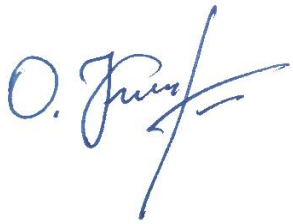
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ



КОМАРНИЦЬКИЙ ОЛЕГ ОЛЕКСАНДРОВИЧ

УДК 004.771

МЕТОДИ ТА МОДЕЛІ ВДОСКОНАЛЕННЯ ТРАНСПАРЕНТНОЇ ТЕХНОЛОГІЇ ТАЄМНОГО ІНТЕРНЕТ-ГОЛОСУВАННЯ

Спеціальність 05.13.06 – інформаційні технології

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ 2021

Дисертацією є рукопис.

Робота виконана на кафедрі телекомунікаційних та радіотехнічних систем Національного авіаційного університету (НАУ).

Науковий керівник: доктор технічних наук, професор
Мачалін Ігор Олексійович,
професор кафедри телекомунікаційних та радіотехнічних систем Національного авіаційного університету.

Офіційні опоненти: доктор технічних наук, професор
Юдін Олександр Костянтинович
завідувач спеціалізованої кафедри №31
Національна академія Служби безпеки України.

доктор технічних наук, професор
Корнієнко Богдан Ярославович
професор кафедри автоматики та управління в технічних системах
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Захист дисертації відбудеться «30» квітня 2021 р. о 15:00 годині на засіданні спеціалізованої вченої ради Д.26.062.01 у Національному авіаційному університеті (НАУ) (м.Київ, пр. Космонавта Комарова, 1, корп._, ауд. _____).

З дисертацією можна ознайомитися у Науково-технічній бібліотеці Національного авіаційного університету за адресою: 03680, м.Київ, пр. Космонавта Комарова, 1 .

Автореферат розісланий «___» _____ 2021 року.

Вчений секретар
спеціалізованої вченої ради,
кандидат технічних наук, доцент Т. Охріменко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. Згідно розпорядженню Кабінету Міністрів України від 8 листопада 2017 року № 797 «Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації» передбачено впровадження електронного голосування, а також електронних референдумів та електронних плебісцитів, що повинні базуватися на принципі підвищення довіри громадян до інструментів електронної демократії.

Особливої актуальності набули технології електронного голосування у 2020 році через появу вірусу COVID-19. З метою збереження здоров'я і життя людей та забезпечення розвитку наукової діяльності в умовах карантину Кабінет Міністрів України 15 липня 2020 р. прийняв Постанову № 607 «Про внесення змін до Порядку присудження наукових ступенів», яка дозволила вченим радам проводити засідання у режимі on-line з використанням засобів таємного дистанційного голосування. У відповідності до цієї постанови методи, що запропоновані у даній роботі, були з успіхом використані в умовах карантину для дистанційного голосування на засіданнях Вченої Ради Київського національного університету будівництва і архітектури 16 жовтня та 30 листопада 2020 року, а також з безпосередньою участю автора 4 грудня 2020 року з 19 до 20 години було проведено дистанційне таємне Інтернет голосування для обрання керівних органів Товариства Червоного Хреста України, де виборці голосували з різних областей України не покидаючи своїх міст.

Технології дистанційного таємного голосування через Інтернет (надалі - ДТГ) мають ряд беззаперечних переваг у порівнянні із традиційними технологіями голосування, котрі потребують обов'язкової присутності виборців під час голосування на виборчих дільницях. Із публікацій витікає, що у сучасних умовах основною перешкодою на шляху впровадження ДТГ є недовіра виборців щодо відсутності шахрайства з боку персоналу, який обслуговує засоби дистанційного голосування. Єдиним ефективним методом досягнення довіри людей є надання їм можливості аудиту усіх тих програмно-апаратних засобів ДТГ, які можуть викликати недовіру, а саме це є засоби, від яких залежить збереження таємниці голосів та чесність підрахунку. Вирішенню цих питань, а також скороченню витрат часу виборців на процедури дистанційного волевиявлення, присвячена дана робота.

Зв'язок роботи з науковими програмами, планами, темами. Висвітлені в дисертації наукові результати отримано, здебільшого, в рамках науково-дослідної роботи, яка була виконана Київським національним університетом будівництва і архітектури (КНУБА) на замовлення Державного НДІ автоматизованих систем у будівництві (ДНДІАСБ), що здійснює діяльність у сфері створення комп'ютерних систем для потреб будівельної галузі, та „Укртелеком" (Договори про НДР №165-ХО4 (№ держ. реєстрації 0113U000093), №513-9-931, №514-9-931, №401/03). Автор дисертації був виконавцем цих робіт. Отримані результати використовуються у навчальному процесі КНУБА при викладанні навчальної дисципліни «Комп'ютерні мережі та захист даних», у НТУУ КПІ на основі монографії автора з вересня 2020 року розпочато вивчення дисципліни «Протоколи та алгоритми електронного голосування», а також ідеї автора враховані у НАУ при формуванні змісту навчальної програми «Стратегії обслуговування та ремонту обладнання інфотелекомунікаційних систем».

Мета роботи – зменшення сумарних витрат часу виборців на процедури, що пов'язані з дистанційним голосуванням за рахунок автоматизації довготривалих

процедур та підвищення довіри виборців щодо збереження таємниці їх голосів і відсутності шахрайства у підрахунку шляхом побудови автоматизованої системи безперервного аудиту виборцями програмно-апаратних засобів та процесів, які виконують розшифровку та підрахунок голосів.

Задачі дослідження

1. Здійснити аналіз існуючих технологій ДТГ з точки зору забезпечення довіри виборців до програмно-апаратних засобів та їх технічної підтримки, а також витрат часу виборців на процедуру волевиявлення. Визначити ті характеристики, які негативно впливають на транспарентність програмно-апаратних засобів ДТГ та на якість обслуговування виборців. Визначити та обґрунтувати методи та моделі, що спрямовані на усунення виявлених недоліків.

2. Вирішити наукові завдання, що спрямовані на скорочення витрат часу на пошук *IP*-адрес серверів виборчих дільниць шляхом розробки *структурно-функціональної моделі автоматизації пошуку цих адрес* та відповідного протоколу інформаційної взаємодії програмно-апаратних засобів, що реалізують цей метод. У рамках створеної моделі автоматизації *розробити метод балансування* (вирівнювання) навантаження на сервери пошуку *IP* адрес.

3. Вирішити наукові завдання щодо забезпечення транспарентності системи ДТГ шляхом розробки *моделі аудиту виборцями програмно-апаратних засобів розшифрування та підрахунку голосів виборців*, а також *розробити метод дистанційної автентифікації виборців* у системі ДТГ з тим, щоб усунути необхідність здійснення очних перевірок виборців перед кожним голосуванням.

4. Створити програмно-апаратне середовище для реалізації вдосконаленої технології ДТГ. Упевнитись, що воно здатне забезпечити вимоги транспарентності та задовольняє вимогам щодо часу обслуговування запитів виборців. *Оцінити показники якості функціонування* цього середовища за різних умов використання.

Об’єктом дослідження є процес дистанційного таємного голосування з використанням мережі Інтернет.

Предметом дослідження є методи, моделі та засоби, що спрямовані на забезпечення транспарентності технології ДТГ і зменшення витрат часу виборців на процедури, що пов’язані з дистанційним голосуванням.

Методи дослідження. Адаптивне управління потоками запитів до серверного обладнання розроблено з використанням результатів теорії аналітичного конструювання регуляторів з урахуванням необхідності забезпечення сталості та дотримання показників якості перехідних процесів регулювання потоками запитів. Статистичні параметри створеної системи ДТГ оцінювались з використанням результатів теорії інформації та телетрафіку. Виявлення «слабких місць» у захисті систем ДТГ здійснено з використанням методів побудови комплексних систем захисту, що знайшли своє відображення у чинних нормативних документах з ТЗІ. Розробка методів забезпечення гарантованої конфіденційності та цілісності даних, що передаються каналами зв’язку, а також технології дистанційної автентифікації заснована на теорії криптографічних систем, у т.ч. теорії секретного зв’язку К. Шеннона. Програмне забезпечення удосконаленої системи ДТГ створено з використанням мови програмування *JavaScript*.

Наукова новизна одержаних результатів

1. Вперше розроблено *структурно-функціональну модель автоматизованого пошуку* виборцями *IP*-адрес серверів виборчих дільниць шляхом синтезу структури функціональних елементів цієї моделі та розробки протоколу інформаційної

взаємодії між цими елементами, що дозволяє зменшити витрати часу на здійснення актів волевиявлення в умовах великої кількості виборчих дільниць.

2. Вперше розроблено *метод балансування (вирівнювання) навантаження* на одночасно працюючі сервери, що входять до складу лінійки серверів пошуку *IP*-адрес. В основу методу покладено результати синтезу адаптивного регулятора розподілу потоку запитів виборців між серверами шляхом його зведення до відомої формально вирішеної крайової задачі аналітичного конструювання регуляторів на мінімізацію функціонала Р.Беллмана у класі неперервних динамічних систем регулювання щодо об'єктів, що описуються звичайними лінійними диференціальними рівняннями настроювання першого порядку, що забезпечує сталий режим вирівнювання значень коефіцієнтів завантаження серверів, тим самим запобігаючи можливим перенавантаженням в роботі серверів в умовах непередбачуваних пульсацій трафіку, за рахунок чого підвищується якість технічної підтримки процесу волевиявлення.

3. Дістав подальший розвиток *метод дистанційної автентифікації виборців* у транспарентній системі ДТГ, котрий за рахунок спеціалізованих серверів, що містять бази даних з біологічними або іншими унікальними ознаками виборців, дозволяє уникнути обов'язкової очної перевірки перед кожним актом голосування.

4. Вперше розроблено *модель безперервного аудиту виборцями програмно-апаратних засобів сервера голосування* за рахунок використання відкритого для перевірки монтажу міні комп'ютерів та автоматизації процедур аудиту за допомогою спеціалізованого сервера, який підключено до сервера голосування через спільну локальну мережу, а доступ виборців до нього реалізовано через захищений канал, де центр сертифікації *HTTPS* обирають представники виборців, при цьому інсталяція та запуск серверів виконується під наглядом виборців або їх довірених осіб у період часу, коли на серверах ще немає ніякої критичної інформації, а після запуску серверів виборці продовжують аудит дистанційно без втрати інформації про наявність чи відсутність втручань у роботу серверів, бо усі спроби таких втручань виявляються та реєструються сервером аудиту, що забезпечується спеціально розробленим програмним забезпеченням та відкритими для виборців правилами адміністрування і реєстрацією кодів з'єднань з виборцями на сервері голосування, що дозволяє позбавити виборців підозри про те, що сервер голосування являє собою «чорний ящик» з імітатором який демонструє виборцям нібито чесне голосування, а насправді розкриває і підмінює їхні голоси, бо така підозра руйнує довіру виборців, а також завдяки розробленій моделі виборці можуть самостійно у будь-який момент часу виявляти атаку посередника, яка є найнебезпечнішою загрозою для транспарентних систем ДТГ.

Практичне значення одержаних результатів

1. Використання вдосконаленої транспарентної технології ДТГ, що реалізована на основі розроблених методів та моделей, надала можливість кожному виборцю під час голосування контролювати наявність загроз, які можуть призвести до порушення таємниці голосів та вірності результатів волевиявлення, що усуває причини для недовіри громадян до запропонованої системи ДТГ.

2. Створено та апробовано у реальних умовах програмно-апаратне середовище з відповідною технічною документацією (лістінги програм, специфікації апаратних засобів, інструкції користувачам та адміністраторам), яке може бути використано для побудови транспарентних систем ДТГ будь-якої

розмірності у будь-яких сферах людської активності із заявленою в роботі функціональністю та якістю технічної підтримки процесу волевиявлення.

3. Розроблені специфікації протоколу взаємодії елементів системи ДТГ та відповідного програмного забезпечення (ПЗ) використано для створення інтерфейсів транспарентних систем ДТГ. Позитивною особливістю цих інтерфейсів у порівнянні з існуючими є те, що користування ними дозволяє виборцям впевнитись у відсутності загроз щодо порушення таємниці голосів та підробки результатів волевиявлення. Розроблені специфікації ПЗ підсистеми захисту інформації рекомендується застосовувати для виявлення атак посередника. Розроблені специфікації засобів автентифікації рекомендується використовувати для дистанційної автентифікації виборців з тим, щоб усунути необхідність проходження виборцями обов'язкової очної перевірки перед кожним голосуванням.

4. Результати роботи впровадженні у ДНДІАСБ, НАУ, НТУУ КПІ та КНУБА, де протягом останніх двох років регулярно проводяться вибори до органів студентського самоврядування. З жовтня 2020 року за допомогою запропонованої у даній роботі системи ДТГ проводяться голосування на засіданнях Вченої Ради КНУБА, а також з грудня 2020 року проводиться дистанційне таємне Інтернет голосування для обрання керівних органів Товариства Червоного Хреста України, де виборці голосують з різних областей України не покидаючи своїх міст.

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, отримані автором самостійно, обмежуються обсягом тих результатів наукової діяльності, які відображені у цій роботі. Із робіт, що опубліковані у співавторстві, у дисертаційній роботі використовуються результати, що отримані особисто здобувачем. (Творчий вклад здобувача у роботах із співавторами відображено у розділі «ПУБЛІКАЦІЇ ЗА ТЕМОЮ ДИСЕРТАЦІЇ»).

Апробація результатів дисертації. Результати досліджень дисертаційної роботи доповідались, обговорювались і отримали позитивну оцінку на:

1. Міжнародна науково-технічна конференція «Сучасні наукові дослідження та розробки: теоретична цінність та практичні результати» (м.Братіслава,14-19 березня 2016 р.).

2. 5-та міжнародної науково-практична конференція «Management of the development of technologies», Секція "Information technology development of education» (Kyiv, 30 – 31 March, 2018).

3. Науково-практична конференція до Дня місцевого самоврядування "Форум прямої демократії" (Київ, 4 грудня 2018 р.).

4. IX Міжнародна науково-практична конференція студентів, аспірантів та молодих вчених «Інформаційні технології: економіка, техніка, освіта» (Київ, 14-15 листопада 2018 р.).

5. Науково-практична конференція КНУБА (м. Київ, 2019).

6. V Всеукраїнська науково-практична конференція «Перспективні напрямки захисту інформації» ОНАЗ ім. О.С.Попова (м. Одеса, 2019)

Публікації. За результатами виконаних досліджень опубліковано 13 наукових робіт, з яких 6 робіт у фахових науково-технічних спеціалізованих виданнях, одна монографія та 6 тез доповідей на науково-технічних конференціях, 1 публікація у міжнародному виданні.

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу,

чотирьох розділів, висновків по кожному розділу та загальних висновків по роботі в цілому, списку використаних літературних джерел (122 найменувань), 2 додатки. Повний обсяг дисертації - 155 сторінок (без анотації), у тому числі 137 сторінок основного тексту, 29 рисунків, 12 таблиць.

ОСНОВНА ЧАСТИНА

У **вступі** обґрунтовано актуальність теми дисертації, сформульовано мету дослідження, визначено коло наукових задач, що підлягають вирішенню, вказано на наукову новизну, практичне значення отриманих результатів, наведено дані про їх апробацію та впровадження.

У першому розділі здійснено аналіз характеристик існуючих систем ДТГ, та розглянуто принципи їх функціонування. Операційна система сервера виборчої дільниці (ВД) у транспарентній системі ДТГ після певних процедур налаштування дозволяє виконувати користувачам ті, і тільки ті дії, що є елементами множини Q.

$$Q = V \cup A \cup K, \qquad (1)$$

де V – множина дій голосуючих виборців; A – множина можливих (штатних і нештатних) дій адміністратора сервера; K – множина дій контролюючих осіб.

F – множина всіх даних, що розміщені у файловій системі сервера, включаючи файли з програмами; C – множина відображень команд адміністратора сервера, D – множина файлів у директорії адміністратора; B – множина даних в оперативній пам'яті прикладної програми, причому $B \not\subset F$; M – множина даних для моніторингу запитів виборців, причому $M \subset B$.

Концептуальну модель такої системи ДТГ представлено на рис. 1.

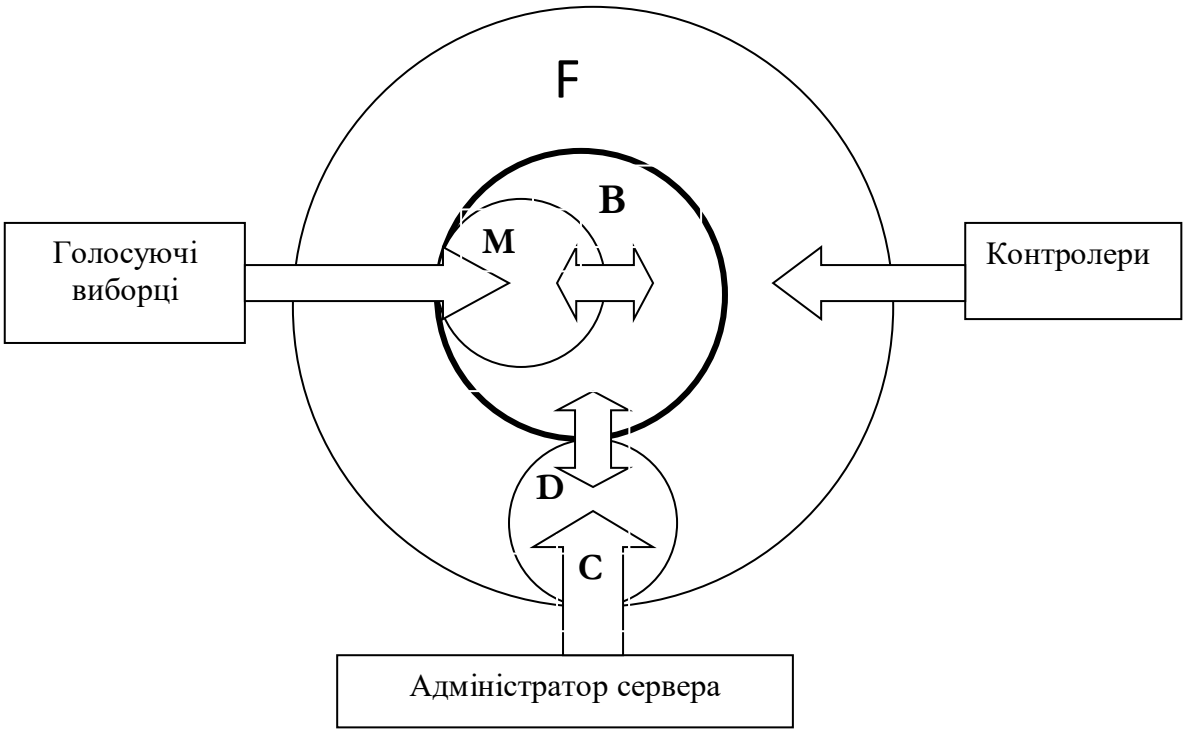


Рис.1. Концептуальна модель існуючої транспарентної системи ДТГ

Множини дій користувачів над цими об'єктами описують наступні вирази:

$$V = \{G_1, ..., G_i, ..., G_n\}, \quad (2)$$

де G_i – функція, яка відповідає і-тому варіанту запиту виборця до сервера, $i = \overline{1,n}$; n – кількість варіантів запитів виборця до сервера (наприклад: голосування, отримання довідки про хід голосування тощо).

$$A = W \cup E, \quad (3)$$

де W – множина дій адміністратора щодо приєднання файлів до множини D;
E – множина дій адміністратора щодо запуску на виконання файлів (програм) з множини D.

$$K = R \cup P, \quad (4)$$

де R – множина дій щодо доступу контролерів для ознайомлення з об'єктами множини F, причому $C \subset F$, $D \subset F$; P – множина дій контролера щодо перевірки статусу процесів на сервері.

На рис. 2 прийнято наступні позначення: ПБД ДВ – період заповнення бази даних претендентів на дистанційне волевиявлення; ПП ДВ – період завантаження електронних бюлетенів після остаточного коригування.

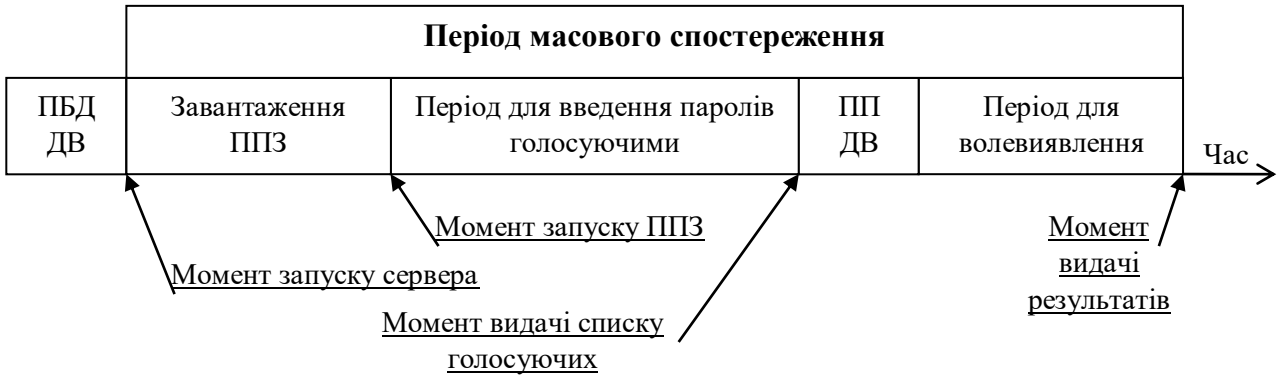


Рис. 2. Технологічний цикл функціонування транспарентної системи ДТГ

Аналіз структури системи ДТГ та технологічного циклу її функціонування виявив недоліки існуючої транспарентної системи, такі як відсутність аудиту апаратних засобів, які забезпечують збереження таємниці голосів та їх підрахунок, а також відсутність автоматизованого пошуку виборцями *IP* адрес серверів своїх виборчих дільниць і засобів дистанційної автентифікації осіб виборців, а також засобів контролю виборцями під час голосування дій адміністратора та виявлення атаки посередника *MITM* (*Man In The Middle*), яку вважають однією із найбільш небезпечних загроз в системах ДТГ.

Порівняння характеристик існуючих технологій ДТГ представлено у таблиці 1.

Таблиця 1

Порівняння технологій дистанційного таємного Інтернет-голосування

Опис технології	Критерій порівняння якості обслуговування виборців				
	Витрати часу на доступ до сервера	Витрати часу на процедуру голосування	Необхідність очної перевірки особи	Необхідність встановлення клієнтського програмного забезпечення	Прозорість апаратних засобів
Запропонована у роботі Пригари М.П.	Значні	Малі	Перед кожним голосуванням	Немає	Немає
Естонська система	Значні	Значні	Тільки один раз	Є	Немає
Запатентована у США US 2017/ 0109955	Значні	Значні	Тільки один раз	Є	Немає

Здійсненню наукових досліджень, пов'язаних з усуненням цих недоліків, присвячені наступні етапи даної роботи.

У другому розділі з метою скорочення витрат часу на здійснення актів волевиявлення розроблено систему та відповідну технологію автоматизованого пошуку виборцями *IP* адрес серверів ВД, до яких вони мають право на доступ. Розроблено структурно-функціональну модель автоматизації такого пошуку (див.рис.3) та відповідний протокол інформаційної взаємодії програмно-апаратних елементів цієї моделі.

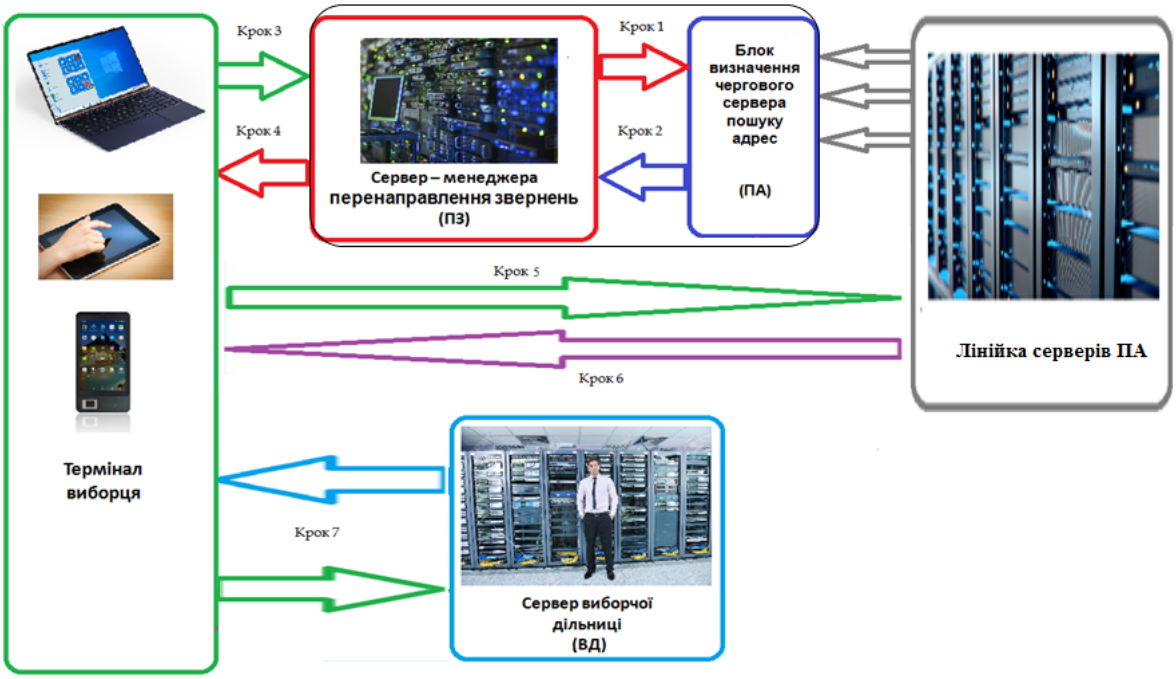


Рис. 3. Узагальнена структурно-функціональна модель автоматизації пошуку необхідних для здійснення голосування *IP*-адрес серверів ВД, до яких виборці мають право на доступ

Згідно розробленого протоколу, перш ніж запит виборця надійде на обробку до сервера ВД (дія 7), воно спочатку приймається сервером перенаправлення запитів виборців (ПЗ) (дія 3), який за допомогою блоку визначення сервера пошуку адрес (ПА) розподіляє у реальному часі потік запитів виборців між серверами лінійки серверів ПА (дії 1 та 2), реалізуючи механізм розподілу, що розглянутий нижче. Зокрема, сервер ПЗВ відправляє *IP*-адресу чергового сервера ПА, яка визначена механізмом розподілу (дія 4), і одразу після цього готується до обслуговування нового запиту від чергового виборця, переходячи до виконання дії 1. Отримавши *IP* адресу визначеного сервера ПА, термінал виборця звертається за цією адресою до цього сервера ПА для отримання від нього в інтерактивному режимі *IP* адресу сервера своєї виборчої дільниці. Визначений сервер ПА здійснює пошук цієї адреси (дія 5), у результаті термінал чергового виборця отримує від чергового сервера ПА *IP* адресу сервера ВД, що обслуговує даного виборця (дія 6).

Вищеназвана технологія базується на використанні програмно реалізованого на сервері ПЗВ адаптивного механізму розподілу потоків даних між серверами ПА, що підтримує процес розподілу робочого навантаження між серверами ПА у напрямку вирівнювання поточних значень їхніх коефіцієнтів завантаження за умов: 1) непрогнозованості сплесків (пульсацій) цього потоку у період голосування; 2) невизначеності щодо тривалості обробки кожного окремого запиту кожним із серверів ПА. (Під коефіцієнтом завантаження сервера ПА розуміється відношення проміжку часу, коли цей сервер безпосередньо здійснює обробку запитів, до тривалості часового інтервалу поточного кроку адаптації, тобто відображається значеннями безперервної величини у діапазоні від 0 до 1.) Для цих умов здійснено синтез регулятора розподілу потоку шляхом його зведення до відомої формально вирішеної крайової задачі аналітичного конструювання регуляторів на мінімізацію функціонала Р.Беллмана у класі динамічних систем регулювання щодо об’єктів, які описуються звичайними лінійними диференціальними рівняннями настроювання першого порядку. Під синтезом у даному випадку розуміється конструювання регулятора, що здатний забезпечити сталу траєкторію змін стану об’єкту регулювання у фазовому просторі C^2 із заданими характеристиками якості перехідного процесу. Синтезований регулятор відслідковує як динаміку змін інтенсивності вхідного потоку запитів (зокрема, використовуючи механізм, що реалізує відомий алгоритм відра токенів, згідно якого нестаціонарний потік перетворюється на послідовність часових відрізків сходинко подібного стаціонарного потоку із випадковими значеннями показника його інтенсивності), так і динаміку перехідного процесу вирівнювання названих вище коефіцієнтів з метою мінімізації похибок регулювання та з урахуванням обмежень, що забезпечують сталість системи регулювання.

Формальна постановка задачі синтезу шуканого регулятора, зокрема визначення рівнянь настроювання та вектора керування у замкнутій формі, передбачає необхідність представлення функціоналу *I*, що зв’язує в одне ціле параметри процесу розподілу, умови та обмеження, що накладені на цей процес, виразом (5):

$$I = \int_0^{\infty} (N^T CPC^T N + \alpha N^T CQC^T N + u^T Ru)dt \qquad (5)$$

,

де $\boldsymbol{N}$ – вектор керованих змінних, тобто вектор коефіцієнтів завантаження серверів ПА, траєкторію змін котрого слід визначити у фазовому простору C^2; $\boldsymbol{C}$ – матриця регулюючих зв'язків між серверами ПА, значення котрої визначаються на кожному кроці чисельного інтегрування рівнянь настроювання; $\boldsymbol{P}$ – діагональна позитивно визначена матриця вагових коефіцієнтів при регулюючих зв'язках між серверами ПА (у даному випадку вони однакові та дорівнюють *1*); $\boldsymbol{Q}$ - $m \times m$- мірна позитивно визначена симетрична матриця квадратичної форми як складова функції Ляпунова/Беллмана, що впливає на швидкість та сталість перехідного процесу вирівнювання змінних; α - позитивна константа – показник загасання функції Беллмана (цей параметр підбирається експериментально з тим, щоб знайти компромісне співвідношення між швидкістю перехідного процесу та величиною помилок вирівнювання змінних); $\boldsymbol{u}$ - вектор керуючих впливів, що знаходиться як лінійна функція компонентів вектору $\boldsymbol{N}$; $\boldsymbol{R}$ - $m \times m$ - мірна симетрична позитивно визначена матриця вагових коефіцієнтів при керуваннях (у даному випадку вони однакові та дорівнюють *1*); T - символ операції транспонування матриці; $[t_{0i}, t_{1i}]$ – часовий проміжок інтегрування, де t_{0i} - момент початку процесу вирівнювання керованих змінних на і-му поточному часовому інтервалі усереднення потоку запитів, а t_{1i} – момент закінчення цього інтервалу ($t_{1i} \to \infty$).

Перший член підінтегрального виразу у функціоналі (5) являє собою зважену суму квадратів відмінків (через коефіцієнти матриці $\boldsymbol{P}$) вирівнювальних змінних. Мінімізація значення функціоналу (5) приводить до вирівнювання змінних, що є керованими. Другий член функціоналу (5) є квадратична форма функції Ляпунова/Беллмана із показником загасання $\boldsymbol{\alpha}$, яка уведена у функціонал для визначення швидкості та обмеження процесу вирівнювання, що є важливим для забезпечення сталості цього процесу в умовах значних пульсацій трафіку. Третій член функціоналу обмежує керування та одночасно сприяє формальному замиканню процедури визначення керування. У даному випадку під керуванням розуміється вибір траєкторії змін вектору вирівнювальних змінних, що забезпечує сталість системи вирівнювання.

Відповідно до відомих результатів теорії аналітичних регуляторів у нашому випадку система настроювання має представлятися векторно-матричним диференційним рівнянням у вигляді:

$$\dot{N} = -CR^{-1}C^T CQC^T N\,, \tag{6}$$

а вектор керування у вигляді (7):

$$u = -R^{-1}C^T CQC^T N \;;\quad u^T = -N^T CQC^T CR^{-1}\;. \tag{7}$$

Як бачимо, вектор керованих змінних $\boldsymbol{N}$ пов'язаний з вектором керуючих впливів $\boldsymbol{u}$ через матрицю регулюючих зв'язків $\boldsymbol{C}$. Якщо дотримуватися визначених вище умов, та наведених нижче обмежень, то процес вирівнювання коефіцієнтів завантаження серверів буде здійснюватися по траєкторії, що мінімізує значення функціоналу (5). На кожному часовому інтервалі усереднення потоку запитів буде здійснюватися вирівнювання значень керованих змінних з похибками, що залежать як від тривалості цього інтервалу, так і від значення показника загасання α. Бажані значення часового інтервалу усереднення потоку та показника $\boldsymbol{\alpha}$ обираються експериментально.

Теорія аналітичних регуляторів для нашої системи визначає наступні обмеження:

1. Функція Беллмана повинна мати наступний вигляд (8):

$$V = N^T CQC^T N \quad . \tag{8}$$

2. Визначення матриці Q, що входить до складу функції Беллмана, має здійснюватися шляхом рішення рівняння (9), яке у даному випадку має виконуватися для будь-яких значень винесених за дужки множників:

$$N^T C \cdot (P + \alpha Q - QC^T CR^{-1} C^T CQ) \cdot C^T N = 0 . \tag{9}$$

3. Поточне значення інтенсивності потоку запитів у будь-який момент має не перевищувати величину загальної пропускної здатності серверів ПА.

В якості початкових умов роботи механізму вирівнювання задається кількість серверів ПА у лінійці та значення показника загасання α.

У результаті «роботи» рівнянь настроювання (відповідно з будь-яким методом чисельного інтегрування) з фізичної точки зору значення коефіцієнтів завантаження серверів ПА у реальному часі крок за кроком будуть вирівнюватися шляхом відповідного перерозподілу часток загального потоку запитів виборців між серверами ПА.

Шляхом комп'ютерного імітаційного моделювання подібної системи настроювання, що здійснено іншими дослідниками, показано, що якщо для некерованої системи розподілу запитів досяжним для лінійки серверів ПА є коефіцієнт завантаження 0,323, то для системи розподілу, замкнутої регулятором, можливий коефіцієнт завантаження може досягати значення 0,886. Названі кількісні показники отримано для випадку, коли пульсації трафіку моделювались з використанням відомої підпрограми генерації випадкових чисел, що рівномірно розподілені у довільно обраних межах.

У третьому розділі запропоновано модель безперервного аудиту виборцями програмно-апаратних засобів сервера голосування. Для цього поставлено та вирішено задачу синтезу системи контролю функціонування сервера голосування. На цьому сервері і тільки на ньому під час голосування може зберігатись інформація, з якою пов'язані питання довіри виборців. Тому треба надати доступ виборцям під час голосування до інформації з цього сервера, яка свідчить про неможливість розкриття таємниці голосів, а також про відсутність фальсифікацій щодо їх підрахунку. Інтерфейс для отримання такої інформації вже було запропоновано у роботі М.П. Пригари. Це є інтерфейс для контролерів (див. рис.1). Наша задача полягає у створенні захищеного каналу доставки інформації з цього інтерфейсу до виборців під час голосування. Крім того, слід обрати технічні засоби з відкритим монтажем, який би спрощував процедуру аудиту. Також для захисту каналу від електромагнітних випромінювань розроблено інформаційну технологію автоматизованого радіомоніторингу.

Для розв'язання даної задачі сервер голосування реалізовано на відкритій платі міні комп'ютера, до якого через спільну локальну мережу *Ethernet* підключено спеціалізований сервер аудиту. Таке підключення виключає можливість реалізації атаки посередника між серверами, бо розірвання зв'язку фіксується як порушення. Принцип роботи контролюючого сервера полягає у наступному. Періодично кожні декілька секунд цей сервер за протоколом *SSH* звертається до сервера голосування за інформацією про поточні активні процеси (команда *ps -aux*). На процеси, що запущені контролерами і операційною системою

цей сервер не реагує, а у разі появи будь-якого іншого процесу – протоколюються його параметри і відправляється сигнал тривоги на пристрої, які вказані контролерами. Необхідно, щоб встановлювали і підключали контролюючі сервери представники виборців, або щоб це відбувалось під їх наглядом. Підключення контролюючих серверів і їх запуск слід робити у той час коли на сервері голосування ще не має критичної інформації. Тому ніяких обмежень щодо доступу виборців та їх довірених осіб для перевірки апаратних засобів вводити не потрібно. Цим забезпечується довіра громадян до засобів розшифровки і підрахунку голосів, бо інакше може виникати підозра у тому, що сервер голосування являє собою «чорний ящик» з імітатором який демонструє виборцям нібито чесне голосування, а насправді розкриває і підмінює їхні голоси. Після запуску контролюючого сервера виборці можуть продовжувати безперервний контроль у дистанційному режимі без втрати інформації про можливі порушення. Слід зауважити, що будь-якій групі громадян можна дозволяти встановлення своїх контролюючих серверів (фізичних або логічних) у необмеженій кількості. Для доступу виборців до цих серверів слід використовувати протокол *HTTPS* з вибором центру сертифікації на розсуд громадян. Програма контролюючого сервера виявляє і протоколює усі дії адміністратора щодо управління сервером голосування. Адміністратор повинен керуватись спеціальною відкритою для виборців інструкцією, яка зобов'язує після кожного сеансу управління сервером голосування перед завершальною командою ***exit*** вводити команду ***history > haabbccdd.txt*** , де замість букв ***aabbccdd*** слід вказати дату і час завершення сеансу роботи, а саме так: ***aa*** – номер місяцю, ***bb*** – число, ***cc*** – години, ***dd*** – хвилини. При цьому буде утворено файл з усіма командами, які були введені адміністратором у даному сеансі роботи. Це дозволяє виборцям контролювати роботу адміністратора шляхом порівняння змісту створених файлів з переліком штатних команд.

Також через контролюючий сервер кожен виборець може впевнитись у тому, що він спілкується зі штатним сервером голосування, а не з підробкою зловмисників.

Концептуальна модель вдосконаленої системи ДТГ представлена на рис.4;

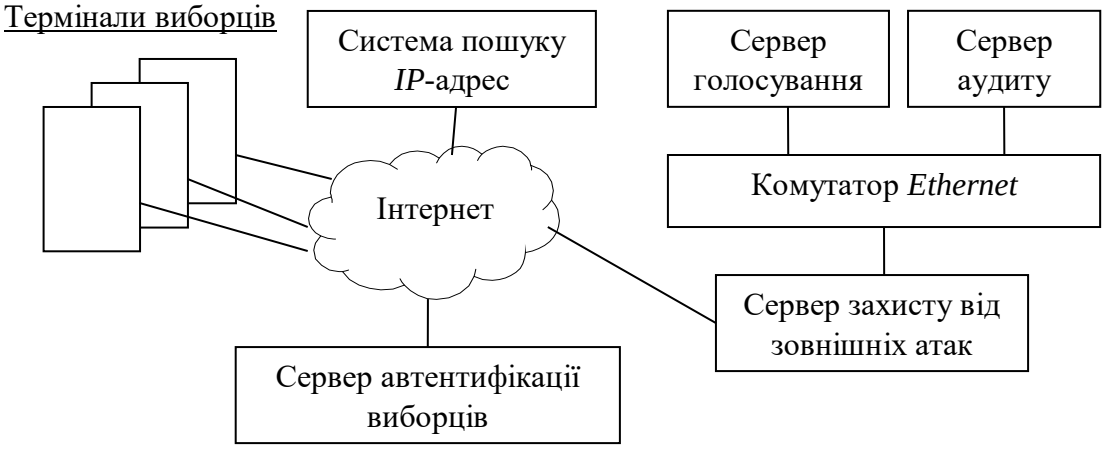


Рис. 4. Концептуальна модель вдосконаленої системи ДТГ

Для виявлення атаки посередника виборець через клавішу аудиту отримує доступ до журналу реєстрації з'єднань з сервером. Фрагмент цього журналу показано на рис.5.

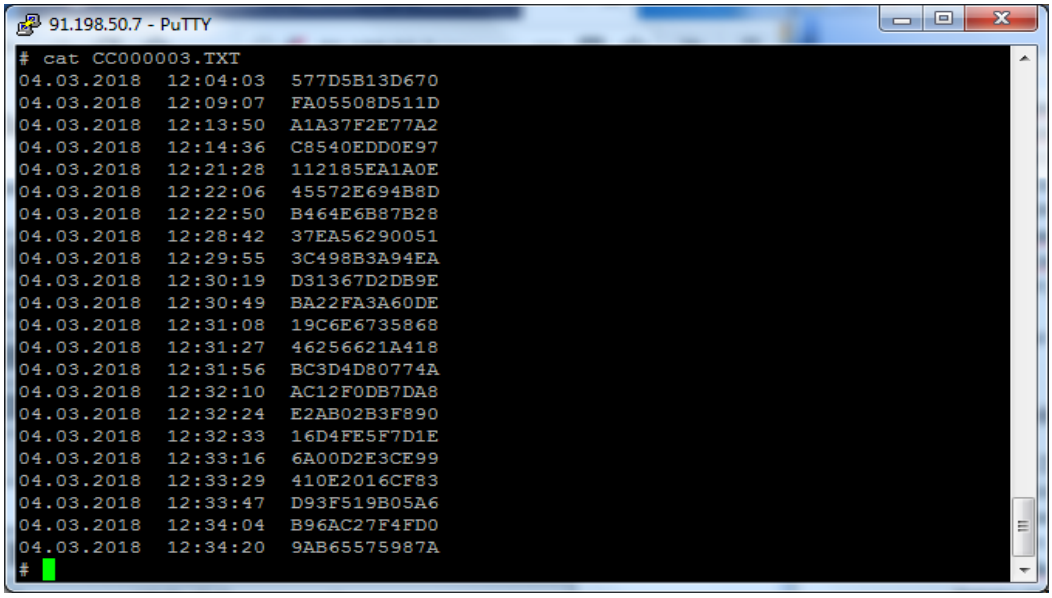


Рис. 5. Результат роздруківки сторінки журналу реєстрації з’єднань з сервером

У цьому журналі, крім дати і часу з’єднання роздруковуються коди, що являють собою випадкову степінь примітивного елементу поля Галуа, яка відправляється виборцю для обміну ключами за алгоритмом Діффі-Геллмана.

Представлення виборцю даних для перевірки з’єднання з сервером показано на рис. 6.

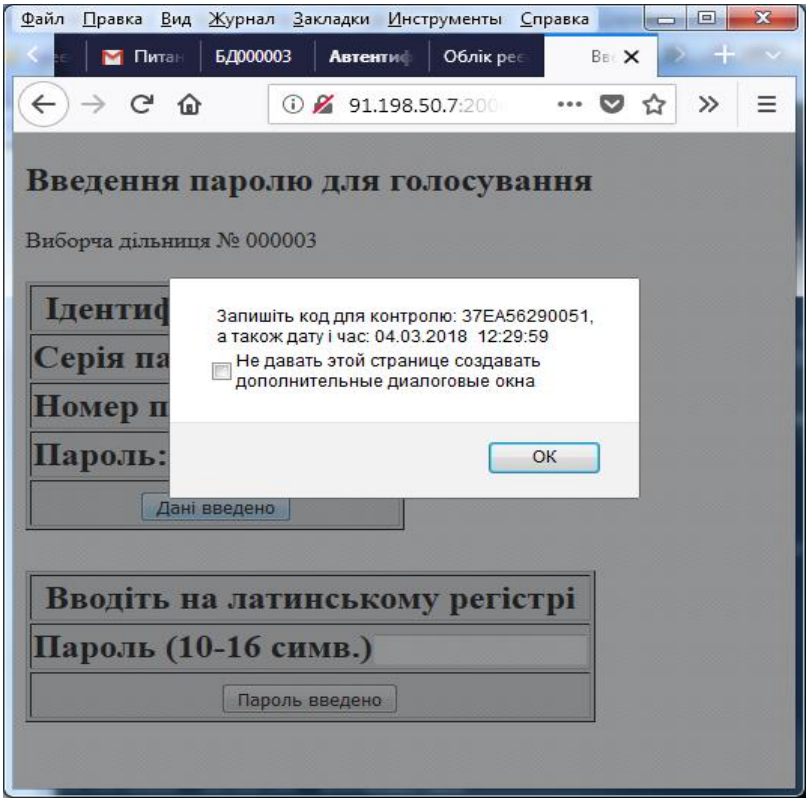


Рис. 6. Представлення виборцю даних для перевірки з’єднання з сервером

Шляхом порівняння кодів на момент часу свого запиту у журналі і в отриманому повідомленні може одразу впевнитись, що він дійсно спілкується зі штатним сервером для голосування.

У разі реалізації атаки посередника зловмисник повинен для обміну ключами з виборцем використовувати свою випадкову степінь, код якої не може співпадати з кодом, що занесений у журнал сервера для голосування. Звернення виборця через контролюючий сервер до журналу на сервері ВД відбувається за протоколом *HTTPS*, що виключає можливість атаки посередника на цьому з'єднанні, а контролюючий сервер підключено у єдину мережу *Ethernet* із сервером для голосування, де неможливо розірвати з'єднання для реалізації атаки, бо наявність зв'язку між цими серверами контролюється безперервно.

Поставлено та вирішено завдання з розробки методу автоматичної дистанційної автентифікації виборців, що придатний для використання у транспарентних системах ДТГ. Метод може знайти застосування для підтримки процедури отримання виборцем парольної інформації на свій термінал у дистанційному режимі, що виключає необхідність фізичної присутності цього виборця на виборчій дільниці для очної перевірки його особи та суттєво зменшує трудовитрати працівників виборчих дільниць. Метод передбачає створення додаткового програмно-апаратного елемента системи ДТГ - спеціалізованого сервера, що надає дозвіл/заборону на уведення потенційними виборцями паролів для здійснення актів волевиявлення (сервер ДВП).

Початкові умови використання технології:

1) створення сервера ДВП.

2) створення на сервері ДВП бази даних (БД) з унікальними біологічними та/або іншими ознаками виборців, що дозволяють автентифікувати особи виборців.

3) встановлення на сервері ДВП сертифікованого ПЗ для розпізнавання осіб виборців по ознакам, що занесені у БД.

Послідовність реалізації процесів, що складають технологію дистанційної автентифікації виборців:

1. Реалізація за запитом виборця процесу утворення захищеного з'єднання між виборцем та сервером ДВП (через обмін ключами за алгоритмом Діффі-Геллмана).

2. Реалізація процесу ідентифікації виборця з метою отримання дозволу на здійснення процедури авторизації через утворене захищене з'єднання (у результаті виборець отримує запит на введення біологічних або інших додаткових ознак своєї особи).

3. Реалізація процесу автентифікації виборця (Виборець виконує запит до сервера ДВП щодо введення додаткових ознак та отримує повідомлення про вдалу автентификацію і надання 10 хвилин для введення паролю. У разі невдалої автентифікації виборець отримає запрошення на повторну спробу введення додаткових ознак. Кількість унікальних ознак виборця, що враховуються, не обмежується прийнятою політикою безпеки).

4. Повторна реалізація за запитом виборця процесу утворення захищеного з'єднання між виборцем та сервером ДВП (через обмін ключами за алгоритмом Діффі-Геллмана).

5. Реалізація процесу авторизації виборця (Виборець авторизується через захищене з'єднання на сервері дистанційного голосування (ДГ) і очікує дозвіл на відправку пароля).

6. Реалізація процесу утворення захищеного з'єднання між сервером ДГ та сервером ДВП (через обмін ключами за алгоритмом Діффі-Геллмана).

7. Реалізація процесу обміну даними щодо ідентифікатора виборця між сервером ДГ та сервером ДВП (Сервер ДГ відправляє на сервер ДВП запит з ідентифікатором виборця і, якщо момент запиту вкладається у виділені 10 хвилин, отримує відповідь з цим самим ідентифікатором).

8. Реалізація процесу отримання дозволу виборцем для введення паролю (Сервер ДГ відправляє на термінал виборця дозвіл для введення паролю).

9. Реалізація процесу відправки виборцем парольної інформації (Виборець відправляє на сервер пароль для голосування і отримує відповідь про успішне завершення процедури).

Схема інформаційної взаємодії програмно-апаратних компонентів транспарентної системи ДТГ, що реалізують наведену вище послідовність процесів дистанційної автентифікації представлена на рис. 7.

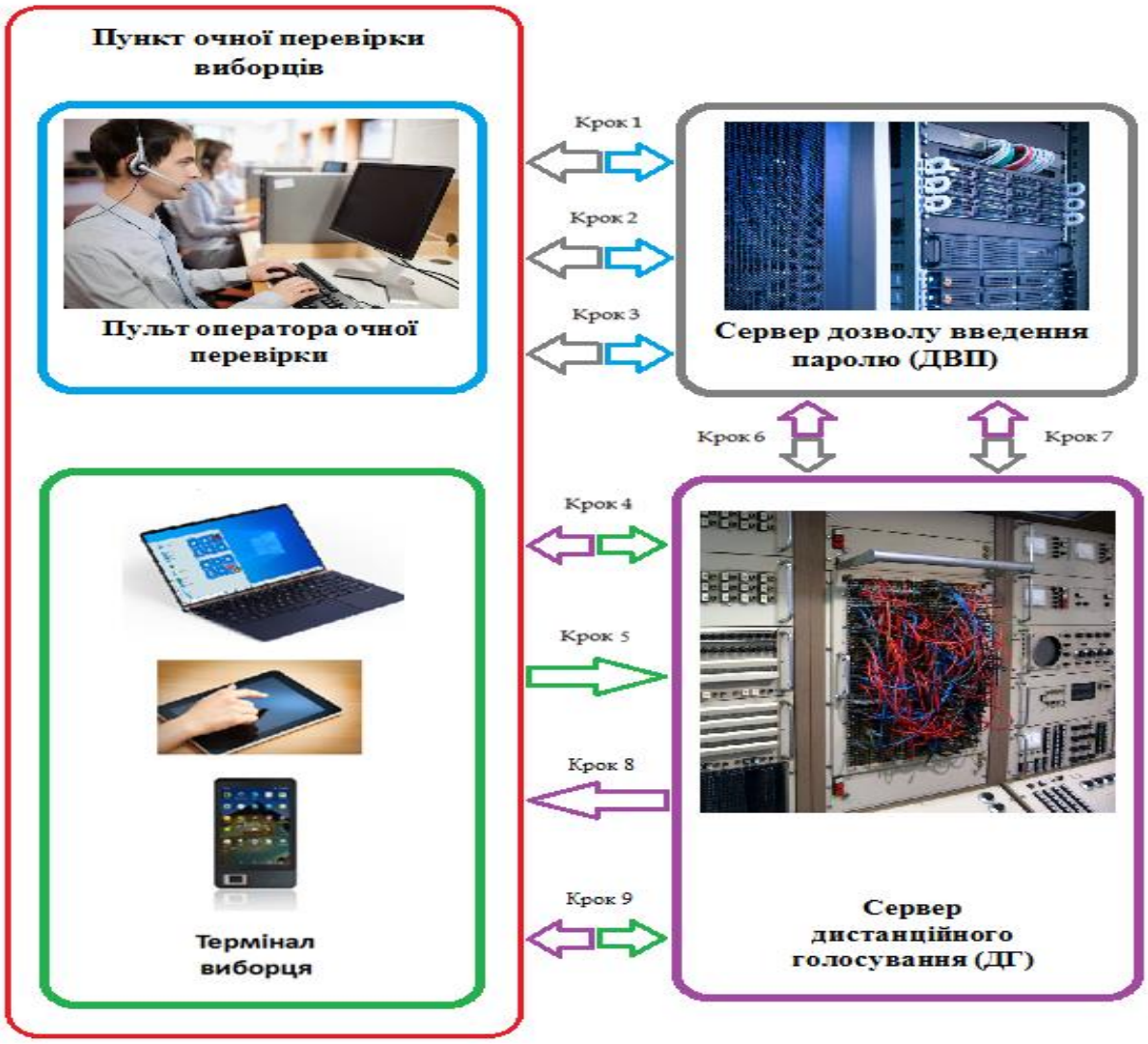


Рис. 7. Ілюстрація роботи засобів підтримки технології отримання пароля для голосування без очної перевірки

У четвертому розділі описано експериментальне дослідження вдосконаленої транспарентної системи ДТГ з метою практичного доведення із підтвердженням на прикладі конкретної програмно-апаратної реалізації можливості побудови відкритої (повністю контрольованої) системи, де ключову роль при перевірці коректності функціонування грають користувачі мережі Інтернет, включаючи всіх без винятку громадян, які мають бажання проконтролювати вірність функціонування системи. Це дозволяє усунути привід для підозр у тому, що хтось має можливість для прихованих від громадян фальсифікацій чи інших порушень штатного режиму роботи системи, бо кожному, хто має подібні підозри, надається можливість аудиту системи. Експериментальну систему було побудовано так, щоб унеможливити приховані порушення штатного режиму роботи за рахунок вибору широко відомих програмно-апаратних засобів та доступних для громадян процедур контролю. Для проведення вимірювань часу обробки запитів в екстремальних умовах сплеску трафіка запитів було створено два додаткових режими у меню вибору дільниці («Пробний разовий пароль» та «Пробне голосування») на сайті http://vybir.knuba.edu.ua/ . Результати вимірювань наведено у таблиці 2.

Таблиця 2

Результати вимірювання часу обробки запитів виборців сервером на міні-комп'ютері *Raspberry Pi* 3*B*

Найменування запиту	Час обробки сервером, с	Час очікування відповіді клієнтом, с
Процедура введення одноразових паролів для голосування		
Виклик *HTML* документу	<0.01	1-5
Обмін ключами	<0.01	<1
Відправка даних з отриманням номеру в черзі на обробки	<0.1	1-5
Отримання результату обробки	2 (на кожний запит з черги)	2*q (q – номер в черзі)
Отримання коду для перевірки	<0.01	<1
Процедура голосування		
Виклик *HTML* документу	<0.01	1-5
Обмін ключами	<0.01	<1
Відправка даних з отриманням номеру в черзі на обробки	<0.1	1-5
Отримання результату обробки	2 (на кожний запит з черги)	2*q (q – номер в черзі)
Отримання коду для перевірки	<0.01	<1

Отримані результати вимірювання часу обробки запитів сервером, а також часу очікування відповіді від сервера показують, що у разі одночасного звернення до сервера 30 виборців затримка обробки запитів сервером не перевищить двох

хвилин, а під час голосування сервер здатен обслуговувати за годину більше ніж 1500 виборців. Це свідчить про те що, застосування даної системи на міні-комп'ютерах *Raspberry Pi* 3*B* цілком задовольняє вимогам щодо швидкодії обслуговування, бо кількість виборців на дільниці не може перевищити 2500.

Удосконалено технологію ДТГ з урахуванням обмежень, що пов'язані із забезпеченням її транспарентності. Зміст зроблених удосконалень:

1. Автоматизовано пошук *IP* адрес серверів виборчих дільниць, що дозволило виборцям не витрачати зайвий час на здійснення такого пошуку.

2. Реалізовано технологію дистанційної автентифікації, що усунуло необхідність очної перевірки виборців і, от же, необхідність фізичної присутності виборців на виборчих дільницях в період уточнення їхніх списків.

3. Реалізовано метод аудиту виборцями дій адміністратора щодо управління сервером голосування, а також метод виявлення атак посередника, що дозволяє впевнитись у відсутності загроз щодо розкриття таємниці голосів чи фальсифікації результатів волевиявлення.

ВИСНОВКИ

1. Здійснено аналіз характеристик існуючих технологій ДТГ на предмет наявності у них дієвих механізмів контролю коректності їхнього функціонування з боку суспільства, оскільки вони забезпечують гарантії збереження таємниці голосів та істинності результатів волевиявлення за умов, коли відсутня довіра до всіх без винятку суб'єктів, що можуть бути зацікавлені у результатах волевиявлення. Проаналізовано також можливості існуючих технологій щодо якості надання послуг виборцям та технічної підтримки процесу волевиявлення. Виявлено наступні недоліки існуючих технологій ДТГ:

1) відсутність можливості виконувати безперервний аудит дій адміністратора щодо управління сервером голосування та виявляти атаки посередника, що негативно впливає на рівень довіри громадян до процесу волевиявлення;

2) відсутність автоматизованого пошуку виборцями *IP* адрес своїх виборчих дільниць, що потребує зайвих витрат часу при дистанційному голосуванні;

3) відсутність автоматизації процесу автентифікації виборців, що обумовлює необхідність здійснення обтяжливих очних перевірок осіб виборців в період уточнення списків голосуючих перед кожним актом волевиявлення.

Тому були визначені як актуальні наукові завдання розробки методів забезпечення транспарентної роботи засобів ДТГ і автоматизації процесів пошуку виборцями *IP* адрес серверів їхніх виборчих дільниць та автоматизації процесів, які ускладнюють процедуру волевиявлення, потребуючи зайвих витрат часу.

2. Розроблено структурно-функціональну модель автоматизації пошуку виборцями *IP* адрес серверів їхніх виборчих дільниць, а також протокол інформаційної взаємодії елементів цієї моделі. Оскільки пошук *IP* адрес є довготривалою процедурою, то передбачено застосування лінійки одночасно працюючих серверів для цього пошуку. Згідно розробленого протоколу, запити виборців приймаються сервером, який розподіляє весь потік запитів між серверами пошуку *IP* адрес. Застосування даної моделі скорочує витрати часу на здійснення актів волевиявлення.

3. Розроблено метод балансування (вирівнювання) навантаження на одночасно працюючі сервери, що входять до складу лінійки серверів автоматизованого пошуку *IP* адрес. Оскільки потік запитів характеризується

непередбачуваними пульсаціями, то для вирівнювання навантаження на ці сервери обрано адаптивний принцип роботи, що здійснює розподіл потоку запитів виборців з урахуванням динаміки змін як інтенсивності потоку запитів, так і тривалості пошуку адрес кожним із серверів. Регулятор діє у напрямку вирівнювання значень коефіцієнтів завантаження серверів, тим самим запобігаючи можливим перенавантаженням в роботі лінійки серверів і, от же, можливим затримкам в обслуговуванні виборців.

4. Дістав подальший розвиток метод автентифікації виборців у системі ДТГ, котрий за рахунок введення спеціалізованих серверів дозволу введення паролю, що містять бази даних з біологічними або іншими ознаками виборців, та створення захищених з'єднань між цими серверами з сервером голосування, забезпечує можливість дистанційної додаткової автентифікації осіб виборців. Реалізація цього методу надає виборцям можливість позбутися обов'язкової очної перевірки перед кожним актом волевиявлення.

5. Запропоновано модель безперервного автоматизованого аудиту виборцями програмно-апаратних засобів сервера голосування за рахунок використання відкритого для перевірки монтажу міні комп'ютерів та автоматизації процедур аудиту за допомогою спеціалізованого сервера, який підключено до сервера голосування через спільну локальну мережу, а доступ виборців до нього реалізовано через захищений канал, де центр сертифікації обирають представники виборців, при цьому інсталяція та запуск серверів виконується під наглядом виборців або їх довірених осіб у період часу, коли на серверах ще немає ніякої критичної інформації, а після запуску серверів виборці продовжують аудит дистанційно без втрати інформації про наявність чи відсутність втручань у роботу серверів, бо усі спроби таких втручань виявляються та реєструються сервером аудиту, що забезпечується спеціально розробленим програмним забезпеченням та відкритими для виборців правилами адміністрування і реєстрацією кодів з'єднань з виборцями на сервері голосування, що дозволяє усунути можливість підозри про те, що сервер голосування являє собою «чорний ящик» з імітатором який демонструє виборцям нібито чесне голосування, а насправді розкриває і підмінює їхні голоси, бо така підозра руйнує довіру виборців.

6. Розроблена модель безперервного автоматизованого аудиту програмно-апаратних засобів сервера голосування дозволяє виборцям під час голосування самостійно виявляти атаки посередника шляхом порівняння кодів з'єднання, що надаються у повідомленнях під час голосування зі значеннями, які реєструються у журналі з'єднань на сервері голосування, до якого виборці отримують доступ через захищений протоколом *HTTPS* канал зв'язку з сервером аудиту.

7. Продемонстровано на прикладі конкретної програмно-апаратної платформи у складі міні-комп'ютерів *Raspberry Pi* 3*B*, операційної системи *OpenBSD* та програмного забезпечення *Node.js* можливість коректної реалізації усіх необхідних складових транспарентної системи ДТГ. Все це підтверджено під час проведення реальних виборів керівних органів Товариства Червоного Хреста України 4 грудня 2020 року, де виборці голосували з різних областей України не покидаючи своїх міст.

8. Отримані результати вимірювання часу обробки запитів сервером, а також часу очікування відповіді від сервера показують, що у разі одночасного звернення до сервера 30-ти виборців затримка обробки запитів сервером не перевищить двох хвилин, а під час голосування сервер здатен обслуговувати за годину більше ніж

1500 виборців. Це свідчить про те що, застосування даної системи на міні-комп'ютерах *Raspberry Pi* 3*B* цілком задовольняє вимогам ЦВК щодо швидкодії обслуговування, бо кількість виборців на дільниці не може перевищити 2500 осіб.

9. В умовах організації можливості альтеративного вибору порядку голосування (дистанційного через Інтернет або з безпосередньою фізичною присутністю на виборчій дільниці) використання міні-комп'ютерного обладнання є доцільним вже у теперішній час.

10. У разі прийняття відповідного виборчого законодавства впровадження транспарентних систем ДТГ на виборах до центральних органів влади з використанням міні-комп'ютерів, є можливим і доцільним вже сьогодні.

ПУБЛІКАЦІЇ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. В.М. Чуприн, В.М.Вишняков, О.О. Комарницький, «Метод протидії атакам посередника у транспарентній системі інтернет голосування», Захист інформації, Ukrainian Information Security Research Journal. - К.: НАУ, 2018. – Т.20. -№3. – С.180-187. *Здобувачу належить розробка основного принципу, що покладений в основу розробленого методу.*

2. І.О. Мачалін, В.М. Вишняков, О.О. Комарницький, «Технологія автентифікації виборців у відкритій системі інтернет-голосування», Науково-технічний журнал «РАДИОЭЛЕКТРОНИКА И ИНФОРМАТИКА». - № 2(81), апрель – июнь 2018. - С. 55-63. *Здобувачу належить розробка основних ідей, що лежать в основі розробленої технології автентифікації.*

3. І.О. Мачалін, О.О. Комарницький, В.О. Гнатюк, «Удосконалення технології доступу до ресурсів транспарентних систем Інтернет-голосування, Науковий журнал «Наукоємні технології». - № 4 (40), 2018. - С. 415 – 423. *Здобувач розробив схему та протокол інформаційної взаємодії елементів серверного обладнання.*

4. В.М. Чуприн, В. О. Антонов, О. О. Комарницький, «Метод розподілу навантаження між серверами системи інтернет-голосування», Захист інформації Ukrainian Information Security Research Jornal. – К.:НАУ, 2019. – Т. 21. - №1, - С. 25-34. *Здобувачу належить ідея застосування адаптивного регулювання потоком запитів виборців із застосування методу динамічного програмування.*

5. В.М. Вишняков, О.О. Комарницький, А.О. Жуковський, «Методи контролю керування системою Інтернет голосування», Управління розвитком складних систем. – 2019. - № 38 – С. 82-89. *Здобувачу належить розробка методу виявлення позаштатних проникнень до сервера виборчої дільниці під час його функціонування.*

6. С.В. Цюцюра, О.О. Комарницький, «Застосування новітніх інформаційних технологій в Україні», Сучасні наукові дослідження та розробки: теоретична цінність та практичні результати: тези Міжнародної науково-практичної конференції (14-19 березня 2016 р., Братислава), 2016, С. 155-156.

7. О.О. Комарницький, Г.Б. Нестерук, «Захист систем дистанційного опитування від атак посередника», Матеріали 5-ої міжнародної науково-практичної конференції «Management of the development of technologies», Секція "Information technology development of education» (Kyiv, 30 – 31 March, 2018), Київ, С.76.

8. П.В. Ворона, В.М. Вишняков, О.О. Комарницький, Д.Ю. Хлапонін, «Принципи побудови транспарентних систем таємного електронного голосування»,

Науково-практична конференція до Дня місцевого самоврядування "Форум прямої демократії", 4 грудня 2018 р.: тези доп. – К., 2018. – С.169-171.

9. О.О. Комарницький, Д.Ю. Хлапонін, «Системи таємного електронного голосування як елемент цифрової демократії», IX Міжнародна науково-практична конференція студентів, аспірантів та молодих вчених «Інформаційні технології: економіка, техніка,освіта», 14-15 листопада 2018 р.: тези доп. – К., 2018. – С.169-171.

10. В.М. Вышняков, О.А. Комарницкий Транспарентные системы электронной демократии. Accent Graphics Communications & Publishing, Оттава, Канада, 2019, 98 с. *Здобувачу належить розробка основних ідей, що лежать в основі побудови транспарентних систем.*

11. О.О. Комарницький Особливості забезпечення безпеки інформації в системах електронної демократії. // Матеріали V науково-практичної конференції «Перспективні напрямки захисту інформації» ОНАЗ ім. О.С.Попова, тези доп. Одеса, 2019. - С. 23 – 25.

12. D.I.Bakhtiiarov, O.Y.Lavrynenko, N.O.Lishchynovska, O.O. Komarnytskyi, (2020) Methods of evaluation and forecasting of levels of electromagnetic radiation in urban environments (in Ukrainian) Actual issues of modern science. No. 1. Vol. 2, add. Collection of Scientific Articles, 06-2 (06), 1-17. European Scientific e-Journal. Hlučín-Bobrovníky: “Anisiia Tomanek” OSVČ. *Здобувачу належить розробка основного принципу захисту каналу від електромагнітних випромінювань в системах електронного голосування.*

13. В.М. Вышняков, О.А. Комарницкий, И.А. Мачалин Разрешение проблемы доверия к системам электронного голосования. «Colloquium-journal» Wydrukowano w «Chocimska 24, 00-001 Warszawa, Poland» №29 (81), 2020 Ч.1 С.44-50. *Здобувачу належить розробка основних ідей, щодо побудови систем електронного голосування для забезпечення довіри виборців.*

АНОТАЦІЯ

Комарницький О.О. Методи та моделі вдосконалення транспарентної технології таємного Інтернет-голосування – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – «Інформаційні технології». – Національний авіаційний університет, Київ, 2021.

Дисертаційна робота присвячена проблемі забезпечення довіри громадян до систем дистанційного таємного голосування через Інтернет (ДТГ), а також скороченню витрат часу виборців на процедуру волевиявлення.

Удосконалення спрямовані на підвищення рівня автоматизації трудомістких процедур та надання виборцям можливості аудиту системи ДТГ з метою набуття впевненості у відсутності зловмисного втручання у роботу сервера голосування, яке може призвести до розкриття таємниці голосів та фальсифікації підрахунку, що усуває причини для недовіри до чесності роботи системи ДТГ.

Побудовано модель та відповідний протокол інформаційної взаємодії елементів системи ДТГ, які завдяки застосуванню додатково розробленого серверного обладнання здатні підтримувати автоматизований пошук *IP* адрес серверів виборчих дільниць під час здійснення виборцями процедури Інтернет голосування і при цьому за рахунок розгалуження процесів уникати довготривалих затримок у доступі виборців до ресурсів системи Інтернет голосування. Розроблено технологію оптимального адаптивного розподілу потоку запитів виборців між

серверами, що здійснюють автоматизований пошук *IP* адрес серверів виборчих дільниць, реалізація якого дозволяє удосконалити технологію дистанційного доступу виборців до ресурсів системи ДТГ, зокрема рівномірно завантажувати серверне обладнання в умовах пульсацій трафіка і таким чином знижувати ризики перенавантаження обладнання трафіком. Запропоновано метод протидії атакам посередника (*MITM*) у відкритій системі ДТГ, який дозволяє кожному виборцю перед здійсненням акту волевиявлення за допомогою штатних термінальних засобів Інтернет самостійно впевнитись у тому, що він дійсно спілкується зі штатним сервером своєї виборчої дільниці, а не його фальшивим аналогом, що імітує процес волевиявлення для виборців. Удосконалено технологію дистанційної автентифікації виборців у системі ДТГ, завдяки чому створюються більш зручні умови голосування для виборців, зокрема не вимагається від них проходження обов'язкової очної перевірки перед кожним актом голосування.

Ключові слова: дистанційне таємне голосування, довіра до систем голосування, транспарентність, адаптивне управління потоком запитів, контрольованість програмно-апаратного засобів, дистанційна автентифікація.

ABSTRACT

Komarnitskiy O.O. Methods and models for improving the transparent technology of secret Internet voting. –Manuscript.

Dissertation on the receipt Candidate of Technical Sciences degree in specialty 05.13.06 are "Information technologies". - National aviation university, Kyiv, 2021.

The dissertation is devoted to the problem of ensuring citizens' trust in remote secret ballot systems via the Internet (RSB), as well as reducing the time spent by voters on the procedure of expression of will .

Improvements are aimed at increasing the level of automation of time-consuming procedures and giving voters the opportunity to audit the RSB system to ensure that there is no malicious interference with the voting server, which could lead to disclosure of votes and falsification of counting, which eliminates reasons for distrust of the RSB system.

A model and corresponding protocol of informative co-operation of elements of the system RSB are built. Due to application of the additionally worked out server equipment the system is able to support the automated search of IP-addresses of servers of electoral districts during realization of procedure electors the Internet of voting. Due to branching of processes the system is able to avoid of long duration delays in access of electors to the resources of the system the Internet voting.

The method of optimal adaptive distribution of stream of appeals of electors is used between servers that produce the automated search of IP addresses of servers of electoral districts. Realization of method allows to perfect technology of the controlled from distance access of electors to the resources of the system RSB, in particular evenly to load a server equipment in the conditions of pulsations of traffic and thus to reduce the risks of overload of equipment.

The method of counteraction to the attacks of mediator (MITM) is offered in open system RSB. A method allows to every elector before realization of act of will by means of regular terminal facilities the Internet independently to make sure of that he really intermingles with the regular server of the electoral district, but not him by a false analogue that imitates the process of will for electors.

Keywords: remote secret ballot, trust in voting systems, transparency, adaptive control of the flow of requests, controllability of software and hardware, remote authentication.