DOI: 10.18372/2410-7840.21.13544
УДК 004.773

МЕТОД РОЗПОДІЛУ НАВАНТАЖЕННЯ МІЖ СЕРВЕРАМИ СИСТЕМИ ІНТЕРНЕТ-ГОЛОСУВАННЯ

Володимир Чуприн, Веніамін Антонов, Олег Комарницький

Запропоновано метод оптимального адаптивного розподілу потоку звернень виборців між спеціалізованими серверами захищеної системи інтернет-голосування, що здійснюють за запитами виборців автоматичний пошук ip-адрес потрібних їм серверів виборчих дільниць. За основу узята схема доступу виборців до серверів виборчих дільниць, що детально розглянута у [3]. Для автоматизації пошуку у цій схемі використано лінійку спеціалізованих серверів пошуку адрес (ПА), програмні засоби котрих у відповідь на звернення виборців у реальному часі виконують процедуру пошуку відповідно до будь-якого із відомих методів пошуку, а знайдені значення ip-адрес надсилають на термінальні вузли ініціаторів звернень. Поряд з лінійкою серверів ПА, що мають функціонувати одночасно і незалежно один від одного, у склад обладнання системи дистанційного таємного голосування уведено також додатковий засіб – сервер-менеджер ПЗ (сервер переведення звернень), котрий у реальному часі має здійснювати адаптивний розподіл потоку звернень між серверами ПА з тим, щоб забезпечити рівномірне завантаження цих серверів в умовах непрогнозованих сплесків (пульсацій) потоку звернень під час голосування. Реалізація методу дозволяє удосконалити технологію дистанційного доступу виборців до захищених ресурсів транспарентної системи інтернет-голосування. Зокрема, забезпечити рівномірне завантаження серверного обладнання в умовах непрогнозованих сплесків (пульсацій) трафіка виборців, а також можливість підтримки прийнятного рівня захисту та якості обробки цих звернень (зокрема, підтримки прийнятного значення середнього часу очікування у черзі на обслуговування звернення) з використанням мінімальної кількості серверного обладнання. Параметри цієї технології визначено як результат вирішення відповідної оптимізаційної задачі, що реалізує метод динамічного програмування Р.Белмана.

Ключові слова: *транспарентна система інтернет-голосування, серверне обладнання, дистанційний доступ, оптимальний розподіл трафіка, метод адаптивного регулювання Р. Белмана.*

Вступ

Тема даної публікації присвячена питанням удосконалення існуючих методів забезпечення доступу виборців до захищених інформаційних ресурсів транспарентних систем дистанційного таємного інтернет-голосування (ДТГ) [1, 2]. За основу узята схема доступу виборців до серверів виборчих дільниць (СВД) [3], що реалізує автоматичний пошук IP-адрес СВД. Для автоматизації пошуку у цій схемі використано лінійку спеціалізованих серверів пошуку адрес (ПА), програмні засоби котрих у відповідь на звернення виборців у реальному часі виконують процедуру пошуку відповідно до будь-якого із відомих методів пошуку [1, 3], а знайдені значення IP-адрес надсилають на термінальні вузли ініціаторів звернень. Проблема в тому, що внаслідок непередбачуваних пульсацій потоку звернень та непередбачуваної тривалості процедури пошуку серверами ПА ці сервери завантажуються випадковим чином нерівномірно – одні сервери можуть функціонувати перевантаженими у той час, як інші будуть недовантаженими. Тому поряд з лінійкою серверів ПА, що мають функціонувати одночасно і незалежно один від одного, у склад обладнання системи ДТГ уведено також додатковий засіб – сервер-менеджер ПЗ (сервер переведення звернень), котрий 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 [3].

Актуальність теми дослідження

У роботі [3] здійснено постановку та запропоновано загальну схему рішення задачі розподілу потоку звернень виборців на обслуговування між серверами ПА, однак розробку методів вирішення цієї задачі, тим більш з урахуванням конкретних умов функціонування обладнання, що реалізує автоматичний пошук IP-адрес СВД, не виконано. Це унеможливлює використання результатів роботи [3] на практиці. Відсутність автоматичного пошуку IP-адрес СВД негативно впливає на бажання громадян користуватися послугами системи ДТГ, а не прогнозовані пульсації інтенсивності потоку звернень виборців до СВД у непередбачувані моменти часу можуть призвести до затримки процесу пошуку необхідної адреси через перевантаженість цього сервера. Тому теоретичний і практичний інтерес являє розробка методу розподілу навантаження між серверами пошуку адрес ПА системи ДТГ. Вкрай бажано, щоб розроблюваний метод забезпечував оптимізацію процесу розподілу потоку звернень з урахуванням динаміки непередбачуваних пульсацій цього потоку.

Мета даного дослідження – розробити та обґрунтувати на формальному рівні метод оптимального розподілу у реальному часі потоку звернень виборців між серверами пошуку адрес (ПА).

1. Формалізована постановка задачі оптимального розподілу потоку звернень між серверами пошуку адрес

Виходячи із розглянутих у [3] умов та обмежень, в якості цільової функції у даній оптимізаційній задачі доцільно обрати певним чином визначену інтегральну величину відхилення реальних поточних значень навантажень на кожний із серверів ПА від значень рівномірного навантаження цих серверів. Зрозуміло, що величину цього відхилення слід мінімізувати з урахуванням характеристик потоку звернень виборців, що контролюються сервером-менеджером ПЗ. Бо тільки у цьому випадку суттєво знижується ризик втрат запитів виборців на обслуговування у період голосування. А в якості обмеження має бути обрана величина загальної пропускної спроможності лінійки серверів ПА у даному сегменті мережі доступу. Вибраний критерій оптимальності має відповідати умові забезпечення рівності поточних значень коефіцієнтів завантаження серверів ПА в усталеному (рос. – установившемся) режимі, коли інтенсивності потоків звернень, що надходять до ПА, є постійними та не відчувають флуктуацій. Проте на практиці зміни інтенсивності потоку звернень виборців до системи ДТГ під час голосування мають непередбачуваний характер. Тому систему розподілу цього потоку слід розглядати як динамічну систему, що реалізує адаптивний механізм авторегулювання.

Розглянемо сегмент системи ДТГ, що має n серверів ПА [3]. Логічно припустити, що пропускна спроможність цього сегменту ΔF не може змінюватися у період виборчої кампанії (і, от же є константою), оскільки у цей період як правила політики інформаційної безпеки, так і склад апаратних засобів системи ДТГ не може бути змінений. Тому пропускна спроможність даного сегменту щодо обробки запитів від виборців представляється як сума пропускних здатностей серверів ПА $f_1, f_2, f_3, ..., f_n$, що входять до складу сегмента:

$$\Delta F = f_1 + f_2 + f_3 + \ldots + f_n. \qquad (1)$$

Оптимальний розподіл потоку звернень між серверами пошуку адрес передбачає доцільність визначення як прямих, так і зворотних коефіцієнтів навантаження серверів ПА. Прямі коефіцієнти завантаження показують рівень завантаження серверів ПА трафіком звернень голосуючих суб'єктів відносно їхньої пропускної здатності. Зворотні коефіцієнти завантаження показують, наскільки пропускні спроможності серверів ПА щодо обробки запитів перевищують швидкості реальних поточних потоків запитів, що ними обслуговуються.

Прямі коефіцієнти навантаження $k_1, k_2, k_3, \ldots, k_n$ визначимо наступним чином:

$$k_1 = \frac{s_1}{f_1},\ k_2 = \frac{s_2}{f_2},\ \ldots, k_n = \frac{s_n}{f_n}, \qquad (2)$$

де $s_1, s_2, s_3, \ldots, s_n$ - швидкості потоків оброблюваних серверами ПА звернень від виборців.

Зворотні коефіцієнти завантаження серверів ПА $\eta_1, \eta_2, \eta_3, \ldots, \eta_n$ визначимо як відно-шення

$$\eta_1 = \frac{f_1}{s_1},\ \eta_2 = \frac{f_2}{s_2},\ \ldots,\ \eta_n = \frac{f_n}{s_n}. \qquad (3)$$

Швидкості потоків звернень виборців, що надходять на обробку серверами ПА, можуть змінюватися як у бік збільшення, так і у бік зменшення. Тому параметри, що характеризують рівні навантаження на ці сервери трафіком звернень, доцільно представляти у векторній формі. Тим більш, що векторна форма запису цих параметрів спрощує процес програмування адаптивного алгоритму розподілу потоків звернень.

Отже, будемо мати вектор прямих коефі-цієнтів завантаження серверів ПА

$$\dot{\boldsymbol{\kappa}} = \begin{pmatrix} k_1 \\ k_2 \\ . \\ . \\ . \\ k_n \end{pmatrix} \qquad (4)$$

та вектор зворотних коефіцієнтів завантаження серверів ПА

$$\dot{\boldsymbol{\eta}} = \begin{pmatrix} \eta_1 \\ \eta_2 \\ . \\ . \\ . \\ \eta_n \end{pmatrix}. \qquad (5)$$

Таким чином, поточний стан кожного сервера ПА будемо характеризувати чотирма параметрами: його пропускною здатністю щодо обробки звернень виборців, поточною швидкістю потоку цих звернень і відповідними поточними значеннями його прямого і зворотного коефіцієнтів завантаження.

Перш, ніж здійснити постановку задачі оптимального розподілу потоку звернень між серверами пошуку адрес, слід узяти до уваги наступні вихідні міркування.

По-перше, сервер ПЗ має забезпечувати можливість динамічного розподілу у реальному часі загального потоку звернень від виборців між серверами ПА з урахуванням як можливих трендів та пульсацій потоків звернень до цих серверів, так і непередбачуваних за величиною проміжків часу, необхідних цим серверам для пошуку *IP*-адрес серверів виборчих дільниць (ВД). Зрозуміло, що за цих умов прогнозувати час пошуку *IP*-адрес серверами ВД не уявляється можливим. Саме тому із множини можливих методів доцільно обрати адаптивний метод авторегулювання.

По-друге, для побудови адаптивного алгоритму настроювання засобу розподілу потоків, функції котрого виконує сервер-менеджер ПЗ, доцільно використати векторні форми запису керованих змінних, в якості котрих у даній задачі розглядають встановлені менеджером поточні значення швидкості потоку звернень, що подаються на обробку на порти кожного сервера ПА. У даному випадку, коли функція розподілу потоку звернень виборців не є відомою, а швидкість цього потоку динамічно змінюється у реальному часі, до того ж не прогнозованим шляхом, логічно використати результати теорії адаптивного управління. Зокрема, припустити, що засіб адаптивного розподілу потоку звернень від виборців між серверами ПА має діяти у напрямку вирівнювання значень коефіцієнтів завантаження цих серверів за умови неперевищення значення загальної незмінної пропускної спроможності сегменту системи ДТГ, що є предметом розгляду.

По-третє, для вирішення задачі керування розподілом потоку запитів між серверами ПА на основі спостереження за рівнями їхнього завантаження у реальному часі необхідно вирішити задачу динамічного вирівнювання коефіцієнтів завантаження цих серверів.

Тоді процес авторегулювання адаптивним розподілом потоку на формальному рівні у загальному неявному вигляді можна відобразити у вигляді диференціального рівняння настроювання, де права частина цього рівняння має відображати функціонал управління процесом авторегулювання, а ліва частина - вектор керованих змінних, а саме:

$$\dot{\boldsymbol{k}} = \boldsymbol{\Phi}_{\boldsymbol{k}} \tag{6}$$

- для прямих коефіцієнтів завантаження;

$$\dot{\boldsymbol{\eta}} = \boldsymbol{\Phi}_{\boldsymbol{\eta}} \tag{7}$$

- для зворотних коефіцієнтів завантаження.

З фізичної точки зору у результаті покрокового (тобто, крок за кроком) рішення рівняння настроювання значення коефіцієнтів завантаження серверів ПА повинні у реальному часі поступово вирівнюватися шляхом відповідного перерозподілу часток загального потоку звернень виборців між цими серверами за умови, що ΔF=const.

Для того, щоб конкретно відобразити процес адаптивного авторегулювання, необхідно конкретизувати вигляд правих частин рівнянь настроювання (6) та (7), а саме обрати вид керування, задати вектор керуючих впливів та визначити безпосередній функціональний зв'язок між керованими змінними.

2. Схема рішення задачі оптимального розподілу потоків

Процес розподілу навантаження домену ДТГ трафіком звернень виборців це процес покрокового інтегрування у реальному часі рівняння настроювання з урахуванням певних умов та обмежень, що визначені далі у тексті даної статті. Чисельне інтегрування рівняння настроювання (6) або (7) на одному кроці може бути виконано з кроком $\boldsymbol{h}$ відповідно до метода Ейлера [3]:

$$k(t+h) = k(t) + \Phi_k(t)h \tag{8}$$

- для прямих коефіцієнтів завантаження цих серверів;

$$\eta(t+h) = \eta(t) + \Phi_\eta(t)h \tag{9}$$

- для зворотних коефіцієнтів завантаження серверів ПА.

Для рішення наведених вище рівнянь можна використати будь-який чисельний метод інтегрування диференціальних рівнянь. Наприклад, метод Адамса або Ейлера. Зрозуміло, що функціонали управління процесом авторегулювання $\boldsymbol{\Phi_k}$ та $\boldsymbol{\Phi_\eta}$ у рівняннях настроювання (6) та (7) мають бути конкретизовані.

З фізичної точки зору у результаті інтегрування (8) або (9) на кожному новому поточному кроці інтегрування будемо мати новий поточний набір коефіцієнтів завантаження серверів ПА, значення котрих, відповідно до обраного рівняння настроювання, будуть відрізнятися між собою менше, ніж до виконання цього кроку інтегрування. Так що, з кожним наступним кроком ця різниця має поступово зменшуватися. Швидкість зменшення різниці між коефіцієнтами завантаження задається вибором значень відповідних параметрів у правій частині рівняння (6) або (7). Ця

швидкість має бути узгоджена із швидкістю змін інтенсивності трафіка звернень виборців.

Новим значенням коефіцієнтів завантаження, отриманим на даному кроці інтегрування, відповідають нові рекомендовані значення часток від швидкості загального потоку звернень від виборців, що мають бути спрямовані на обробку відповідними серверами ПА. Ці частки обчислюються виходячи з нормування на сталість їхньої суми, яка за величиною, як було вже вказано, має дорівнювати ΔF, тобто пропускній здатності розглянутого сегменту системи ДТГ.

Нові значення часток від швидкості загального потоку звернень, що мають встановлюватися сервером ПЗ і відповідним чином розподілятися між серверами ПА, задаються наступними виразами:

$$\begin{aligned} s_1 &= \frac{f_1 + f_2 + ... + f_n}{\Delta F} k_1 f_1, \\ s_2 &= \frac{f_1 + f_2 + ... + f_n}{\Delta F} k_2 f_2, \\ s_n &= \frac{f_1 + f_2 + ... + f_n}{\Delta F} k_n f_n. \end{aligned} \qquad (10)$$

Структура виразів (10) відображає умову, що під час роботи механізму настроювання виконується співвідношення (1), а саме: сума продуктивності усіх серверів ПА дорівнює загальній пропускній здатності домену системи ДТГ.

Процес динамічного вирівнювання коефіцієнтів завантаження серверів ПА має здійснюватися з дотриманням певним чином визначених умов та обмежень, зокрема підтримувати необхідну швидкість вирівнювання при змінах величини інтенсивності потоку звернень, враховувати швидкість та величину цих змін. Вкрай бажано також, щоб процес вирівнювання здійснювався по оптимальній траєкторії, що забезпечує максимально можливу у поточних умовах швидкість вирівнювання. Таким умовам та обмеженням відповідає метод аналітичного конструювання регуляторів, що запропонований у [5] і удосконалений у роботах [6, 7]. Цей метод є різновидом відомого методу динамічного програмування Р.Белмана, що широко застосовується при вирішенні задач оптимально керування динамічними системами. Цей метод враховує швидкість перехідних процесів у динамічно керованих системах, що вкрай важливо і у нашому випадку динамічного перерозподілу часток загального потоку звернень між серверами ПА.

3. Побудова функції вирівнювання керованих змінних

У нашому випадку регулятори системи адаптивного розподілу потоку звернень (тобто, сервер-менеджер ПЗ) мають функціонувати у реальному часі згідно з методом динамічного програмування Р.Белмана [5]. Це передбачає необхідність визначення функції вирівнювання керованих змінних у явному вигляді.

Визначимо можливий вигляд цієї функції для найпростішого прикладу системи настроювання, що має усього три керовані змінні n_1, n_2, n_3. (У [5] показано, що побудова функції вирівнювання для динамічних систем настроювання більш високого порядку буде здійснюватися аналогічно). При цьому будемо мати на увазі, що функція вирівнювання є позитивно визначеною і дорівнює нулю тільки у випадку, коли усі керовані змінні мають однакові значення.

У нашому прикладі три керовані змінні утворюють вектор

$$\boldsymbol{N} = \begin{pmatrix} n_1 \\ n_2 \\ n_3 \end{pmatrix}. \qquad (11)$$

Далі призначимо матрицю регулюючих зв'язків, зокрема у вигляді

$$\boldsymbol{C} = \begin{pmatrix} 1 & 0 & -1 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}. \qquad (12)$$

Загальне правило побудови матриць регулюючих зв'язків виду (12) надано у [5], відповідно до якого кількість стовпців у матриці має дорівнювати кількості змінних, що потребують керування. У нашому випадку це кількість серверів ПА. Сервери ПА у матриці C є пронумерованими: перший рядок цієї матриці характеризує перший сервер ПА, другий рядок – другий сервер і т.д. У свою чергу, кількість рядків матриці має дорівнювати максимально можливому числу різних пар, складених із серверів ПА за умови, що у кожній парі номер хоча б одного сервера різниться від номера у будь-якій іншій парі. Тобто, усі враховані пари серверів ПА мають бути різними. Такий поділ на пари забезпечує можливість встановлення функціональних зв'язків між будь-якими двома серверами із визначеної лінійки серверів ПА. Порядок розташування серверів в утворених таким чином парах значення не має. От же, у нашому прикладі між

трьома серверами (оскільки маємо три стовпці матриці *C*) можна попарно встановити три функціональні зв'язки (тобто, утворити три різних пари серверів), що в конструкції матриці *C* відображається трьома рядками. Для відображення взаємозв'язків між чотирма серверами матриця має складатися із шести рядків, а між п'ятьма серверами – із десяти рядків. Відбирання ресурсу у сервера (у нашому випадку це зменшення швидкості потоку звернень до цього сервера) відображається знаком мінус. Додавання ресурсу до сервера (це збільшення потоку звернень) відображається знаком плюс. Так що, фізична інтерпретація змісту першого рядка матриці (12) може бути така: між першим і другим серверами ПА реалізується керування, що полягає у передаванні ресурсу (тобто, якоїсь частки потоку звернень) від першого сервера ПА у другий, що відбито знаками відповідних одиничних елементів у матриці. Другий рядок відповідно відображає передачу частки потоку звернень від третього сервера у перший. Третій рядок відповідає передачі ресурсу з другого сервера у третій. Порядок запису рядків або стовпців у матриці *C* не має значення. Так, роль стовпців і рядків може взаємно мінятися. Цю матрицю можливо записати і у транспонованому вигляді.

Для визначення функції вирівнювання у явному вигляді при побудові аналітичного регулятора необхідно визначити добуток між матрицею регулюючих зв'язків та транспонованим вектором керованих змінних і далі цей добуток використати для утворення квадратичної форми, яка за певних умов і представлятиме шукану функцію вирівнювання.

У нашому прикладі такий добуток буде мати наступний вигляд:

$$\boldsymbol{N}^{T}\boldsymbol{C}=(n_1,n_2,n_3)\cdot\begin{pmatrix}-1 & 1 & 0\\ 1 & 0 & -1\\ 0 & -1 & 1\end{pmatrix}=(n_1-n_2,\ n_2-n_3,\ n_3-n_1). \quad (13)$$

Як бачимо, добуток (13) є транспонованим вектором трьох керованих змінних, тобто вектором-рядком. Кожен компонент вектора-рядка являє відмінок між значеннями відповідної пари керованих змінних, що складають вектор $\boldsymbol{N}$.

Теорія аналітичних регуляторів передбачає також можливість визначення матриці вагових коефіцієнтів $\boldsymbol{P}$, яка задає «вагу» кожному регулюючому зв'язку між керованими змінними. Ця матриця має бути діагональною, позитивно визначеною та представленою у наступному вигляді:

$$\boldsymbol{P}=\begin{pmatrix}p_{11} & 0 & 0 & 0 & 0 & 0\\ 0 & p_{22} & 0 & 0 & 0 & 0\\ 0 & 0 & p_{33} & 0 & 0 & 0\\ - & - & - & - & - & -\\ - & - & - & - & - & -\\ 0 & 0 & 0 & 0 & 0 & p_{nn}\end{pmatrix}. \quad (14)$$

При побудові системи розподілу потоку звернень доцільно утворити квадратичну форму виду

$$\boldsymbol{N}^{T}\boldsymbol{C}\boldsymbol{P}\boldsymbol{C}^{T}\boldsymbol{N} \quad (15)$$

з використанням матриці (14), у якій «вагу» кожного регулюючого зв'язку прирівняти до 1.

У нашому прикладі, де розглядаються лише три керовані змінні, квадратична форма (15) буде мати наступний вигляд:

$$(n_1-n_2,\ n_2-n_3,\ n_3-n_1)\cdot\begin{pmatrix}p_{11} & 0 & 0\\ 0 & p_{22} & 0\\ 0 & 0 & p_{33}\end{pmatrix}\times\begin{pmatrix}n_1-n_2\\ n_2-n_3\\ n_3-n_1\end{pmatrix}= \quad (16)$$
$$p_{11}(n_1-n_2)^2+p_{22}(n_2-n_3)^2+p_{33}(n_3-n_1)^2,$$

де $p_{11}+p_{22}+p_{33}=1$.

Як бачимо, отримана квадратична форма (16) може бути придатною для вирівнювання значень коефіцієнтів завантаження серверів ПА [4], оскільки являє зважену суму квадратів відмінків між усіма можливими значеннями керованих змінних. Вона є позитивно визначеною і дорівнює нулеві тільки у випадку, якщо всі перемінні дорівнюють нулю. Так що, вираз (16) і визначає функцію вирівнювання.

4. Синтез рівняння настроювання

Вище було показано, що задача настроювання засобу розподілу потоку звернень виборців між серверами ПА (тобто, задача настроювання сервера-менеджера ПЗ на адаптивний режим роботи) зводиться до задачі вирівнювання коефіцієнтів завантаження цих серверів. При цьому механізм настроювання має функціонувати у реальному часі таким чином, щоб під час його роботи сума керованих змінних була постійною величиною. Дана задача може бути вирішена шляхом використання методу динамічного програмування Р.Белмана. Для цього потрібно конкретизувати рівняння настроювання, задати оптимізуючий функціонал і записати відповідне їм рівняння Белмана. Це дозволить звести задачу динамічного програмування до задачі аналітичного конструювання регуляторів, рішення якої зводиться, як відомо, до рішення рівняння Рікаті [5-7].

Почнемо із синтезу рівняння настроювання. Якщо йти шляхом використання методу динамічного програмування, то поводження компонентів даної системи розподілу навантаження з урахуванням (6) або (7) логічно підкорити рівнянню настроювання у наступному вигляді:

$$\boldsymbol{N} = \boldsymbol{C}\boldsymbol{u}, \qquad (17)$$

де $\boldsymbol{N}$ - l-мірний вектор керованих вирівнювальних змінних, $\boldsymbol{C}$ - $l \times m$ - прямокутна, у загальному виді не квадратна, матриця регулюючих зв'язків, $\boldsymbol{u}$ - m-мірний вектор керуючих впливів.

Якщо приведене вище рівняння настроювання (17) побудовано таким чином, що вектор керуючих впливів $\boldsymbol{u}$ знаходиться як лінійна функція компонентів вектору керованих змінних $\boldsymbol{N}$, то при будь-якому довільному векторному керуванні під час вирівнювання коефіцієнтів навантаження серверів ПА забезпечується збереження суми компонент вектору керованих змінних $\boldsymbol{N}$.

У теорії побудови аналітичних регуляторів для динамічних систем [5-7] показано, що формування рівняння настроювання виду (17) фактично зводиться до доказу того, що воно під час роботи механізму настроювання зможе забезпечити збереження суми керованих змінних. Доказ цього твердження, що зроблений з використанням теореми про стійкість (рос. – устойчивость) [8], міститься, зокрема, у [7]. У процесі доказу для системи виду (17) було призначено допоміжну функцію у вигляді квадратичної форми, далі розглянуто допоміжне стійке рівняння, якому підкоряється допоміжна функція, і шляхом перетворення допоміжного рівняння у тотожність на рішеннях досліджуваної системи було визначено керування.

Отже, у нашому прикладі системи авторегулювання із трьома змінними з урахуванням (17) система настроювання представляється як

$$\begin{pmatrix} \dot{n}_1 \\ \dot{n}_2 \\ \dot{n}3 \end{pmatrix} = \begin{pmatrix} -1 & 1 & 0 \\ 1 & -1 & 0 \\ -1 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & -1 & 1 \\ 0 & 1 & -1 \end{pmatrix} \cdot \boldsymbol{u}, \qquad (18)$$

де права частина рівняння (18) визначає вектор похідних від трьох керованих змінних.

І якщо вектор керування u у (18) являє лінійну функцію керованих змінних виду

$$\boldsymbol{u} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \\ n_3 \end{pmatrix}, \qquad (19)$$

де k_{11}, k_{12}, k_{13}, k_{21} k_{22}, k_{23}, k_{31}, k_{32}, k_{33} - коефіцієнти підсилення лінійного регулятора, то підставляючи у (18) вираз (19) отримаємо кінцевий вираз для рівняння настроювання у замкненій формі.

У [5-7] показано, що похідні від керованих перемінних у виразі (18) однакові за величиною і протилежні за знаком, отже, їхня сума зберігається.

5. Синтез системи настроювання

Рівняння настроювання виду (17) забезпечує в адаптивному режимі аперіодичний (не коливальний) характер зміни поточних значень коефіцієнтів завантаження серверів ПА трафіком звернень виборців під час здійснення актів дистанційного голосування у напрямі їхнього вирівнювання. Але важливо мати можливість впливу на швидкість процесу вирівнювання. Адже фактор швидкодії є істотним, тому що пульсації трафіка можуть бути досить великими і за частотою і за тривалістю.

Поставимо задачу забезпечення заданої швидкодії процесу вирівнювання із заданою якістю перехідних процесів при обмеженні керування.

Якщо маємо рівняння настроювання виду (17), то доцільно скористатися результатами рішення задачі аналітичного конструювання регуляторів, які наведені у [5]. У цьому випадку функціонал I, значення котрого у процесі оптимізації має бути мінімізоване, слід задати у вигляді

$$I = \int_0^\infty (N^T C P C^T N + \alpha N^T C Q C^T N + u^T R u) dt, \qquad (20)$$

де P - $m \times m$-мірна квадратна симетрична не негативно визначена матриця вагових коефіцієнтів, яка задає «вагу» кожному регулюючому зв'язку між керованими змінними; α - позитивна константа – множник при функції Белмана у функціоналі – показник загасання функції Белмана; R - $m \times m$ - мірна симетрична позитивно визначена матриця вагових коефіцієнтів при керуваннях; Q - $m \times m$ - мірна позитивно визначена симетрична матриця квадратичної форми – складова функції Белмана; T - символ операції транспонування матриці.

Як бачимо із (20), сума у підінтегральному виразі функціоналу I складається із трьох членів.

Перший член підінтегрального виразу – це функція вирівнювання керованих змінних (див. вираз (15)). Вона згідно (16) являє собою зважену суму квадратів відмінків (через коефіцієнти матриці *P*) керованих змінних. У процесі вирівнювання ця сума має поступово зменшуватися. І чим вона більша, тим довше за часом здійснюється процес вирівнювання, тим буде більше значення функціоналу *I*. Так що, оптимізація параметрів процесу вирівнювання позитивно впливає на мінімізацію значення функціоналу *I*.

Другий член підінтегрального виразу - це є функція Белмана, яка уведена у функціонал у вигляді складової із заданим показником загасання. Звісно [5], що на оптимальних траєкторіях функція Белмана убуває із швидкістю підінтегрального виразу функціоналу *I*. Використаний у даній роботі функціонал є подібним тому, що запропонований в [5]. Згідно з побудовою його підінтегрального виразу функція Белмана на оптимальних траєкторіях в цьому випадку убуває із швидкістю не меншій за здобуток її самої та показника загасання α. Тому, шляхом вибору достатньо великого значення α є можливим забезпечити за умов замкнутої системи авторегулювання швидкодію не меншу за таку, що визначається показником загасання. Як бачимо, функція Белмана у даному випадку представлена як і функція вирівнювання - у вигляді квадратичної форми

$$V = N^T CQC^T N. \qquad (21)$$

Третій член підінтегрального виразу відображає конструкцію регулятора, тобто визначає структуру та алгоритм його роботи [5]. Його уведення у підінтегральний вираз функціоналу дозволяє обмежити керування та формально замкнути процедуру визначення оптимального керування.

Яким чином оптимізувати функціонал I, знайти вектор керування u та одержати остаточний вираз для замкнутої системи адаптивного розподілу навантаження між серверами ПА - детально розглянуто у теорії конструювання аналітичних регуляторів, зокрема у [5-7]. Ми ж обмежимся наведенням остаточних виразів, що представляють синтезовану систему настроювання.

Зокрема, шляхом диференціювання по вектору керування виразу, що представляє рівняння Белмана, і наступним прирівню-ванням результату нулеві, знайдемо вектор керування у наступному вигляді:

$$\begin{aligned} u &= -R^{-1}C^T CQC^T N, \\ u^T &= -N^T CQC^T CR^{-1}. \end{aligned} \qquad (22)$$

У виразі (23) вище були визначені усі його компоненти, окрім параметра Q - квадратичної форми складової функції Белмана. Визначення цієї квадратичної форми здійснюється шляхом рішення так званого рівняння Рікаті [5-7].

Якщо підставити визначений параметр Q у (23), то отримаємо остаточний вираз для шуканого регулятора у вигляді замкнутої системи настроювання

$$\dot{N} = -CR^{-1}C^T CQC^T N. \qquad (23)$$

Підкреслимо, що для замкнутої системи настроювання (24) при будь-якому початковому значенні вектору керованих змінних стале значення керованого вектору таке, що його компоненти є однаковими, а їхня сума протягом усього процесу настроювання є незмінною.

Висновки

1. Поставлена мета даного дослідження досягнута: вперше розроблено метод адаптивного розподілу потоку звернень виборців на обслуговування між серверами адресації системи дистанційного таємного голосування через Інтернет, що дозволяє:

– реалізувати вперше на практиці автоматичний пошук *ip*-адрес серверів виборчих дільниць;

– удосконалити технологію дистанційного доступу виборців до ресурсів системи ДТГ, зокрема здійснювати рівномірне завантаження серверного обладнання в умовах пульсацій трафіка і таким чином знижувати ризики перенавантаження обладнання трафіком;

– оптимізувати процес адаптивного регулювання механізму розподілу шляхом синтезу відповідної системи настроювання з використанням методу динамічного програмування Р.Белмана та результатів теорії конструювання аналітичних регуляторів.

2. Задача керування розподілом потоку запитів виборців на обслуговування для здійснення голосування між серверами ПА представлена як задача динамічного вирівнювання коефіцієнтів завантаження цих серверів. При цьому використано один із різновидів методу динамічного програмування Р.Белмана – метод аналітичного конструювання регуляторів, що дозволило оптимізувати параметри системи настроювання та узгодити їх із параметрами потоку звернень виборців.

3. З урахуванням умов функціонування системи ДТГ запропоновано та наповнено конкретним змістом відповідне диференціальне рівняння настроювання, що на формальному рівні відображає процес авторегулювання динамічним перерозподілом потоку звернень виборців між серверами ПА. Розглянуто можливі схеми рішення цього рівняння, зокрема для його чисельного інтегрування на кожному кроці запропоновано використати метод Ейлера або Адамса.

4. Оптимізовано процес настроювання системи адаптивного авторегулювання. Вибрано критерій оптимальності, що відповідає умові забезпечення рівності поточних значень коефіцієнтів завантаження серверів в устояному (рос. – установившемся) режимі, коли інтенсивності запитів, що надходять до ПА, є постійними та не відчувають флуктуацій. При цьому цільова функція оптимізації забезпечує мінімум кількості ПА у складі системи ДТГ (точніше кажучи, мінімум необхідного значення загальної пропускної спроможності цієї системи) при заданому рівні якості обслуговування запитів.

5. Під час аналітичного конструювання регуляторів побудована відповідна функція Белмана. Це дало змогу конкретизувати рівняння настроювання, задати оптимізуючий функціонал і записати відповідне їм рівняння Белмана.

6. Задачу аналітичного конструювання регуляторів зведено до рішення рівняння Рікаті – матричного квадратного рівняння, необхідного для пошуку матриці функції Белмана. Шляхом підстановки знайденої матриці у вираз для керування одержано остаточний вираз для шуканих регуляторів.

ЛІТЕРАТУРА

[1]. М. Пригара, Захищена система технічної підтримки процесів дистанційного волевиявлення. Рукопис. Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21. Системи захисту інформації. Національний авіаційний університет, Київ, 2018.

[2]. В. Чуприн, В. Вишняков, М. Пригара, "Захист операційного середовища систем Інтернет голосування", *Захист інформації*, Т. 19, №1, С. 56-66, 2017.

[3]. І. Мачалін, О. Комарницький, В. Гнатюк, "Удосконалення технології доступу до ресурсів транспарентних систем інтернет-голосування", *Наукоємні технології*, №4(40), С. 415-422, 2018.

[4]. Ascher Uri M., Petzold, Linda Ruth. C*omputer methods for ordinary differential equations and differential-algebraic equations*. 1998.

[5]. В. Антонов, "Метод построения качественных регуляторов", *Кибернетика и вычислительная техника*. - К.:ІК АНУ, 2000, Вип. 126, С. 40-48.

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

[7]. Ю. Кочергін, "Задача авторегулирования перераспределением пропускной способности пакетного комутатора между его портами", *Математичні машини і системи*, К.: ІК АНУ, Вип. 2, С. 60-70, 2006.

[8]. В. Антонов, "Теорема об устойчивости", *Теория и методы исследования авиационных автоматических систем и тренажеров. Выпуск 3*. Изд-во КИИГА, С. 14-19, 1993.

[9]. Мхамад Ібрагім Ахмад Альомар, Удосконалення технології управління розподілом ресурсів пакетних мереж. Рукопис. Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 Комп'ютерні системи та компоненти. Національний авіаційний університет, Київ, 2015.

МЕТОД РАСПРЕДЕЛЕНИЯ НАГРУЗКИ МЕЖДУ СЕРВЕРАМИ СИСТЕМЫ ИНТЕРНЕТ-ГОЛОСОВАНИЯ

Предложен метод оптимального адаптивного распределения потока запросов избирателей между специализированными серверами защищённой системы интернет-голосования, которые выполняют согласно запросам избирателей автоматический поиск *ip*-адресов нужных им серверов избирательных участков. За основу взята схема доступа избирателей к серверам избирательных участков, которая детально рассмотрена в [3]. Для автоматизации поиска в этой схеме использована линейка специализированных серверов поиска адресов (ПА), программные средства которых в ответ на запросы избирателей в реальном времени выполняют процедуру поиска в соответствии с любым из известных методов поиска, а найденные значения *ip*-адресов посылают на терминальные узлы инициаторов запросов. Наряду с линейкой серверов ПА, которые функционируют одновременно и независимо друг от друга, в состав оборудования системы дистанционного тайного голосования введён также дополнительный элемент – сервер-менеджер ПЗ (сервер перевода запросов), который в реальном времени должен выполнять адаптивное распределение потока запросов между серверами ПА с тем, чтобы обеспечить равномерную загрузку этих серверов в условиях непрогнозируемых всплесков (пульсаций) потока запросов во время голосования. Реализация этого метода позволяет усовершенствовать технологию дистанционного доступа избирателей к защищённым ресурсам транспарентной системы интернет-голосования. В частности, обеспечить равномерную загрузку серверного оборудования в условиях непрогнозируемых всплесков (пульсаций) трафика избирателей, а также возможность поддержки

принятого уровня защиты и качества обработки этих запросов (в частности, поддержки принятого значения среднего времени ожидания в очереди на обслуживание запроса) с использованием минимального количества серверного оборудования. Параметры этой технологии определены в результате решения соответствующей оптимизационной задачи, которая реализует метод динамического программирования Р. Бэллмана. В работе сформулирована соответствующая целевая функция, найден явный вид оптимизирующего функционала и функции Бэллмана, синтезировано уравнение Рикати, определён вектор управления.
Ключевые слова: атака посреднока, транспарентная система, Интернет голосование, защита информации, противодействие атакам посредника.

METHOD OF PARTITION OF LOAD BETWEEN SERVERS OF SYSTEM THE INTERNET VOTING

The method of optimal adaptive distribution of stream of queries of electors is offered between the servers of the system internet-voting, that produce the automatic search of ip-address of servers of electoral districts. For basis the chart of access of electors is taken to servers of electoral districts, that in detail is considered in [3]. For automation of search the line of the specialized servers of search of addresses (SA) is used in this chart. Programmatic facilities of these servers in reply to the queries of electors in real time execute procedure of search in accordance with any of the known methods of search. The found values of ip-addresses are sent on the terminal knots of initiators of queries.Along with the line of servers of SA that functions imultaneously and independent of each other, in complement of equipment of the controlled from distance secret voting system the additional element of queries is entered also. It is manager (server of translation of queries), that in real time must execute adaptive distribution of stream of queries between the servers of SA with that to provide the even loading of these servers in the conditions of the unforecast splashes (pulsations) of stream of queries during voting. Realization of method allows to perfect technology of the controlled from distance access of electors to the resources of the system internet-voting. In particular, to provide the even loading of server equipment in the conditions of the unforecast pulsations of traffic of electors, and also possibility of support of acceptable level of quality of treatment of these queries (in particular, support of acceptable value of mean time of expectation in a turn on maintenance of queries) with the use of the least of server equipment. Parameters of this technology are certainly as a result of decision of corresponding optimization task that will realize method of the dynamic programming of Bellman.
Keywords: transparent voting system over the Internet, server equipment, controlled from distance access, optimal distribution of traffic, method of the adaptive adjusting of R. Bellman.

Чуприн Володимир Михайлович, кандидат технічних наук, професор кафедри телекомунікаційних систем Національного авіаційного університету.
E-mail: mega_chupr@ukr.net.
Orcid ID: 0000-0001-9412-7413.
Чуприн Владимир Михайлович, кандидат технических наук, профессор кафедры телекоммуникационных систем Национального авиационного университета.
Chupryn Volodymyr, PhD in engineering, professor, Department of Telecommunication Systems, National Aviation University.

Антонов Веніамін Валерійович, кандидат технічних наук, доцент кафедри телекомунікаційних систем Національного авіаційного університету.
E-mail: mega_chupr@ukr.net.
Orcid ID: 0000-0003-2244-262X.
Антонов Вениамин Валерьевич, кандидат технических наук, доцент кафедры телекоммуникационных систем Национального авиационного университета.
Antonov Benjamin, PhD in engineering, associate professor of department of Telecommunication systems of the National aviation university.

Комарницький Олег Олександрович, головний спеціаліст, Департамент інформаційно-комунікаційних технологій Київської міської державної адміністрації.
E-mail: komarnitskiy2012@gmail.com.
Orcid ID: 0000-0003-4830-919X.
Комарницкий Олег Александрович, главный специалист, Департамент информационно-коммуникационных технологий Киевской городской государственной администрации.
Komarnitskiy Oleg, Chief Specialist, Department of Information and Communication Technologies of Kyiv City State Administration.