Тригуб Р. О., Тригуб О. С., Горборуков В. В.

ПРОГРАМНА СИСТЕМА ДОСЛІДЖЕННЯ СЛАБОСТРУКТУРОВАНИХ ЗАДАЧ БАГАТОКРИТЕРІАЛЬНОЇ ОПТИМІЗАЦІЇ

Розроблено систему підтримки прийняття оптимальних рішень при розв'язанні слабоструктурованих задач багатокритеріальної оптимізації, яка може бути корисна особам чи колегіальним органам, що приймають відповідальні рішення. Існуючі на сьогодні програмні системи, які розв'язують такого класу задачі, обмежуються лише пошуком найкращої альтернативи, тоді як запропонована система також (крім вирішення цієї задачі) дозволяє розробити інструкції («настанови до дій») для будь-якої альтернативи, що програла, дотримання яких гарантуватиме даній альтернативі перемогу.

Ключові слова: слабоструктуровані задачі, багатокритеріальна оптимізація, метод аналізу ієрархій, критерії, альтернативи.

Матеріал надійшов 25.06.2013

УДК 004.946

Анісімова Л. А.

ПРОТОКОЛИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

У статті розглянуто основні положення концепції електронного уряду, протоколи електронного голосування та проаналізовано їх щодо надійності та можливості програмної реалізації і впровадження.

Ключові слова: електронний уряд, електронне голосування, протоколи електронного голосування, програмні системи підтримки електронного уряду.

Вступ

Наразі системи підтримки електронного уряду є важливою складовою комунікації урядових структур та громадян держави. Зростає зацікавленість України у пришвидшенні донесення інформації до її громадян і підвищенні надійності спілкування. Прикладом є впровадження електронного оподаткування та подачі податкових звітів [1].

Важливою складовою у системі електронного уряду є електронне голосування. Хоча про системи віддаленого голосування почали говорити відносно недавно (можна сказати, що ця галузь є надбанням XXI ст.), але вони стрімко набирають популярності як у бізнесі, так і в урядових структурах. Однак існує низка суттєвих відмінностей між вимогами до проектування корпоративних систем голосування та систем голосування загальнодержавного масштабу. Основними критеріями, з одного боку, є підвищені вимоги до захищеності такої системи, а з іншого – забезпечення конституційних прав громадян таємниці голосування. Відомі приклади застосування інтернет-голосування для проведення регіональних та загальнодержавних виборів. У 2007 році Естонія провела перші парламентські вибори, де електронне голосування прирівнювалось до традиційного голосування на виборчій дільниці.

Метою цієї роботи є огляд протоколів електронного голосування і криптографічних методів та їх аналіз щодо застосування в реальних умовах.

Електронний уряд

Термін «Електронний уряд» (E-Government, electronic government, digital government, online government) означає використання інтернет-технологій в якості платформи обміну інформації, надання послуг і ведення справ з громадянами, бізнесом, іншими гілками влади / уряду. Електронний уряд може бути застосовано законодавчою владою, судовою і будь-якою іншою для того, щоб підвищити внутрішню ефективність, пов'язану з якістю управління та організації, забезпечення комунальних послуг чи процесів демократичної форми правління. Основними на сьогодні моделями є Government-to-Customer (G2C), Government-to-Business (G2B), Government-to-Government (G2G) та Government-to-Employees (G2E). У кожній з цих сфер взаємодії присутні чотири типи діяльності:

- поширення інформації засобами Інтернет;
- взаємний обмін між відомствами та громадянами, бізнес-структурами чи іншими державними організаціями;
- ведення транзакцій (депонування податкових декларацій);
- управління (он-лайн голосування, проведення кампаній).

До найсуттєвіших переваг електронного уряду можна віднести: підвищену продуктивність, зручність і доступність забезпечення суспільних некомерційних послуг.

Останнім часом його розглядають швидше як концепцію, спрямовану на підвищення ефективності діяльності держави в цілому. Програмні системи підтримки електронного уряду (ПСПЕУ) традиційно містять вільний доступ громадян до державної інформації, переведення державних установ на безпаперове діловодство, встановлення для всіх державних установ показників ефективності роботи на рік і регулярний їх контроль, що проводиться як парламентом, так і громадянами, введення у державних установах пластикових карт для ідентифікації державних службовців, перерахування їм коштів. Зрозуміло, що ПСПЕУ це система державного управління на основі електронних засобів обробки, передачі і розповсюдження інформації. Її базову структуру відображено на рис. 1.

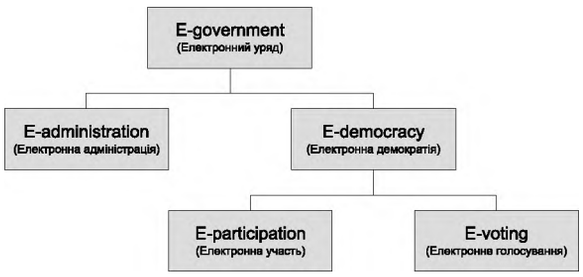

Рис. 1. Структура ПСПЕУ

Електронне голосування

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.

Електронні урни – спосіб голосування за допомогою спеціалізованих машин в обладнаних для цього дільницях під наглядом урядових працівників. Виборці здійснюють свій вибір електронно (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 уможливлює голосування із будь-якого місця у зручний для виборця час [2; 3].

Ескіз загальної системи інтернет-голосування зображено на рис. 2. На дільницях клієнтом є термінал – електронна урна. Для віддаленого інтернет-голосування це буде комп'ютер вдома чи на робочому місці. Клієнти підключаються до локальних Інтернет-провайдерів і до провайдерів серверної сторони за допомогою Інтернет. Серверна частина складається із двох підсистем: бути обмежень щодо місцезнаходження виборця. Виборчі системи повинні працювати надійно, без втрати будь-яких голосів, незважаючи на можливі численні збої проміжного обладнання чи втрату інтернет-зв'язку. Зрозуміло, що система повинна передбачати комплекс захисних дій щодо зловмисного коду чи шпигунських програм з боку клієнта [2].

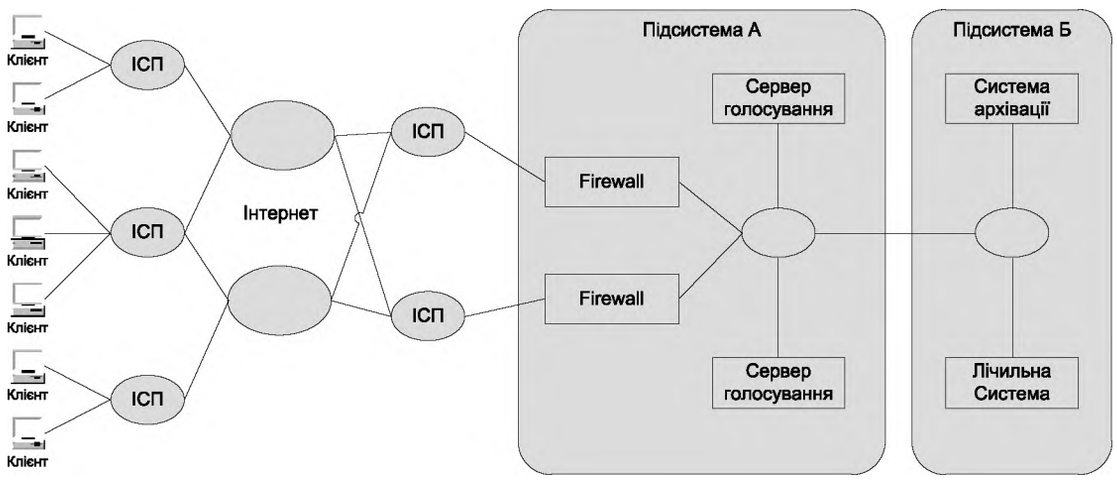

Рис. 2. Ескіз загальної системи інтернет-голосування

Підсистеми А, яка відповідальна за збір зашифрованих бюлетенів, та Підсистеми Б, яка дешифрує бюлетені, підраховує та архівує голоси, генерує результати.

Система інтернет-голосування повинна задовольняти низці критеріїв як-от: демократичність, приватність, цілісність, зручність, верифікованість і доступність, мобільність і надійність [3]. Лише авторизовані виборці можуть брати участь у виборах. Голосування можливе лише раз для кожного виборця. Ніхто не може зробити копію чийогось бюлетеня. Ніхто не може прослідкувати волевиявлення конкретного виборця. Жоден із виборців не може довести, що він проголосував тим чи іншим чином. Неможливо змінити, підмінити, знищити бюлетень виборця. Усі дійсні голоси повинні враховуватись у кінцевому підрахунку. Недійсні бюлетені не можуть враховуватись при підрахунку. Голосування повинно здійснюватися швидко, не вимагаючи від виборців спеціальних вмінь чи значних апаратних ресурсів. Обладнання для голосування повинно підтримувати різні формати питань (введення кандидатів, опитування, підтримка мов); бути сумісним із різними стандартними платформами і технологіями; доступним людям із фізичними вадами. Має бути можливість перевірити чи всі бюлетені коректно враховані при підрахунку і не повинно

Вразливість систем віддаленого голосування

Комп'ютерні системи вразливі до атак у трьох ключових вузлах: сервер, клієнт і канал зв'язку. Атаки, пов'язані із проникненням, націлені на безпосередньо серверні та клієнтські компоненти, тоді як атаки DoS-типу (Denial of Service) спрямовані на погіршення або повне виведення із ладу каналу зв'язку між ними.

В інсайдерських атаках застосовується механізм умисного завантаження на цільовий хост зловмисної програми у формі «троянського коня» або програми віддаленого контролю. При запуску вона може шпигувати за бюлетенями, перешкоджати виборцям здійснювати голосування або, що найгірше, змінювати вміст бюлетеня. Особливої підступності надає програмі те, що її може бути запущено на виконання без шансу на виявлення; а такі механізми забезпечення безпеки, як шифрування та аутентифікація (наприклад, SSL і захищений гіпертекстовий транспортний протокол https), оскільки рівень абстракції ворога є нижчим за своїм функціонуванням. Антивірусне програмне забезпечення виявляється безсилим проти такої атаки, бо механізми розпізнання, як правило, шукають відомі сигнатури або відслідковують інші ознаки неправомірних дій.

Ці приховані атаки, як правило, надходять від невідомих чи змінених програм. Вони переробляють системні файли, щоб можна було ефективно «авторизувати» зміни, які було зроблено самими (після чого може бути крадькома відключений захист від вірусів).

Канал зв'язку є каналом між клієнтом-виборцем та сервером (де проводиться підрахунок голосів). Під час віддаленого голосування цьому каналу слід довіряти, він має бути надійним під час передачі голосів. Хоча поточні криптографічні технології, наприклад інфраструктура ключів, достатні для забезпечення безпеки спілкування при передачі голосів (за умови, що дотримано необхідних стандартів), однак гарантувати самого зв'язку неможливо. Найбільшою загрозою в цьому відношенні є атаки відмови в обслуговуванні (DoS), яка передбачає використання одного чи більше комп'ютерів для переривання зв'язку між клієнтом та сервером шляхом переповнення буфера сервера надмірною кількістю запитів. Впродовж усієї атаки зв'язок із сервером дуже обмежений або взагалі відсутній. Удосконалення цієї техніки полягає у розподіленій відмові в обслуговуванні (DDoS, Distributed Denial of Service), коли програми, які називаються *демонами*, встановлюються на багатьох комп'ютерах без відома їх власників (шляхом використання будь-якого механізму передачі, про які зазначено вище), і використовуються для атаки (рис. 3). Таким чином зловмисник може цілеспрямовано надсилати запити з багатьох комп'ютерів для виведення із ладу сервера.

На сьогодні не існує способу запобігти DoS-атаці чи зупинити її під час дії без переривання зв'язку. Незважаючи на те, що проводиться дослідження для пошуку способів обмеження цієї загрози, не визначено жодного вирішення даної проблеми.

Рис. 3. Схема DDoS-атаки

При голосуванні за допомогою електронних урн можливе уникнення цих загроз шляхом надання можливості клієнтам працювати навіть у випадку, коли зв'язок між зоною виборця та сервером втрачений без попередження і на даний момент недоступний. Відповідно, ці системи повинні переходити у режим прямого запису, а при відновленні зв'язку продовжувати передачу голосів без втрати жодного. Такі системи голосування не вразливі до DoS-атак.

Протоколи таємного голосування

Як уже зазначалося, комп'ютерне голосування неможливо застосувати для звичайних виборів, доки не існує протоколу, який одночасно оберігає від шахрайства і захищає таємницю особи. Ідеальний протокол повинен містити такі властивості: голосування можливе лише для тих, хто має на це право; кожен може голосувати не більше одного разу; ніхто не може дізнатись, за кого проголосував конкретний виборець; ніхто не може проголосувати замість іншого (це виявляється найскладнішою вимогою); ніхто не може таємно змінити чийсь голос; кожен виборець може перевірити, чи його голос враховано при проведенні підсумків виборів. Окрім того, для деяких схем голосування може знадобитися додаткова вимога: кожен знає, хто брав участь у голосуванні, а хто ні.

Концепції для впровадження електронного голосування базуються на криптографічних процедурах. У цьому руслі фундаментальними є праці Діффі та Хеллмана щодо асиметричного шифрування і Рівеста, Шаміра, Адлмана щодо цифрового підпису і систем відкритого ключа.

Спрощені протоколи голосування

Розглянемо спрощені протоколи голосування та пов'язані з цим проблеми. Найпростіший протокол голосування виглядатиме таким чином:

1) кожний виборець шифрує свій бюлетень відкритим ключем Центральної виборчої комісії (ЦВК);
2) виборець відправляє свій бюлетень до ЦВК;
3) ЦВК розшифровує бюлетені, підводить підсумки і опубліковує результати голосування.

Цей протокол має недоліки. ЦВК не може дізнатися, звідки отримано бюлетені, і навіть чи належать надіслані бюлетені виборцям. У неї немає можливості визначити, чи не голосували виборці більше одного разу. Позитивною стороною є неможливість змінити бюлетень іншої людини, але ніхто і не намагатиметься це зробити, тому що набагато простіше голосувати повторно, добиваючись потрібних результатів виборів.

Розглянемо наступний протокол:

1) виборець підписує свій бюлетень власним закритим ключем;
2) виборець шифрує свій бюлетень відкритим ключем ЦВК;
3) виборець посилає свій бюлетень до ЦВК;
4) ЦВК розшифровує бюлетені, перевіряє підписи, підводить підсумки і опубліковує результати голосування.

Цей протокол задовольняє таким властивостям. Тільки законні виборці можуть голосувати, і ніхто не може голосувати більше одного разу, ЦВК може записувати бюлетені, отримані на етапі (3). Кожен бюлетень підписаний закритим ключем виборця, тому ЦВК знає, хто голосував, а хто ні, і як голосував кожен виборець. Якщо отриманий бюлетень не підписано законним користувачем, або бюлетень підписано виборцем, який вже проголосував, то такий бюлетень ігнорується комісією. Крім того, через цифровий підпис ніхто не може змінити бюлетень іншого виборця, навіть якщо вдасться перехопити його на етапі (2).

Проблема цього протоколу в тому, що оскільки підпис додається до бюлетеня, ЦВК знає, хто за кого голосував. Шифрування бюлетенів відкритим ключем ЦВК заважає стороннім зловживати протоколом і дізнаватися, хто за кого голосував, але громадянам доведеться абсолютно довіряти ЦВК. Виходом тут є розділення повноважень ЦВК. Матимемо наступний протокол. Крім сутності, що відповідає за генерацію та поширення ключів, нам необхідний адміністратор, який відповідає за підтримку списку виборців, і колектор, який збирає та підраховує голоси.

Усі наділені повноваженнями інстанції (виборець, адміністратор і колектор) отримують пару закритого і відкритого ключів. Колектор також отримує ідентифікатор, з яким він зіставляється у списку виборців. Виборець заповнює свій бюлетень і кодує його відкритим ключем колектора, потім підписує його (своїм закритим ключем). Разом зі своїм ідентифікатором він кодує його відкритим ключем адміністратора. Адміністратор отримує це повідомлення і розкодовує його своїм закритим ключем (він єдиний, хто знає цей ключ), таким чином отримуючи ідентифікатор виборця. Він також має встановити автентичність повідомлення. Це є можливим з використанням відкритого ключа виборця, що зіставляється із цим ідентифікатором. Важливо зазначити, що адміністратор не може прочитати вміст бюлетеня. Він зашифрований відкритим ключем колектора. Насамкінець адміністратор підписує цей зашифрований бюлетень своїм закритим ключем, чим дозволяє колектору перевірити відправника (адміністратора). Знаючи відкритий ключ адміністратора і свій власний закритий ключ, колектор отримує (анонімний) голос.

Очевидно, що така процедура має певні недоліки: адміністратор може знищувати та додавати голоси, колектор може змінювати, знищувати та додавати голоси, а за умови змови вищезгаданих осіб таємність голосування гарантувати неможливо. Щодо таємного голосування, то довіра до адміністратора і колектора необхідна. Якщо проектувати систему, яка працює незалежно від нашої довіри, то все буде набагато складніше, і постане вимога використання сліпих підписів та анонімних каналів зв'язку.

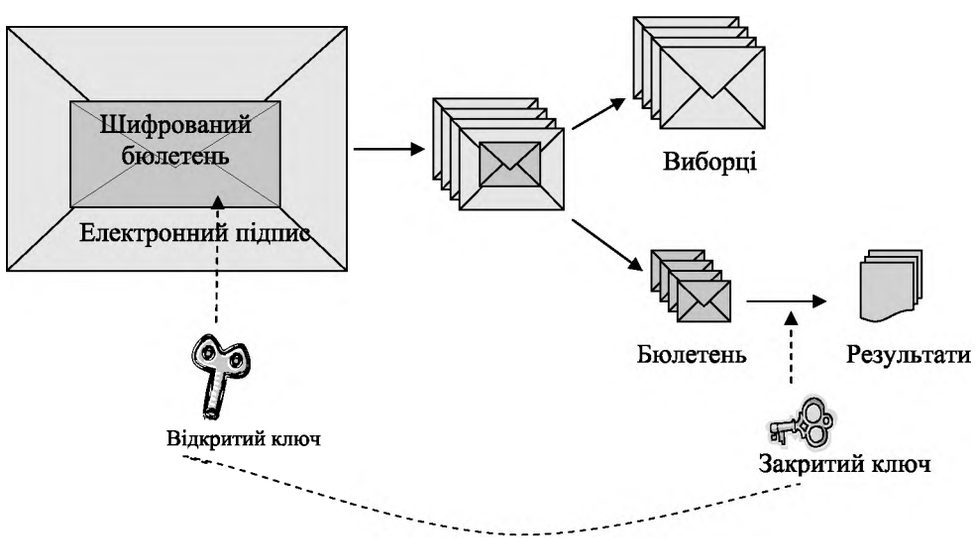

Рис. 4. Удосконалений протокол

Необхідно відокремити бюлетень від виборця, зберігши при цьому процедуру ідентифікації особи (рис. 4).

1. Кожен виборець створює 10 наборів повідомлень. Кожен набір містить правильний бюлетень для кожного можливого результату (наприклад, якщо бюлетенем є одна з відповідей «так» - «ні», то кожен набір складається з двох бюлетенів, один для «так», а другий для «ні»). Кожне повідомлення містить також випадковим чином створений ідентифікаційний номер, достатньо великий, щоб уникнути плутанини з іншими виборцями.
2. Кожен виборець особисто маскує всі повідомлення і посилає їх у ЦВК разом з множниками маскування.
3. ЦВК у своїй базі даних перевіряє, що користувач не надсилав раніше для підписання свої замасковані бюлетені. ЦВК відкриває 9 з 10 наборів, перевіряючи, що вони правильно сформовані. Потім індивідуально підписує кожне повідомлення набору і відсилає виборцеві, зберігаючи ім'я виборця у своїй базі даних.
4. Виборець знімає маскування з повідомлень і отримує набір бюлетенів, підписаних ЦВК. (Ці бюлетені підписані, але не зашифровані, тому виборець легко побачить, який з бюлетенів – «так», а який – «ні».)
5. Кожен виборець вибирає один з бюлетенів і шифрує його відкритим ключем ЦВК.
6. Виборець відправляє свій бюлетень.
7. ЦВК розшифровує бюлетені, перевіряє підписи, перевіряє у базі даних унікальність ідентифікаційного номера, зберігає послідовний номер і підводить підсумки. Після чого опубліковує результати голосування разом з кожним послідовним номером і відповідним бюлетенем.

Виборець-шахрай не зможе обдурити цю систему. Протокол сліпого підпису забезпечує унікальність кожного поданого бюлетеня. Якщо він спробує відправити той же бюлетень двічі, ЦВК виявить дублювання послідовних номерів на етапі (7) і не враховуватиме другий бюлетень. Якщо він спробує отримати декілька бюлетенів на етапі (2), ЦВК виявить це на етапі (3). Шахрай не може створити свої власні бюлетені, тому що не знає закритого ключа комісії. З тієї ж причини він не може перехопити і змінити чужі бюлетені.

Протокол на етапі (3) повинен забезпечити унікальність бюлетенів. Без цього етапу шахрай міг би створити таку саму послідовність бюлетенів, за винятком ідентифікаційного номера, і завірити їх у ЦВК, яка не зможе дізнатися, як голосував конкретний виборець. Оскільки протокол сліпого підпису маскує послідовні номери бюлетенів до моменту підбиття підсумків, ЦВК не зможе установити зв'язок між підписаним нею замаскованим бюлетенем і бюлетенем, який враховується при проведенні підсумків. Опублікування переліку послідовних номерів і пов'язаних з ними бюлетенів дозволяє користувачам переконатися, що їх бюлетені були правильно враховані. Але проблеми ще залишаються. Якщо етап (6) не анонімний і ЦВК може записати, хто який бюлетень прислав, то зможе і дізнатися, хто за кого голосував. Проте це неможливо, якщо комісія отримує бюлетені в запечатаній урні для голосування і рахує їх пізніше. Хоча ЦВК і не вдасться встановити зв'язок між виборцями і їх бюлетенями, але вона зможе створити велику кількість підписаних і правильних бюлетенів і зшахраювати, приславши їх сама собі. І якщо виборець виявить, що ЦВК підмінила його бюлетень, вона не доведе цього.

Голосування з двома Центральними комісіями

Одним з рішень є розділити ЦВК навпіл. Жодна з них не матиме достатньо влади, щоб зшахраювати на свій розсуд.

У наступному протоколі використовується Центральне управління реєстрації (ЦУР), що займається перевіркою користувачів, і окрема ЦВК для підрахунку бюлетенів [4].

1. Кожен виборець відправляє лист до ЦУР, запитуючи реєстраційний номер.
2. ЦУР повертає виборцеві випадковий реєстраційний номер, веде список реєстраційних номерів. Крім того, ЦУР зберігає список одержувачів реєстраційних номерів на випадок, якщо хтось спробує проголосувати двічі.
3. ЦУР відправляє список реєстраційних номерів до ЦВК.
4. Кожен виборець вибирає випадковий ідентифікаційний номер, створює повідомлення з цим номером, реєстраційним номером, отриманим в ЦУР, і своїм бюлетенем. Він посилає це повідомлення до ЦВК.
5. ЦВК перевіряє реєстраційні номери за списком, отриманим від ЦУР на етапі (3). Якщо реєстраційний номер є у списку, ЦВК викреслює його (щоб уникнути повторного голосування). ЦВК додає ідентифікаційний номер до списку тих, хто проголосував за певного кандидата, і додає одиницю до відповідного підсумкового числа.

6. Після того, як усі бюлетені буде отримано, ЦВК публікує результати разом із списками, що містять ідентифікаційні номери і відповідні бюлетені.

Як і в попередньому протоколі кожен виборець може побачити список ідентифікаційних номерів і знайти у ньому свій власний. Так він переконається, що його бюлетень враховано. Звичайно, всі повідомлення, якими обмінюються учасники протоколу, повинні бути зашифровані і підписані, щоб перешкодити зловмиснику видати себе за іншого або перехопити повідомлення.

ЦВК не може змінити бюлетені, тому що кожен виборець шукатиме свій реєстраційний номер. Якщо виборець не знаходить свій реєстраційний номер або знаходить його в підсумковому списку з іншим результатом голосування, він одразу дізнається, що відбувся обман. ЦВК не може додати бюлетень в урну, яка знаходиться під спостереженням ЦУР. Натомість ЦУР відомо, скільки виборців реєструвалося, їх реєстраційні номери і виявить будь-які зміни.

Шахрай, що не володіє виборчими правами, може спробувати зшахраювати, вгадавши правильний реєстраційний номер. Загроза цього може бути мінімізована, якщо кількість можливих реєстраційних номерів набагато більша, ніж кількість реальних реєстраційних номерів: 100-бітове число для мільйона виборців. Звичайно ж, реєстраційні номери повинні генеруватися випадковим чином.

Не дивлячись на це, ЦУР повинна бути органом влади, **який викликає і задовольняє довіру**, адже вона може зареєструвати незаконних виборців. Вона також може зареєструвати законних виборців кілька разів. Цей ризик можливо звести до мінімуму, якщо ЦУР опублікує список зареєстрованих виборців (але без їх реєстраційних номерів). Якщо число виборців у цьому списку менше, ніж число підрахованих бюлетенів, то викликає підозру. Проте якщо зареєстровано більше виборців, ніж надійшло бюлетенів, то це може означати, що деякі зареєстровані виборці не скористалися правом волевиявлення. Цей протокол беззахисний перед змовою ЦВК і ЦУР. Якщо вони діють разом, то можуть об'єднати свої бази даних і дізнатися, хто за кого голосує.

Голосування з однією Центральною комісією

Щоб уникнути небезпеки змови між ЦУР і ЦВК можна використовувати складніший протокол. Цей протокол ідентичний попередньому з двома змінами: ЦУР і ЦВК – єдина організація, і для анонімного розподілу реєстраційних номерів на етапі (2) використовується операційна система ANDOS. Оскільки протокол анонімного розподілу ключів не дозволяє ЦВК дізнатися, у якого виборця який реєстраційний номер, у ЦВК немає способу зв'язати реєстраційні номери і отримані бюлетені. Але ЦВК повинна бути надійним органом, щоб не видавати реєстраційних номерів незаконним виборцям. Цю проблему також можна вирішити за допомогою сліпих підписів.

Покращений протокол голосування з однією ЦВК: у цьому протоколі також використовується ANDOS. Він задовольняє усім шести вимогам надійного протоколу голосування. Він не задовольняє сьомій вимозі, але володіє двома властивостями:

7. Виборець може змінити свою думку (анулювати свій бюлетень і проголосувати знову) протягом заданого періоду часу.
8. Якщо виборець виявляє, що його бюлетень порахований неправильно, він може встановити і виправити проблему, не ризикуючи безпекою свого бюлетеня.

Покращений протокол голосування з однією Центральною комісією

Покращений протокол голосування з однією ЦВК:

1. ЦВК публікує список усіх виборців, які мають право брати участь у голосуванні.
2. Протягом певного терміну кожен виборець повідомляє до ЦВК, чи планує він голосувати.
3. ЦВК публікує список виборців, що беруть участь у виборах.
4. Кожен виборець отримує ідентифікаційний номер I за допомогою протоколу ANDOS.
5. Кожен виборець генерує пару відкритий/закритий ключ: k, d. Виборець створює і посилає до ЦВК таке повідомлення: $I,E_k(I,v)$, де v – бюлетень. Це повідомлення посилається анонімно.
6. ЦВК підтверджує отримання бюлетеня, публікуючи $E_k(I, v)$.
7. Кожен виборець посилає ЦВК: I, d.
8. ЦВК розшифровує бюлетені. В кінці виборів вона публікує результати і, для кожного варіанта вибору, список відповідних значень $E_k(I, v)$.
9. Якщо виборець виявляє, що його бюлетень підрахований неправильно, він протестує, посилаючи до ЦВК: $I, E_k(I, v), d$.
10. Якщо виборець хоче змінити свій бюлетень з v на v', він посилає до ЦВК: $I, E_k(I, v'), d$.

Інший варіант протоколу голосування використовує замість ANDOS сліпі підписи, але, по суті, мало чим відрізняється. Етапи (1) – (3) є організаційними. Їх мета полягає в тому, щоб дізнатися і опублікувати усіх дійсних виборців. Хоча дехто, ймовірно, не братиме участі в голосуванні, це зменшує можливість ЦВК додати підроблені бюлетені.

На етапі (4) два виборці можуть отримати один і той самий ідентифікаційний номер. Ця можливість може бути мінімізована, якщо число можливих ідентифікаційних номерів буде значно більшим, ніж число реальних виборців. Якщо два виборці присилають бюлетені з однаковим ідентифікатором, ЦВК генерує новий ідентифікаційний номер, I', вибирає одного з виборців і публікує: $I', E_k(I, v)$. Власник цього бюлетеня дізнається про плутанину, що відбулася, і посилає свій бюлетень знову, повторюючи етап (5) з новим ідентифікаційним номером.

Етап (6) дає кожному виборцеві можливість перевірити, що ЦВК правильно отримала його бюлетень. Якщо його бюлетень неправильно підрахований, він може довести це на етапі (9). Припускаючи, що бюлетень виборця на етапі (6) правильний, повідомлення, яке він посилає на етапі (9) доводить, що його бюлетень був неправильно підрахований.

Однією з проблем цього протоколу є те, що шахрайська ЦВК скористається бюлетенями виборців, які повідомили про намір голосувати на етапі (2), але не голосували насправді. Іншою проблемою є складність протоколу ANDOS. Автори рекомендують розбивати виборців на менші групи, виборчі округи.

Ще однією, серйознішою проблемою є те, що ЦВК може не підрахувати якусь частину бюлетенів. Ця проблема нерозв'язна: виборець стверджує, що ЦВК навмисно знехтувала її бюлетенем, а ЦВК стверджує, що виборець ніколи не голосував.

Висновки

Хоча електронне голосування на даний момент зазнає жорсткої критики з боку спеціалістів з огляду на вразливість архітектури Інтернет та апаратно-програмного забезпечення, ця галузь активно досліджується та впроваджується у повсякденному житті. У цій статті розглянуто протоколи електронного голосування та проаналізовано їх на предмет надійності та можливості програмної реалізації і впровадження. Дослідження є основою для побудови спроектованого клієнт-серверного застосування віддаленого електронного голосування, яке буде досліджуватись у подальших роботах.

Список літератури

1. KOA Voting System [Електронний ресурс]. – Режим доступу: http://kind.ucd.ie/products/opensource/KOA/. – Назва з екрана.
2. David Jefferson, Aviel D. Rubin, Barbara Simons, David Wagner. A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE) [Електронний ресурс]. – Режим доступу: http://servesecurityreport.org/. – Назва з екрана.
3. Mägi, Triinu. Practical Security Analysis of E-voting Systems [Електронний ресурс]. – Режим доступу: http://triinu.net/e-voting/master%20thesis%20e-voting%20security.pdf. – Назва з екрана.

L. Anisimova

PROTOCOLS OF ELECTRONIC VOTING

In the article the basic concept of e-government, e-voting protocols and analyzed them for reliability and capabilities of program implementation.

Keywords: e-government, e-voting, e-voting protocols, software systems supporting e-government.

Матеріал надійшов 15.09.2013