців скористалось цим засобом. З кожними послідуючими виборами їх кількість зростала і у 2011 році становила майже 25% [1].

За останні 10 років ДГ впроваджувалось також в Англії, Канаді, Мексиці, Польщі, Аргентині, Німеччині, Швеції, Фінляндії та Японії [2]. Ще у багатьох країнах розробляються подібні системи.

В Естонії посвідченням особи є електронна ідентифікаційна карта. Комп'ютери, з яких можна проголосувати повинні мати пристрій для читання таких карт. На сайті можна ознайомитись зі значною частиною вихідних текстів цієї системи [3].

Згідно зі статтею 25 Міжнародного Пакту від 16 грудня 1966 р. "Про громадянські та політичні права", яка регулює міжнародні вимоги до виборів, система голосування повинна забезпечити такі принципи:

1. Загальне виборче право;
2. Рівність прав виборців;
3. Свободу волевиявлення;
4. Таємницю голосування;
5. Безпосередність;
6. Справжність;
7. Періодичність.

Слід вважати, що наявні паперові системи голосування відповідають цим принципам.

Електронні системи співіснують зі старими, поступово замінюючи технології голосування на більш зручні і досконаліші. При цьому на кожному кроці впровадження відбувається ретельна перевірка нових засобів з метою виявлення можливих слабких місць, які можуть стати причиною порушення міжнародних вимог до виборів.

Існуюча в Україні система виборів складається з такої ієрархії комісій:

1. Центральна виборча комісія (ЦВК);
2. Окружні виборчі комісії;
3. Дільничні виборчі комісії.

З квітня 2012 року у ЦВК визначили, що кожна виборча дільниця повинна обслуговувати не більше ніж 2500 виборців. Загальна кількість цих дільниць близько 33 тисяч [4].

Першим важливим кроком в напрямку ДГ в Україні є створення Державного реєстру виборців (ДРВ) [5]. Цей реєстр підтримується в електронному вигляді і дозволяє кожному виборцю створити особистий кабінет в мережі Інтернет.

З досвіду інших країн бачимо, що дозвіл на ДГ надається у період, який передує традиційним виборам. За виборцями, які мали дозвіл на ДГ, але не проголосували залишається право проголосувати за старою технологією.

Важливою вимогою до ДГ є забезпечення таємниці голосів, що потребує комп'ютерного часу на криптографічні перетворення сигналів з метою захисту інформації від прослуховування у каналах зв'язку. Ця вимога за умов великої кількості виборців примушує розподіляти систему на ділянки, кожну з яких буде обслуговувати окремий сервер.

Вузьким місцем у технології ДГ є можливість перевантаження першого сервера, який приймає запити від виборців. Через це в естонській системи період голосування збільшено до тижня, але таке рішення не можна вважати вдалим. В цей період часу ще іде агітація і виборці можуть міняти своє рішення. Для цього надано можливість голосувати багато разів. Зрозуміло, що враховується тільки останній голос. Але такий підхід вимагає запам'ятовувати голоси кожного виборця, що надає принципову можливість їх передивлятись, а це є суттєвим порушенням права виборця на таємницю свого голосу.

Наша система позбавлена цього недоліку.

З точки зору відомого криптолога світу Брюса Шнайера абсолютну гарантію захищеності системи голосування можна досягти тільки за умов повністю відкритого програмного забезпечення [6]. Саме така система пропонується у цій роботі.

Мета статті

Метою даної роботи є надання рекомендацій щодо вибору принципів побудови системи дистанційного голосування в Україні для забезпечення виборців більш зручною процедурою волевиявлення.

Основний матеріал досліджень

Зрозуміло, що ніяка реальна виборча система не може бути повністю позбавлена можливості якихось порушень і зловживань, але будемо вважати неприпустимим за рахунок підвищення зручності погіршити забезпечення міжнародних принципів.

Відомо, що підробка результатів голосування здавна робилась під час підрахунку голосів. У СРСР урни були непрозорі, а підрахунком займались за зачиненими дверима. Результат завжди був маже 100%.

Зараз урни прозорі, підрахунок відкритий, але все одно процедура ручного підрахунку бюлетенів залишається слабким місцем, бо тут є можливості для фальсифікацій через, так званий, людський фактор.

На вищих рівнях ієрархії виборчих комісій майже неможливо фальсифікувати результати. У ЦВК діє електронна система, яка висвітлює на табло підрахунок голосів у реальному часі. Спочатку цей підрахунок базуються на даних, що надходять по каналах зв'язку, а потім уточнюється на основі отриманих документів.

Спроби підробки результатів підрахунку легко виявити, бо це звичайне додавання чисел. А от підробку самих чисел виявити складно. Для цього перераховують бюлетені, але неможливо виявити замінені або спеціально зіпсовані бюлетені.

У випадку дистанційного голосування такі порушення неможливі.

Наведемо та проаналізуємо послідовність дій у системі ДГ:

1. Реєстрація виборця для ДГ.
2. Встановлення дозволу на ДГ у виборах.
3. Ідентифікація та автентифікація виборця за дистанційним зверненням.
4. Надання виборцю можливості голосувати у разі наявності відповідного дозволу.
5. Зарахування результату ДГ та оповіщення про це виборця.
6. Встановлення ознаки використання права голосу, яка блокує дозвіл (див. п. 2).
7. Відправлення результатів голосування у вигляді списків виборців та підсумків голосів.
8. Додавання результатів ДГ у протокол виборчої дільниці.

Розглянемо особливості реалізації кожної дії.

В Україні створено 756 відділків ведення ДРВ, які приймають заяви щодо уточнення даних. Доцільно у цих відділках приймати заяви на ДГ. При цьому порядок реєстрації буде таким.

- Виборець створює особистий кабінет на сайті drv.gov.ua, для чого він вказує адресу електронної пошти, на яку йому надходить відповідь з номером його дільниці (це вже працює). На сайті вказано адреси відділків.
- Виборець особисто подає заяву на ДГ у відділок свого регіону, маючи паспорт і мобільний телефон.
- Представник відділку створює запис про виборця у реєстрі ДГ на сервері відповідної виборчої дільниці.

Зауважимо, що ця реєстрація надає можливість ДГ у всіх наступних виборах до моменту зміни місця проживання або інших змін у ДРВ.

Для ДГ на сервері виборчої дільниці необхідно зберігати номери паспортів та мобільних телефонів для ідентифікації та автентифікації виборців.

Враховуючи, що кількість виборців в Україні значно більше ніж в Естонії, а період ДГ не повинен перевищувати одну добу, в нашій системі діалог виборця розподілено на два етапи, які реалізовано на різних серверах.

Задача першого етапу полягає в пошуку адреси дільничного сервера, який повинен обслуговувати весь подальший діалог виборця.

Діалог виборця із сервером першого етапу слід мінімізувати. Крім того, на цьому етапі необхідно забезпечити можливість паралельного підключення додаткових серверів, щоб зменшити ймовірність відмови в обслуговуванні запитів виборців.

Мінімізований діалог з першим сервером може складатись з єдиного запиту до виборця:

- Введіть номер виборчої дільниці.

Цей номер надається виборцю разом з ім'ям сервера під час реєстрації. Уточнення може бути отримано через особистий кабінет виборця.

У роботі першого сервера немає ускладнень, бо кількість дільниць близько 33 тисяч і знайти адресу сервера виборчої дільниці у відповідній таблиці досить просто. На цю адресу автоматично перенаправляється продовження діалогу виборця.

Можливість підключення додаткових серверів першого етапу практично необмежена. Для цього слід дописати адресу нового сервера у таблицю DNS-сервера. При цьому DNS (система доменних імен) сама буде розподіляти потік запитів виборців рівномірно між серверами.

Діалог виборця на другому етапі (із сервером виборчої дільниці) має бути захищеним, а результат волевиявлення необхідно зберігати в таємниці. Іншими словами, слід побудувати систему так, щоб не існувало можливостей побачити результати волевиявлення виборців, а шифрування діалогу було б на стільки надійним, щоб час на його розкриття змусив відкинути подібні спроби.

Ключова роль у процедурі голосування в нашій системі належить серверам виборчих дільниць.

Однією з можливих загроз в нашій системі є спроба занесення фіктивного виборця у реєстр ДГ, що може бути зроблено тільки співробітником відділку ведення реєстру. Всі дії щодо ведення реєстру ДГ контролюються, але для того, щоб відрізнити реєстрацію дійсного виборця від фальсифікованого, необхідна додаткова перевірка. Таку перевірку можуть якісно виконати найближчі сусіди виборця. В роботі [7] запропоновано зробити відкриту довідку в межах кожної дільниці, де буде вказано тільки кількість виборців по адресах.

Така довідка дозволяє легко виявляти можливі приписки та надавати сигнали для ретельних перевірок.

Дозвіл на ДГ (дія 2) встановлюється під час підготовки дільничних списків виборців окружними комісіями за декілька днів до голосування. У цих списках повинна бути проставлена позначка про заборону на отримання бюлетенів для виборців, яким надано дозвіл на ДГ. У разі неможливості скористатись своїм дозволом на ДГ виборець може через подання заяви до дільниці відмінити цей дозвіл і отримати бюлетень.

Діалог виборця із сервером ДГ має бути захищеним від прослуховування в частині даних, які ідентифікують виборця та його волевиявлення.

Для захисту нами обрано шифр Вернама, який називають *One-time-pad* (одноразовий блокнот). В роботі [8] математично доведено, що цей шифр неможливо розкрити.

Алгоритм шифру Вернама легко зрозуміти.

До кожного біта даних додається випадковий біт, що перетворює дані на випадкові символи. Для розшифрування треба відняти біти, які були додані. Довжина випадкової послідовності повинна бути не менше, ніж довжина даних, що підлягають захисту.

Для реалізації цього алгоритму треба мати дві однакові випадкові послідовності у відправника і одержувача. Немає проблеми створити випадкові послідовності в працюючій програмі, але на різних комп'ютерах послідовності будуть різні. Алгоритм Диффі-Хеллмана дозволяє ці дві різні випадкові послідовності перетворити в однакові шляхом обміну повідомленнями у відкритому для прослуховування каналі [9].

Алгоритм Диффі-Хеллмана базується на задачі дискретного логарифмування, яку описує вираз

$$y=q^x \bmod P,$$

де y, x – цілі числа, що являють собою елементи мультиплікативної групи; q – твірний елемент цієї групи; P – просте число, що означає кількість елементів у групі.

Важливою властивістю цієї задачі є те, що для заданих значень q, P, x існує простий метод обчислення y, а для знаходження x у разі відомих q, P, y не існує простих методів, що для великих значень P унеможливлює розв'язання задачі.

Опишемо процедуру перетворення двох різних випадкових чисел в однакові за допомогою алгоритму Диффі-Хеллмана.

На комп'ютері виборця і сервері ДГ створено таємні випадкові числа a і b відповідно та зроблено відповідні перетворення

$$A=q^a \bmod P,$$
$$B=q^b \bmod P.$$

Числа A та B пересилаються по відкритому каналу зв'язку.

Коли на комп'ютер, там де створено число a, потрапляє число B, обчислюють Z з виразу

$$Z=B^a \bmod P.$$

На сервері, де створено число b, отримавши число A, знаходять число K з виразу

$$K=A^b \bmod P.$$

Легко впевнитись, що $Z=K$, бо

$$Z=q^{ba} \bmod P,$$
$$K=q^{ab} \bmod P.$$

У разі, коли P це велике просте число, числа A та B, які може перехопити зловмисник, не дають можливості обчислити значення Z.

Проблема реалізації цієї процедури полягає в тому, що задача знаходження великих простих чисел належить до класу задач, для яких не існує точних рішень. У системах захисту, які базуються на таких числах, неможливо гарантувати, що числа є дійсно прості. Це надає привід для сумнівів у надійності захисту.

Такі сумніви можна подолати, якщо замість групи з простого числа елементів, використовувати поле Галуа. При цьому потрібні нам властивості алгоритму Диффі-Хеллмана зберігаються.

У стандарті України є рекомендовані варіанти полів Галуа [10], один з яких було обрано для захисту даних в нашій системі ДГ. Обраний варіант поля Галуа $GF(2^{503})$ з примітивним поліномом $x^{503} + x^3 + 1$ дозволяє перетворювати двійкові числа довжиною 503 біти (62 алфавітно-цифрових символи). Цього цілком достатньо для шифрування повідомлень, які потребують захисту у нашій системі ДГ. До таких повідомлень слід віднести номер паспорта виборця, пароль та обрані ним варіанти голосування, що разом не можуть перевищувати пару десятків символів. При цьому час на криптографічні перетворення, які реалізовано у нашій системі ДГ на мові програмування *JavaScript*, не перевищує секунду.

Вважаючи, що дані, які необхідно зберегти в таємниці, не виходять за межі діючої програми, куди не існує зовнішнього доступу, єдиний шлях розкриття таємниці – логарифмування над полем Галуа $GF(2^{503})$. Далі проаналізуємо цей шлях.

Найбільш повний порівняльний аналіз методів дискретного логарифмування надано у роботі [11]. Найкращий результат логарифмування над полями $GF(2^n)$ подібного розміру отримано в роботі [12] за допомогою алгоритмів Копперсмита та Відемана, що потребувало місяців комп'ютерного часу.

При цьому сказано, що у разі збільшення степеня *n* до 1000, реалізувати цей метод практично неможливо. Слід зауважити, що у нашій системі ДГ збільшення степеня *n* до тисячі збільшить час на криптографічні перетворення всього до декількох секунд.

Зрозуміло, що в сучасних умовах місяці і навіть години комп'ютерного часу для розкриття голосу кожного виборця витрачати абсолютно недоцільно. Таким чином можна вважати нашу систему ДГ достатньо захищеною і такою, що має можливість посилення захисту на майбутні часи.

Після формування однакових випадкових чисел на сервері і комп'ютері виборця у захищеному вигляді пересилається номер паспорта. Таким чином унеможливлюється розкриття особи виборця. Для автентифікації використано широко відомий метод, який і успішно працює у системі Приват-24. А саме, на мобільний телефон виборця відправляємо СМС з кодом, який повинен ввести виборець. Цей код також відправляється у захищеному вигляді, щоб у разі прослуховування мобільного зв'язку, не можна було встановити місце знаходження виборця у мережі. Далі виборець отримує один або декілька електронних бюлетенів для голосування. Результати голосування також пересилаються захищеними.

Програма на дільничному сервері одночасно може підтримувати діалог з десятками виборців. Цю програму запускають на початку голосування і вона знаходиться в стадії виконання до моменту закінчення голосування. У цій програмі формуються підсумки результатів голосування по кожному виду бюлетенів. Крім цих підсумків ніякі інші дані на виході програми не з'являються. Під час роботи програма звертається до файлів з даними про виборців та з формами електронних бюлетенів.

Після ідентифікації та автентифікації особи виборця на сервері встановлюється інтервал часу для очікування результату волевиявлення. Цей результат одразу після розшифрування додається до підсумку. Ніде не залишається слідів про те, як само, проголосував даний виборець. Після цього у файлі даних встановлюється ознака використання права голосу і відправляється відповідне повідомлення. Це повідомлення дублюємо за допомогою СМС, щоб у разі відмови Інтернет-зв'язку виборець отримав інформацію про успішне завершення голосування.

Відповідальний представник дільничної комісії має можливість на підставі заяви виборця про відмову від дистанційного голосування отримати доступ до сервера своєї дільниці для перевірки наявності та зняття дозволу на ДГ, після чого виборцю може надаватись друкований бюлетень.

В момент завершення періоду голосування на сервері формується файл з підсумками результатів по кожному з бюлетенів. На цьому закінчується робота основної серверної програми.

Остаточним результатом роботи дільничного сервера є видача таких документів:

- список виборців, які проголосували дистанційно;
- список виборців, які мали право на ДГ, але не проголосували;
- результати ДГ по кожному виду бюлетенів.

За цими документами представники дільничної комісії повинні додати результати ДГ у протокол підрахунку голосів.

Впровадження розглянутої системи ДГ не потребує суттєвих економічних витрат, бо у більшості випадків воно являє собою встановлення додаткових програмних засобів на вже наявні комп'ютери. Обрана технологія ДГ, легко вбудовується в наявну виборчу систему України. При цьому після реєстрації виборців для ДГ можна зменшувати кількість друкованих бюлетенів, що дає одразу вагомий економічний ефект.

Висновки

У роботі надано пропозиції щодо створення системи дистанційного голосування з врахуванням особливостей виборчої системи України з метою забезпечення виборців більш зручною процедурою волевиявлення за умов дотримання міжнародних вимог до виборів.

Впровадження системи може відбуватись без вкладання значних обсягів фінансування за рахунок поступового отримання економічного ефекту від скорочення випуску друкованих бюлетенів.

Розроблені авторами комп'ютерні програми для забезпечення таємниці волевиявлення виборців побудовані з використанням виключно відкритих алгоритмів, що не потребує збереження в таємниці вихідних текстів програмного забезпечення і вони можуть бути повністю відкриті для перевірок фахівцями з криптографії.

Список літератури

1. Электронное голосование в Эстонии [Електронний ресурс] –http://ru.wikipedia.org/wiki/Электронное_голосование_в_Эстонии

2. Антонов Я. Международный опыт электронного голосования [Електронний ресурс] –http://www.akademia.edu/4680647/_2

3. E-hääletamise tarkvara [Електронний ресурс] – https://github.com/vvk-ehk/evalimine

4. ЦВК визначилася з виборчими дільницями [Електронний ресурс] –http://www.unian.ua/politics/636023-tsvk-viznachilasya-z-viborchimi-dilnitsyami.html.

5. Державний реєстр виборців [Електронний ресурс] – https://www.drv.gov.ua

6. Unusual Electronic Voting Machine Threat Model [Електронний ресурс] – https://www.schneier.com/blog/archives/2014/05/unusual_electro.html.

7. Проверяемое электронное голосование [Електронний ресурс] –http://habrahabr.ru/post/156423

8. C.E.Shannon. The Communication Theory of Secrecy Systems // Bell System Technical Journal. – 1949 – v.28, n.4 – C.654-715.

9. W.Diffie, M.E.Hellman. New Direction in Cryptography // IEEE Transactions on Information Theory. – 1976 – v.IT-22, n.6. – C. 644-654.

10. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – Чинний з 01.07.2003.

11. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии/ О.Н.Василенко. – М.: МЦНМО, 2003. – 328 с.

12. Thome E. Computation of discrete logarithms in GF(2^{607}) // Advances in Cryptology-AsiaCript'2001. 2001. (Lect. Notes in I. Comput. Sci.; V. 2248). P. 107 – 124.

References

1. The electronic voting in Estonia. [electronic resource]. –http://ru.wikipedia.org/wiki/Электронное_голосование_в_Эстонии

2. Antonov, J. International experience of electronic voting. [electronic resource] –http://www.akademia.edu/4680647/_2

3. E-voting software [electronic resource] – https://github.com/vvk-ehk/evalimine

4. Central Election Commission decided on the polling station [electronic resource] –http://www.unian.ua/politics/636023-tsvk-viznachilasya-z-viborchimi-dilnitsyami.html.

5. State Voter Register [electronic resource] – https://www.drv.gov.ua

6. Unusual Electronic Voting Machine Threat Model [electronic resource] – https://www.schneier.com/blog/archives/2014/05/unusual_electro.html.

7. Verifiable electronic voting [electronic resource]. – http://habrahabr.ru/post/156423

8. Shannon, C.E. (1949). The communication theory of secrecy systems // Bell System Technical Journal, 28, n.4654-715.

9. Diffie, W.M. & Hellman, E. (1976). New Direction in Cryptography // IEEE Transactions on Information Theory, .IT-22, n.6, 644-654.

10. DSTU 4145-2002. Information technology.Cryptographic techniques.Digital signatures based on elliptic curves.Generation and verification. – Valid from 01.07.2003.

11. Vasilenko, O.N., (2003). Number-theoretic algorithms in cryptography. Moscow, Russia: MCNMO, 328.

12. Thome, E. (2001). omputation of discrete logarithms in GF(2607) // Advances in Cryptology-AsiaCript'2001. Lect. Notes in I. Comput. Sci., 2248, 107 – 124.

Стаття надійшла до редколегії 30.10.2014

Рецензент: д-р техн. наук, проф. Г.Ф.Конахович, Національний авіаційний університет, Київ.