

DOI: 10.18372/2310-5461.40.13266

УДК 004.771

І. О. Мачалін, д-р техн. наук, проф.
Національний авіаційний університет
orcid.org/0000-0003-1684-4980
e-mail: tks@nau.edu.ua;

О. О. Комарницький, аспірант
Національний авіаційний університет
orcid.org/0000-0001-5698-2356
e-mail: komarnitskiy2012@gmail.com;

В. О. Гнатюк, канд. техн. наук
Національний авіаційний університет
orcid.org/0000-0002-4916-7149
e-mail: viktorgnatyuk@ukr.net

УДОСКОНАЛЕННЯ ТЕХНОЛОГІЙ ДОСТУПУ ДО РЕСУРСІВ ТРАНСПАРЕНТНИХ СИСТЕМ ІНТЕРНЕТ-ГОЛОСУВАННЯ

Вступ

Основною проблемою, яка стримує процес упровадження систем електронної демократії, у т. ч. систем дистанційного таємного голосування (ДТГ), у практику суспільних відносин, вважається те, що переважна більшість громадян не довіряє у транспарентність (прозорість) цих систем [1–3]. Через це виникає підозра щодо можливості фальсифікації результатів волевиявлення та/або порушення таємниці голосування адміністраторами системи ДТГ.

Аналіз останніх досліджень та публікацій

У праці [1] запропоновано технологію, що забезпечує прозорість роботи системи ДТГ та досконалий захисту її інформаційних ресурсів. Іншими словами, зроблена спроба усунення підстав для недовіри щодо можливості створення «чесних» систем ДТГ. Однак, щоб якомога більше виборців були зацікавлені у користуванні засобами такої ДТГ, треба зробити дистанційне голосування не тільки захищеним від загроз, але і зручним для виборців. Технологія, що запропонована у [1], не є достатньо зручною у користуванні, бо, з метою прискорення обробки голосів та для забезпечення можливості масштабування на будь-яку кількість виборців, в ній передбачено використовувати окремі сервери для кожної виборчої дільниці, а це означає, що виборцю, наприклад, в Україні треба буде відшукати адресу потрібного сервера серед 33 тисяч існуючих. В праці [1] для цього пошуку запропоновано задіяти сервер формування загального результату голосування, на якому є дані про адреси всіх виборчих дільниць. Таке рішення у разі зростання кількості виборців може призвести до затримки процесу пошуку необхідної адреси через пере-

вантаженість сервера, коли зростання інтенсивності потоку звернень виборців до цього серверу у непередбачувані моменти часу може негативно впливати на бажання громадян щодо користування системою дистанційного голосування [3; 4]. Отже, ця технологія потребує удосконалення.

Постановка завдання

Мета роботи — удосконалити технологію дистанційного доступу виборців до серверного обладнання системи Інтернет-голосування у напрямі вирішення завдань із забезпечення безперешкодного доступу виборців до потрібних ресурсів та створення зручного користувацького інтерфейсу.

З технічної точки зору критерії доступності передбачають таке [5; 6]:

- мінімізація відмов в обслуговуванні;
- швидке відновлення роботи після збоїв;
- гаряча заміна обладнання у разі виходу з ладу;
- забезпечення доступу користувачів до потрібних інформаційних ресурсів без зайвих ускладнень.

Розглянемо останній четвертий пункт наданого переліку, оскільки перші три стосуються сфери забезпечення надійності обладнання, яка не є об'єктом даного дослідження.

Зрозуміло, що не можна з метою ліквідації «зайвих ускладнень» зменшувати рівень якості забезпечення цілісності і конфіденційності інформації. Користування паролями неможливо позбутись через вимоги збереження конфіденційності. Тому неможливо позбутись необхідності відповідального ставлення виборців до паролів, які слід не забувати і зберігати у таємниці. Це є дійсно тим єдиним ускладненням при

Інтернет-голосуванні порівняно із традиційним методом голосування. Але користування паролями в Інтернеті — широко розповсюджена процедура, яка є звичайною для будь-якого користувача. Так що цей недолік слід вважати несуттєвим.

У праці [1] показано, що для підвищення захищеності виборців у користуванні ресурсами систем ДТГ доцільно поставити та вирішити два завдання. Перше — зробити доступ до сервера виборчої дільниці зручним. Оскільки основна незручність для виборця пов'язана із необхідністю пошуку адреси своєї виборчої дільниці серед десятків тисяч інших дільниць, то необхідно мінімізувати зусилля із здійснення такого пошуку. Друге завдання — мінімізувати можливу затримку на очікування відповідей від сервера. Оскільки потік звернень виборців до серверного обладнання під час Інтернет-голосування має випадковий непрогнозований характер, то не виключена

можливість виникнення сплесків у цьому потоці [7]. Унаслідок цього можливе перевантаження серверного обладнання трафіком, що призводить до виникнення черг в обслуговуванні звернень або, навіть, до їхньої втрати. Затримки через очікування в чергах вкрай негативно сприймаються більшістю виборців. Тому вони мають бути не більшими певного порогового рівню, що обирається із інтуїтивних міркувань розробниками системи ДТГ.

Існуючі методи забезпечення доступу до інформаційних ресурсів системи Інтернет-голосування

Метод оцінки величини затримки на очікування відповідей від сервера виборчої дільниці (СВД) запропоновано у праці [1], де розглянуто часову діаграму процесу обслуговування виборця цим сервером, а час здійснення процедури пошуку IP-адрес не враховується (рис. 1).

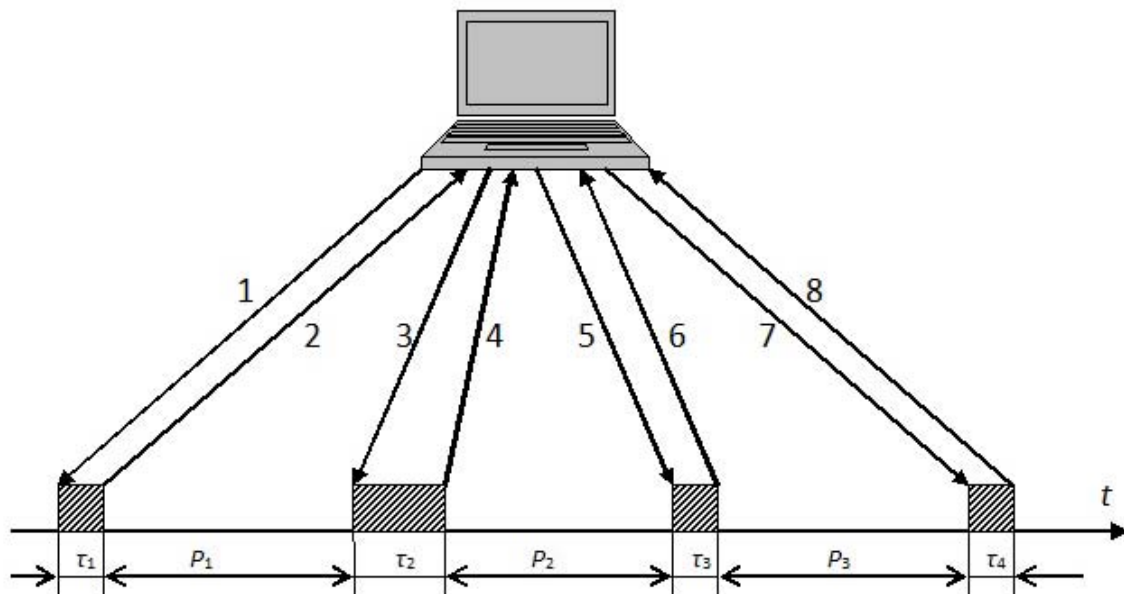


Рис. 1. Часова діаграма процесу обслуговування виборця сервером виборчої дільниці під час здійснення процедури Інтернет-голосування

За результатами аналізу цієї діаграми запропоновано заходи з мінімізації часу очікування відповідей від СВД на запити виборців під час голосування. Зокрема, в програмі *SVD.js* СВД системи ДТГ, яка детально розглянута у [8], передбачена можливість підтримки діалогу зі 100 виборцями одночасно для випадку, коли виборці самостійно здійснюють пошук IP-адрес серверів своїх виборчих дільниць.

Таку кількість виборців для одночасного обслуговування обрано виходячи з експериментальної оцінки відношення сумарної тривалості пауз P_i , які виникають між інтервалами τ_j , що

відповідають часу обробки запитів від одного виборця, до суми цих інтервалів, а саме [1]

$$K = \frac{\sum_{i=1}^w P_i}{\sum_{j=1}^v \tau_j}, \quad (1)$$

де K — оцінка кількості виборців, які можуть одночасно обслуговуватись сервером виборчої дільниці; w — кількість пауз між періодами обслуговування запитів від одного виборця; v — кількість інтервалів часу на обслуговування запитів одного виборця.

Через те, що сумарна тривалість пауз під час обслуговування запитів виборця приблизно у 100 разів більша за суму періодів обробки цих запитів, а серверна програма у періоди пауз може обслуговувати запити від інших виборців (до 99), то час очікування відповіді сервера у середньому буде не перевищувати 2–3 секунди, що слід вважати цілком прийнятною величиною. Однак вищенаведені міркування, що викладені у [1], є справедливими для СВД, який обслуговує не більше ніж 2500 виборців, а сервер визначення *IP*-адреси в умовах України повинен бути здатним обслуговувати більше 10 млн виборців. (Це в ідеалі. На практиці значна частина виборців має змогу визначити *IP*-адресу серверу своєї виборчої дільниці заздалегідь). При цьому сплески трафіка можуть бути значними і, з очевидних міркувань, майже не прогнозованими. Під час таких сплесків можливі ситуації, коли час очікування відповіді сервера буде перевищувати допустиме значення.

Для мінімізації зусиль виборців з пошуку адрес своїх виборчих дільниць при ДТГ в працях [1; 4] їм пропонується користуватися відомим методом пошуку на мапах місцевості. У разі великої кількості можливих варіантів, пошук здійснюють у 2–4 етапи на мапах різного масштабу. У праці [1] розглядається альтернативний варіант пошуку з використанням назв міст або селищ і вулиць, як це вже реалізовано на сайті Державного реєстру виборців за адресою https://www.drj.gov.ua/portal/cm_core.cm_index

Обидва ці методи безпосереднього пошуку виборцем *IP*-адреси сервера своєї виборчої дільниці (ВД) в інтерактивному режимі взаємодії із спеціально виділеним сервером, на котрому містяться дані щодо *IP*-адрес усіх виборчих дільниць, можна впроваджувати разом, залишаючи обрання того чи іншого, на розсуд виборця, але враховуючи значні витрати часу виборцем при використанні як першого, так і другого методу, здійснення такого пошуку для мільйонів виборців потребує побудови більш складної схеми обслуговування, ніж окремих сервер.

Модель (схема) дистанційного доступу, що забезпечує автоматичний пошук *IP*-адрес серверів виборчих дільниць

Модель інформаційної взаємодії елементів системи ДТГ із забезпеченням автоматичного пошуку *IP*-адрес СВД, що пропонується у даній роботі, базується на використанні відомих мето-

дів безпосереднього пошуку виборцями цих адрес, які описані у попередньому розділі. Програми, які реалізують ці методи, встановлюються на сервери пошуку адрес (ПА), що виконують без участі людини в інтерактивному режимі процедуру пошуку *IP*-адрес. Зрозуміло, що пропускна спроможність одного сервера ПА буде недостатньою для того, щоб забезпечити задовільне значення середнього часу очікування у чергах на обробку звернень виборців. Тому у моделі, яку ми пропонуємо, відому технологічну схему обробки інформації, яка детально розглянута у праці [1], доповнено лінійкою серверів ПА та сервером переведення звернень (ПЗ), який розподіляє потік звернень виборців між серверами лінійки з метою уникнення можливих перевантажень у роботі цих серверів. При цьому загальна пропускна спроможність (продуктивність) одного сегменту пошуку *IP*-адрес у системі ДТГ щодо обробки звернень виборців фактично буде дорівнювати сумі продуктивності усіх серверів ПА, що входять до складу цього сегменту. Оскільки продуктивності одного сервера ПЗ залежно від конкретних умов застосування може виявитися недостатньо, у склад системи ДТГ може бути включено кілька сегментів пошуку *IP*-адрес залежно від того, яка частка виборців визначила *IP*-адреси своїх виборчих дільниць заздалегідь до початку здійснення процедури голосування.

Алгоритм роботи сервера ПЗ залежить від характеристик потоку звернень виборців, зокрема від характеристик пульсацій трафіка. Бо не виключено, що активність значної кількості виборців може співпадати у часовому вимірі.

Схематичне відображення протоколу інформаційної взаємодії засобів технічної підтримки автоматичного пошуку *IP*-адрес СВД при здійсненні процедури Інтернет-голосування представлено на рис. 2.

Як бачимо, перш ніж звернення виборця під час Інтернет-голосування надійде на обробку до сервера відповідної виборчої дільниці (ВД), воно спочатку приймається сервером ПЗ, який перенаправляє це звернення на обробку до одного із серверів ПА.

Сервери ПА функціонують одночасно, незалежно один від одного. Кожен з них здійснює обробку отриманого звернення, а саме, здійснює пошук *IP*-адреси сервера ВД, до якої прикріплений виборець, що ініціював це звернення.

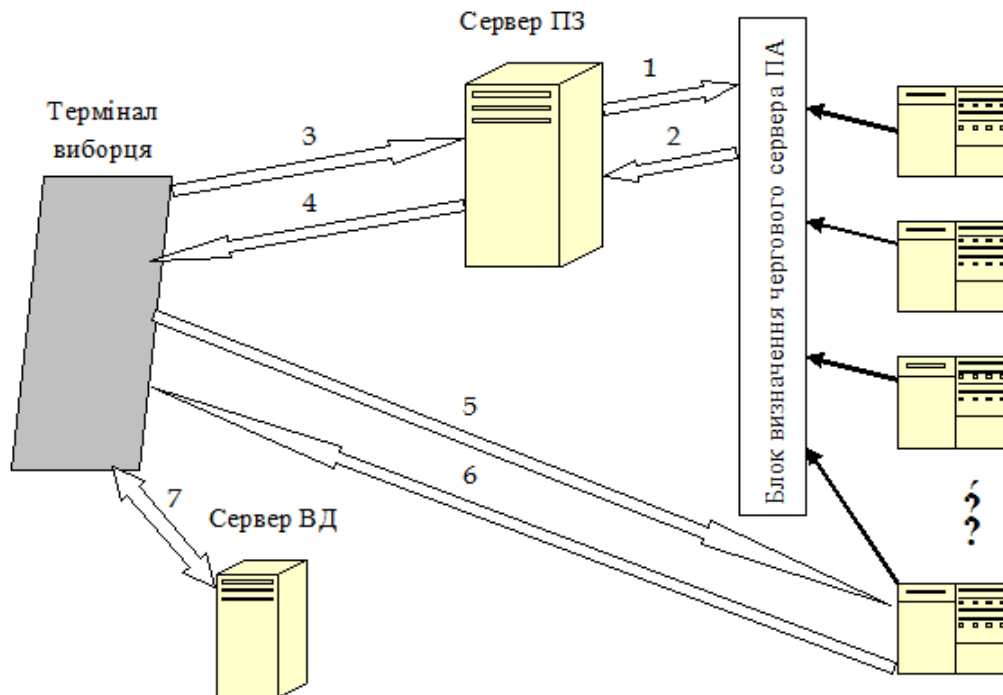


Рис. 2. Протокол інформаційної взаємодії засобів автоматичного пошуку IP-адрес СВД у сегменті системи ДТГ при обслуговуванні запитів виборців під час Інтернет-голосування

Протокол інформаційної взаємодії засобів автоматичного пошуку IP-адрес СВД

Відповідно до запропонованої моделі має виконуватися така послідовність дій:

1. Сервер ПЗ звертається до блоку визначення чергового сервера ПА, який можливо реалізувати у вигляді однієї із програмних компонент сервера ПЗ або у вигляді окремого програмно-апаратного засобу. Цей блок весь час отримує від серверів ПА інформацію про їхню зайнятість. Під черговим сервером ПА ми розуміємо той сервер, який може знайти потрібну IP-адресу за найкоротший час.

2. Сервер ПЗ отримує від блоку визначення чергового сервера ПА ідентифікатор цього сервера, після чого сервер ПЗ стає готовим для передачі IP-адреси сервера ПА на запит від терміналу виборця. З цього моменту сервер ПЗ буде знаходитись у режимі очікування запиту від виборця.

3. Сервер ПЗ отримує очікуваний запит від виборця.

4. Сервер ПЗ відправляє IP-адресу чергового сервера ПА і одразу після цього готується до обслуговування нового запиту від виборця, переходячи до виконання дії 1.

5. Отримавши IP-адресу сервера ПА, термінал виборця звертається за цією адресою до цього сервера для отримання від нього в інтерактивно-

му режимі IP-адреси сервера своєї виборчої дільниці.

6. Термінал виборця отримує від чергового сервера ПА IP-адресу сервера ВД.

7. Виборець розпочинає процедуру ДТГ в інтерактивному режимі на сервері своєї виборчої дільниці.

Кожен сегмент автоматичного пошуку IP-адресу у системі ДТГ має один сервер ПЗ та певним чином обрану кількість серверів ПА. Кількість цих серверів обирають виходячи із необхідності додержання вимог щодо припустимого рівня якості обслуговування запитів виборців під час голосування, а саме припустимого максимального значення часу очікування обробки запиту та очікуваної кількості втрачених запитів, що не пройшли процедуру обробки. Оскільки політика безпеки в домені ДТГ не дозволяє під час голосування змінювати склад програмно-апаратних засобів, то загальна пропускна спроможність сегменту системи ДТГ залежить від кількості серверів ПА. Тому актуальним є завдання оптимального вибору необхідної кількості серверів ПА у цьому сегменті. Однак вирішення цього завдання виходить за рамки даного дослідження. Під час сплесків потоку звернень навантаження на сервери адресації суттєво зростає. Тому, щоб мінімізувати ймовірність перенавантаження цих серверів при обраній їхній кількості, доцільно поставити та вирішити задачу опти-

мального розподілу потоку звернень виборців на обслуговування між серверами ПА за умови, що значення пропускної спроможності сегменту системи ДТГ, що розглядається, є сталою величиною і при постановці оптимізаційної задачі має бути віднесено до розряду обмежень.

Загальна постановка завдання оптимального розподілу потоку звернень виборців на обслуговування між серверами адресації

Реалії виборчих кампаній показують, що інтенсивності потоків запитів, що оброблюються серверами ПА, будуть швидко змінюватися у реальному часі непередбаченим чином. До того ж час пошуку IP-адреси сервером ПА залежить від багатьох непередбачуваних факторів і є випадковою величиною з невідомою щільністю ймовірності. Можуть виникнути ситуації, коли одні сервери перенавантажені запитами у той час, як інші є недовантаженими. Тому, щоб унеможливити такі ситуації, доцільно у склад системи ДТГ увести додаткове обладнання, яке б здійснювало функцію рівномірного розподілу навантаження між серверами ПА. Таку функцію повинен виконувати, спеціальний блок визначення чергового сервера ПА (рис. 2).

У зв'язку із вищезазначеним ставиться завдання: розробити метод оптимального розподілу продуктивності визначеного сегменту системи ДТГ між її серверами ПА залежно від характеру змін інтенсивності потоків запитів, що надходять на входи (уводи) цих серверів, та ступеню їхньої завантаженості трафіком. Критерій оптимальності має бути пов'язаний з умовою забезпечення рівності поточних значень коефіцієнтів завантаження серверів в усталеному (рос. — установившемся) режимі, коли інтенсивності запитів, що надходять до серверів ПА, є постійними та не відчувають флуктуацій. При цьому оптимальний розподіл має здійснюватися за умови, коли кількість серверів ПА у складі сегменту ДТГ та значення їхньої пропускної здатності є заданими величинами. Вибір цих величин має здійснюватися виходячи із необхідності забезпечення мінімуму кількості серверів ПА у складі сегменту системи ДТГ (точніше кажучи, мінімуму необхідного значення загальної пропускної спроможності цього сегменту) при заданому рівні якості обслуговування запитів (зокрема, заданому значенні часу очікування у черзі на обслуговування та (або) заданому значенні коефіцієнта втрат запитів). Можлива постановка і зворотного оптимізаційного завдання, коли необхідно максимізувати рівень якості обслуговування (зокрема, мінімізувати час очікування у черзі та (або) коефіцієнт втрат запитів) при заданій кіль-

кості серверів ПА, тобто при заданому значенні загальної пропускної спроможності сегменту.

На практиці усталені режими потоків запитів можливі лише гіпотетично. Реально ці потоки мають невідворотні флуктуації. Оскільки мова йде не про неперервний потік, а про пульсуючий дискретний потік, та ще й різних (щодо тривалості) об'єктів — сеансів обслуговування запитів виборців, то інтенсивність потоку запитів не може бути визначена та виміряна миттєво. Для вимірювань характеристик інтенсивності потоку запитів необхідно використовувати інформацію щодо поведінки потоку у минулому. Але при цьому до поточного моменту вимірювання ця інформація має відношення лише в тому сенсі, що додатково припускається: на протязі відрізка часу, що йде після вимірювання, інтенсивність потоку запитів практично не змінюється. Отже, надати точне однозначне визначення поняттю «миттєва інтенсивність» не є можливим.

Найпростіше тривіальне рішення сформульованого вище завдання може бути таким: на основі результатів вимірювань інтенсивності обробки потоків, що надходять від серверів ПА до блоку визначення чергового сервера ПА перерозподіляють запити у потоках у перемикальному режимі з урахуванням дій щодо можливого перевищення інтенсивності потоків сумарної пропускної спроможності системи. Але, зважаючи на специфіку технологічного середовища функціонування системи ДТГ, таке рішення не є прийнятне через високу швидкість і не повну передбачуваність зміни потоку запитів, що надходять до сервера ПЗ.

Інше тривіальне рішення цього завдання, що не враховує затримку на вимірювання: на основі результатів вимірювань інтенсивності оброблених потоків запитів, що надходять до блоку визначення чергового сервера ПА від серверів ПА, увідний потік запитів розподіляють таким чином, щоб інтенсивності окремих потоків запитів після розподілу були пропорційні продуктивності серверів (тобто, щоб усі сервери були однаково завантаженими). Але оскільки під час вимірювань затримку неможливо усунути, то таке рішення з принципового погляду неможливо реалізувати. Тому доцільно відслідковувати тенденції щодо змін інтенсивності оброблюваних потоків на сервері ПА.

Таку функцію відслідковування можливо реалізувати шляхом застосування відповідного диференціального рівняння настроювання [8–9]. При цьому увідними функціями керування будуть виміряні значення інтенсивності оброблених потоків усіма серверами ПА, а вивідними — рекомендовані значення інтенсивності увідних

потоків запитів, що мають надходити на обробку до цих серверів. Наближення до режиму однаковості значень коефіцієнтів навантаження серверів створює сприятливу ситуацію, коли однакові за відсотком пульсації потоків запитів на різних серверах не призводять до втрат запитів, якщо величини цих пульсацій знаходяться в межах запасу пропускної здатності системи ДТГ.

У процесі вирішення сформульованого вище завдання варто взяти до уваги такі міркування. У силу високої динамічності і не повної передбачуваності характеру змін інтенсивності реальних потоків запитів, що надходять на сервери ПА, існує можливість оцінювання лише поточних тенденцій у змінах швидкостей потоків на коротких відрізках часу. Тому доцільно будувати алгоритм настроювання механізму розподілу потоків запитів за адаптивним принципом [8; 9].

Саме це і є підставою для реалізації диференціального рівняння настроювання. При цьому поточні зміни потоків повинні впливати на величини коефіцієнтів завантаження серверів (або, як говорять, на ширину смуг пропускання серверів) з урахуванням так званого рівняння настроювання, яке, у свою чергу, має відображати прийнятий закон розподілу загальної пропускної спроможності системи ДТГ між серверами ПА.

Рівняння настроювання повинне забезпечувати відстеження тенденцій у змінах інтенсивності оброблених потоків (включаючи можливість їхнього прогнозування) і бути диференціальним. У такому випадку сформульоване завдання в постановочному плані буде змістовною, замкнутою і внутрішньо несуперечливою, а очевидним корисним наслідком її рішення буде зменшення ймовірності перенавантаження серверів ПА трафіком, що надходить до їхніх портів, і, отже, зменшення величини коефіцієнту втрат необроблених запитів від виборців при заданій кількості серверів ПА у складі системи ДТГ.

Висновки

За результатами аналізу існуючих методів забезпечення доступу виборців до інформаційних ресурсів системи Інтернет-голосування зроблено висновок про доцільність розробки засобу автоматизації пошуку *IP*-адрес серверів виборчих дільниць (СВД), котрі мають надаватися виборцям за їхніми запитамі для здійснення актів дистанційного голосування.

Автоматизація процедури пошуку суттєво підвищує зручність користування послугами системи Інтернет-голосування і зацікавленість виборців здійснювати дистанційне голосування. Для автоматизації пошуку *IP*-адрес серверів СВД запропоновано використати спеціалізований сер-

вер пошуку адрес (ПА), програмні засоби якого у відповідь на звернення виборців у реальному часі мають реалізовувати процедуру пошуку відповідно до будь-якого із відомих методів пошуку, а знайдені значення *IP*-адрес надсилати на термінальні вузли ініціаторів звернень.

Оскільки швидкість пошуку *IP*-адрес, що здійснюється сервером ПА, є набагато нижчою порівняно із швидкістю обробки звернень сервером СВД, то з метою уникнення довготривалих затримок у доступі виборців до ресурсів системи Інтернет-голосування у склад її обладнання слід увести не один, а кілька серверів ПА, що мають функціонувати одночасно і незалежно один від одного. У цьому випадку загальна продуктивність системи голосування буде визначатися сумарною продуктивністю серверів ПА.

Під час сплесків трафіка виборців, що мають випадковий і непередбачуваний характер, а також внаслідок випадкової тривалості часу пошуку *IP*-адрес серверами ПА, можуть виникати ситуації, коли частина серверів ПА перенавантажуються цим трафіком у той час, як інші сервери ПА функціонують недонавантаженими. Тому, щоб мінімізувати ймовірність перенавантаження серверів ПА при певним чином обраній їхній кількості, запропоновано нову схему доступу виборців до ресурсів серверного обладнання системи ДТГ, зокрема у склад обладнання уведено додатковий засіб – сервер-менеджер ПЗ (сервер переведення звернень), який у реальному часі має здійснювати адаптивний розподіл потоку звернень між серверами ПА з тим, щоб забезпечити рівномірне завантаження серверів в умовах непрогнозованих сплесків (пульсацій) цього потоку під час голосування.

З урахуванням вище наведеного розроблено схему взаємодії засобів технічної підтримки процедур Інтернет-голосування з автоматичним пошуком *IP*-адрес серверів виборчих дільниць і відповідний протокол процедури Інтернет-голосування. Здійснено постановку та запропоновано схему вирішення завдання оптимального розподілу під час голосування потоку звернень виборців на обслуговування між серверами пошуку адрес ПА.

Оскільки пульсації потоку звернень та час пошуку *IP*-адрес серверами ПА мають непередбачуваний характер, запропоновано діяти у напрямку вирівнювання значень коефіцієнтів завантаження цих серверів з урахуванням як можливих трендів та пульсацій потоку запитів виборців, так і непередбачуваних за величиною проміжків часу, необхідних серверам ПА для пошуку *IP*-адрес СВД.

ЛІТЕРАТУРА

1. **Пригара М. П.** Захищена система технічної підтримки процесів дистанційного волевиявлення: дис. ... канд. техн. наук: 05.13.21 – Системи захисту інформації. Національний авіаційний університет, Київ, 2018.

2. **Сабанов А. Г.** Вопросы доверия при построении электронного правительства. Информационно-методический журнал «Защита информации. Инсайды», № 2, 2010. URL: http://www.inside-zi.ru/pages/2_2010/66.html (дата звернення 25.11.2018)

3. **Асемьян С. Z., Kortum P., Byrne M. D., Wal-lach D. S.** Usability of Voter Verifiable, End-to-end Voting Systems: Base line Data for Helios, Prêt à Voter, and Scantegrity II. *USENIX Journal of Election-Technology and Systems (JETS)*, 2014, Vol. 2, No 3, pp. 26–56.

4. **Чуприн В. М.,** Вишняков В. М., Пригара М. П. Захист операційного середовища систем Інтер-

нет голосування. *Захист інформації*. 2017, Т. 19, №1, С. 56–66.

5. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

6. НД ТЗІ 2.5-005-099. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

7. **Мхамад Ібрагім Ахмад Альмар** Удосконалення технології управління розподілом ресурсів пакетних мереж: дис. ... канд. техн. наук: 05.13.05 Комп'ютерні системи та компоненти. Національний авіаційний університет, Київ, 2015.

8. **Антонов В. К.** Метод построения качественных регуляторов. *Кибернетика и вычислительная техника*. 2000. Вып. 126. С. 40-48.

9. **Антонов В. К.** Побудова регуляторів із заданою якістю руху за допомогою обмеження зміни функції Ляпунова-Белмана. *Вісник НАУ*. 2001. № 4 (11). С.129-132.

Мачалін І. О., Комарницький О. О., Гнатюк В. О.

УДОСКОНАЛЕННЯ ТЕХНОЛОГІЇ ДОСТУПУ ДО РЕСУРСІВ ТРАНСПАРЕНТНИХ СИСТЕМ ІНТЕРНЕТ-ГОЛОСУВАННЯ

Визначено недоліки існуючих технологій дистанційного доступу виборців до серверного обладнання транспарентних систем голосування через Інтернет. З метою забезпечення безперешкодного доступу виборців до потрібних ресурсів та створення зручного користувацького інтерфейсу запропоновано модель (схему) та відповідний протокол інформаційної взаємодії засобів автоматичного пошуку IP-адрес елементів серверного обладнання при обслуговуванні запитів виборців під час Інтернет-голосування. З метою уникнення перевантаження обладнання трафіком здійснено постановку та запропоновано схему рішення задачі оптимального розподілу під час голосування потоку звернень виборців на обслуговування між елементами серверного обладнання.

Ключові слова: транспарентна система Інтернет-голосування; серверне обладнання; модель дистанційного доступу; автоматизація процедур голосування; оптимальний розподіл трафіка.

Machalin I. A., Komarnitskiy O. O., Gnatyuk V. O.

TECHNOLOGY IMPROVING OF ACCESS TO TRANSPARENT SYSTEMS RESOURCES FOR INTERNET VOTING

Remote voting via the Internet provides significant advantages for voters in terms of convenience, mobility, and time savings, but a constraint on its implementation is the distrust of voters due to uncertainty in keeping secrets and fairness in the counting of voting results. It is clear that the staff that manages the counting server has ample opportunities for abuse. Therefore, in order to increase the level of citizens' confidence in the remote voting system, the challenge is to develop technology that would provide unconditional confidence in the absence of malicious or erroneous actions of personnel in managing the Internet voting system. The article is devoted to the improvement of technology of access of electors within the remote voting system (RVS), which guarantees secrecy of votes and ensures freedom of expression of will in conditions of administrative pressure. The lacks of existent technologies of the controlled from distance access of electors are certain to the server equipment of the transparent (open) voting systems over the Internet. Transparency is that property on that the level of trust of people depends straight. Therefore for providing of transparency of the voting systems it is necessary so to control the actions of personnel in relation to a management a server, that possibility to hide these actions from inspectors was not. With the aim of providing of unimpeded access of electors to the necessary resources and creation of comfortable man-machine interface a model (chart) and corresponding protocol of informative co-operation of automatic search of IP-adress of elements of server equipment are offered at maintenance of queries of electors under time Internet-voting. With the aim of avoidance of long duration delays in access of electors to the resources of the system internet-voting incomposition of her equipment is entered a few servers of search of addresses that function simultaneously and independent of each other. In composition of equipment additional means are entered also is a server-manager that real-time carries out adaptive distribution of stream of appeals between the servers of search of addresses in order to provide the even loading of servers in the conditions of splashes (pulsations) of this

stream during voting. With the aim of avoidance of equipment overload by traffic the chart of decision of task of optimal distribution is offered during voting of stream of queries of electors on service between the elements of server equipment.

Keywords: transparent voting system over the internet; server equipment; model of distance access; automation of procedures of voting; optimal distribution of traffic.

Мачалин И. А., Комарницкий О. О., Гнатюк В. О.

СОВЕРШЕНСТВОВАНИЕ ТЕХНОЛОГИИ ДОСТУПА К РЕСУРСАМ ТРАНСПАРЕНТНЫХ СИСТЕМ ИНТЕРНЕТ-ГОЛОСОВАНИЯ

Определены недостатки существующих технологий удаленного доступа избирателей к серверному оборудованию транспарентной системы голосования через Интернет. С целью обеспечения беспрепятственного доступа избирателей к нужным ресурсам и создания удобного пользовательского интерфейса предложена модель (схему) и соответствующий протокол информационного взаимодействия средств автоматического поиска IP-адреса элементов серверного оборудования при обслуживании запросов избирателей во время Интернет-голосования. Во избежание перегрузки оборудования трафиком осуществлена постановка и предложена схема решения задачи оптимального распределения во время голосования потока обращений избирателей на обслуживание между элементами серверного оборудования.

Ключевые слова: транспарентная система интернет-голосования; серверное оборудование; модель дистанционного доступа; автоматизация процедур голосования; оптимальное распределение трафика.

Стаття надійшла до редакції 08.10.2018 р.
Прийнято до друку 06.11.2018 р.