Голові спеціалізованої вченої ради
26.062.01
Національного авіаційного університету

03058, м. Київ, проспект Любомира
Гузара, 1

ВІДГУК

офіційного опонента

доктора технічних наук, професора кафедри автоматики та управління в технічних системах Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»
Корнієнка Богдана Ярославовича
на дисертацію здобувача кафедри телекомунікаційних та радіотехнічних систем Національного авіаційного університету **Комарницького Олега Олександровича**
на тему
"Методи та моделі вдосконалення транспарентної технології таємного інтернет-голосування",
що представлена на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 "Інформаційні технології"

Актуальність теми

Транспарентні технології дистанційного таємного голосування через Інтернет (надалі - ДТГ), тобто прозорі щодо можливостей всебічного контролю коректності виконання виборчих процедур з боку широкого загалу, мають ряд принципово важливих переваг у порівнянні із традиційними технологіями голосування, найбільш суттєвою із котрих є гарантоване забезпечення відсутності шахрайства з боку персоналу, який обслуговує засоби дистанційного голосування. У сучасних умовах традиційні технології волевиявлення, у т.ч. ДТГ, і не тільки в Україні, не викликають беззаперечної довіри людей щодо збереження таємниці голосів та чесності їхнього підрахунку. На сьогоднішній день тільки транспарентні системи ДТГ надають можливість будь-якій людині під час голосування здійснювати аудит усіх без виключень програмно-апаратних засобів ДТГ, які можуть викликати недовіру, і тим самим забезпечувати досягнення довіри до коректної роботи засобів технічної підтримки процедур голосування. Проте, зроблений пошукачем аналіз існуючої транспарентної технології ДТГ показав, що їй притаманний ряд недоліків, які перешкоджають її широкому впровадженню у практику суспільних відносин. Перш за все, це відсутність аудиту програмно- апаратних засобів, які забезпечують збереження таємниці голосів та їх підрахунок, 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. Усуненню цих недоліків, а також скороченню витрат часу виборців на процедури дистанційного волевиявлення, якраз і присвячена дисертаційна робота О.О. Комарницького. Так що, на мій погляд, обрана пошукачем тема цієї роботи є актуальною, оскільки розроблені у рамках цієї теми методи та моделі вдосконалення транспарентної технології таємного інтернет-голосування здатні надати не тільки кожному виборцю, але й будь-якому користувачеві Інтернету, змогу самостійно добути достатні докази того, що в запропонованій системі ДТГ не є можливим розкриття таємниці голосів та/або фальсифікування результатів волевиявлення.

Зв'язок дисертаційної роботи з пріоритетними напрямками розвитку науки і техніки, державними чи галузевими науковими програмами

Обрана здобувачем тема дисертаційної роботи відповідає сучасним потребам розвитку науки і техніки в Україні. Про це свідчить широкий ряд документів КМУ та ВРУ. Наприклад, Розпорядження Кабінету Міністрів України від 8 листопада 2017 року № 797 «Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації», Постанова КМУ №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, http://euinfocenter.rada.gov.ua/uploads/documents/28784.pdf та інші.

Оцінка змістовної частини дисертаційної роботи

Дисертаційна робота О.О. Комарницького складається зі вступу, чотирьох розділів з висновками по кожному розділу, загальних висновків по роботі в цілому, списку використаних літературних джерел (122 найменувань) та двох додатків.

У ***вступі*** надана характеристика систем ДТГ з точки зору забезпечення транспарентності процесу волевиявлення, сформульовано наукові завдання, що пов'язані із розробкою методів та моделей вдосконалення транспарентної технології ДТГ, розкрита сутність цих завдань, актуальність їхнього вирішення, обґрунтована доцільність проведення виконаних дисертаційних досліджень. Також визначено особистий внесок автора дисертації в отримані наукові результати. Зміст і форма викладу вступного матеріалу відповідає вимогам ВАК України до кандидатських дисертацій.

В ***першому розділі*** на основі порівняння основних характеристик існуючих систем ДТГ запропоновано в якості об'єкту удосконалення обрати існуючу транспарентну СДВ, концептуальну модель та технологічний цикл функціонування котрої проаналізовано в роботі. Аналіз виявив наступні недоліки існуючої транспарентної системи: 1) відсутність можливостей вичерпного контролю засобів технічного забезпечення ДТГ з боку широкого

загалу, які забезпечують збереження таємниці голосів та їх підрахунок; 2) відсутність автоматизованого пошуку виборцями *IP* адрес серверів своїх виборчих дільниць; 3) відсутність засобів дистанційної автентифікації осіб виборців; 4) відсутність засобів контролю виборцями під час голосування дій адміністратора; 5) відсутність засобів виявлення атак посередника *MITM* (*Man In The Middle*). Показано, що для усунення виявлених недоліків необхідно здійснити ряд наукових досліджень, результати яких викладено у наступних розділах даної роботи.

У ***другому розділі*** розроблено структурно-функціональну модель автоматизації пошуку необхідних для здійснення голосування *IP*-адрес серверів виборчих дільниць (ВД), до яких виборці мають право на доступ. Розроблено також відповідний протокол інформаційної взаємодії програмно-апаратних елементів цієї моделі, що дозволяє суттєво скоротити витрати часу на здійснення актів волевиявлення. У рамках вищеназваної моделі автоматизації синтезовано адаптивний механізм розподілу потоків даних між серверами пошуку адрес (ПА), що підтримує процес розподілу увідного потоку звернень виборців між серверами ПА у напрямку вирівнювання поточних значень їхніх коефіцієнтів завантаження з урахуванням непрогнозованого характеру пульсацій цього потоку та невизначеності щодо тривалості обробки кожного окремого звернення кожним із серверів ПА. Саме 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. Таким чином синтезований регулятор здатний забезпечити сталу траєкторію змін стану об'єкту регулювання у фазовому просторі C^2 із заданими характеристиками якості перехідного процесу. В роботі задано вигляд функціоналу Р.Беллмана, що зв'язує в одне ціле параметри процесу розподілу з умовами та обмеженнями, що накладені на цей процес. Визначено умови, за яких синтезований регулятор має відслідковувати як динаміку змін інтенсивності вхідного потоку запитів, так і динаміку перехідного процесу вирівнювання коефіцієнтів завантаження з метою мінімізації похибок регулювання та з урахуванням обмежень, що забезпечують сталість системи регулювання. Визначено рівняння настроювання та вектор керування у замкнутій векторно-матричній формі. Показано, що у результаті «роботи» рівнянь настроювання 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. В роботі стверджується, 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.

В ***третьому розділі*** запропоновано концептуальну модель всебічного

безперервного аудиту широким загалом виборців тих програмно-апаратних засобів сервера голосування, котрі можуть викликати сумніви з точки зору коректності їхнього функціонування. У рамках цієї моделі поставлено та вирішено задачу синтезу системи контролю функціонування цього сервера. Модель передбачає створення захищеного каналу доставки інформації з сервера до виборців під час голосування. У свою чергу, сервер голосування реалізовано на відкритій платі міні комп'ютера, до якого через спільну локальну мережу *Ethernet* підключено спеціалізований сервер аудиту. Показано, що таке підключення виключає можливість реалізації атаки посередника між серверами, бо розірвання зв'язку фіксується як порушення. Через контролюючий сервер кожен виборець може впевнитись у тому, що він спілкується зі штатним сервером голосування, а не з підробкою зловмисників.

Розроблена концептуальна модель вдосконаленої системи ДТГ дозволяє не тільки протидіяти атакам посередника, а і забезпечити автоматичну дистанційну автентифікацію виборців. У рамках цієї моделі розроблено метод автентифікації, що 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 спеціалізованого сервера, що надає дозвіл/заборону на уведення потенційними виборцями паролів для здійснення актів волевиявлення (сервер ДВП).

У ***четвертому розділі*** відображені результати експериментальних досліджень вдосконаленої системи ДТГ, яке здійснено з метою практичного доведення можливості побудови транспарентної (повністю контрольованої) системи, де користувачам мережі Інтернет надана можливість самостійної перевірки коректності функціонування усіх без виключень програмно-апаратних засобів системи ДТГ. Така можливість підтверджена на прикладі конкретної програмно-апаратної реалізації транспарентної системи голосування. Експериментальну систему було побудовано на міні-комп'ютерах *Raspberry Pi 3B* із застосуванням широко відомих програмно-апаратних засобів та доступних для громадян процедур контролю. Експериментально доведено, що ця система унеможливлює здійснення прихованих порушень штатного режиму роботи системи ДТГ. Результати вимірювання часу обробки звернень виборців цією системою, зокрема, показують, що у разі одночасного звернення до системи тридцяти виборців затримка в обробці звернень сервером не перевищує двох хвилин, при цьому сервер на міні-комп'ютерах здатен обслуговувати за годину більше ніж 1500 виборців. Це свідчить про те що, застосування даної системи на міні-комп'ютерах *Raspberry Pi 3B* цілком задовольняє вимогам щодо швидкодії обслуговування, якщо кількість виборців на дільниці не перевищує 2500 осіб.

У ***висновках*** відображено основні отримані пошукачем наукові та практично важливі результати. У ***додатку 1*** містяться тексти програм для реалізації транспарентної технології дистанційного таємного волевиявлення,

а у ***додатку 2*** - акт впровадження отриманих пошукачем результатів.

Список використаних джерел оформлено з урахуванням відповідних вимог та складається із 122 найменувань публікацій, що мають безпосереднє відношення до теми дисертації.

У цілому, зміст роботи спрямований на досягнення поставленої пошукачем мети та у повній мірі відповідає сформульованим задачам. Рішення цих задач є суттю та змістом виконаного наукового дослідження.

Дисертація оформлена у відповідності з прийнятими стандартами, стиль викладення в ній матеріалу має науковий характер і забезпечує доступність та однозначність їхнього сприйняття.

Наукова новизна роботи полягає у наступному:

1) вперше розроблено *структурно-функціональну модель автоматизованого пошуку* виборцями *IP*-адрес серверів виборчих дільниць на основі результатів синтезу структури функціональних елементів цієї моделі та розробки протоколу інформаційної взаємодії між цими елементами, що дозволяє автоматизувати процес та зменшити витрати часу на здійснення такого пошуку;

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;

3) дістав подальший розвиток *метод дистанційної автентифікації виборців у транспарентній СДВ*, котрий за рахунок використання спеціалізованих серверів, що містять бази даних з біологічними або іншими унікальними ознаками виборців дозволяє уникнути обов'язкової очної перевірки перед кожним актом інтернет-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.

Достовірність отриманих в дисертації наукових результатів підтверджена експериментальними дослідженнями на натурних моделях, а також результатами використання удосконаленої пошукачем транспарентної технології ДТГ на практиці.

Практичне значення отриманих результатів полягає в тому, що

1) використання вдосконаленої транспарентної технології волевиявлення, 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 істинності результатів волевиявлення, що усуває причини для недовіри громадян щодо істинності отриманих результатів голосування та гарантій збереження таємниці інтернет-голосування;

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 впроваджено 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 СДВ 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.

5) результати роботи впроваджено та обкатано в комп'ютерній мережі Державного науково-дослідного інституту автоматизованих систем в будівництві, де встановлено відповідне програмне забезпечення для визначення суспільних думок, проведення референдумів, здійснення конкурсних та виборчих процедур (підтверджено актом впровадження).

Ступінь обґрунтованості та достовірності отриманих наукових результатів, висновків та рекомендацій

Дисертант під час вирішення визначеного ним кола наукових завдань, що пов'язані між собою єдиною метою – удосконалити транспарентну технологію ДТГ шляхом усунення названих вище її недоліків - здійснив коректний аналіз та синтез методів та моделей, використання котрих на практиці дозволяє усунути основну перешкоду широкому впровадженню таких систем – недовіру виборців щодо забезпечення таємниці голосування та чесності підрахунку голосів. Пошукач спромігся у повній мірі обгрунтувати достовірність отриманих ним результатів аналізу та синтезу. При цьому він використав широко апробовані методи побудови комплексних систем захисту, що знайшли своє відображення у чинних нормативних документах ТЗІ. Адаптивне вирівнювання навантаження на лінійку серверного обладнання розроблено із залученням результатів теорії аналітичного конструювання регуляторів з урахуванням необхідності забезпечення сталості та дотримання показників якості перехідних процесів регулювання потоками звернень виборців в умовах непрогнозованого характеру сплесків таких потоків та невизначеності щодо тривалості обробки таких звернень. Статистичні параметри удосконаленої пошукачем системи ДТГ оцінювались з використанням результатів теорії інформації та телетрафіку. Розробка методів, що гарантують контрольованість середовища функціонування системи голосування з боку широкого загалу, виконана на основі результатів теорії побудови обчислювальних середовищ. Розробка методів забезпечення гарантованої конфіденційності та цілісності даних, що передаються каналами зв'язку, заснована на теорії криптографічних систем, у т.ч. теорії секретного зв'язку К. Шеннона. Обгрунтовано відповідний вибір операційної системи та апаратних засобів серверного обладнання.

Висновки та рекомендації, що сформульовані в дисертаційній роботі, у повній мірі враховують наукову та прикладну сутність поставлених пошукачем завдань. Вони є придатними для практичного використання.

Ідентичність змісту автореферату та рукопису дисертації

Автореферат і рукопис пояснювальної записки до дисертаційної роботи Комарницького О. О., відповідно до вимог МОН України, були розміщені в електронному депозитарії Національного авіаційного університету за один місяць до дати проведення процедури захисту.

На основі результатів аналізу змісту автореферату та тексту дисертації здобувача, можна зробити висновки, що основні положення дисертації адекватно відображені у змісті автореферату. В авторефераті з необхідною повнотою відображено загальну характеристику, основній зміст та висновки дисертаційної

роботи. Стиль викладення матеріалів дисертаційної роботи в цілому забезпечує достатню повноту викладу, однозначність та доступність їхнього сприйняття. Наукові завдання дослідження, шляхи їх вирішення, отримані результати та висновки викладено на достатньому рівні формалізму, без зайвих роз'яснень та міркувань. Цілком зрозуміло, у чому полягає наукова новизна отриманих результатів, наукова і практична цінність виконаної роботи та особисті здобутки пошукача.

Відповідність теми і змісту дисертації паспорту спеціальності, за якою вона подана на захист

Тема дисертації та її зміст у повній мірі відповідають формулі й галузі досліджень відповідно до положень, що викладені у паспорті спеціальності 05.13.06 – інформаційні технології.

Повнота викладення сформульованих наукових положень, висновків та рекомендацій в опублікованих працях

Основні результати дисертації достатньо повно опубліковані в наукових фахових виданнях, профіль яких відповідає спеціальності за якою дисертація подана на захист. За темою дисертаційної роботи опубліковано 13 наукових праць, в тому числі 6 із яких у фахових науково-технічних спеціалізованих виданнях та одна монографія. Крім того, зазначені положення дисертаційної роботи пройшли обов'язкову і достатню апробацію на міжнародних науково-практичних конференціях та семінарах в Україні та за кордоном (представлено 6 тез доповідей на науково-технічних конференціях). В авторефераті і дисертації наведено дані щодо конкретного особистого вкладу здобувача.

Кількість опублікувань результатів роботи та їх якість відповідає вимогам ВАК України до кандидатських дисертацій.

За аналізом матеріалів дисертаційної роботи можна відмітити наступні **зауваження та недоліки**:

1. В роботі не розглянуто питання стійкості транспарентних систем щодо можливих хакерських атак.

2. У другому розділі на сторінці 56 вказано, що у даному випадку доцільно обрати показник ефективності процесу авторегулювання, який описано виразом (2.5), але при цьому не надано пояснень щодо такого вибору. За поясненнями цього вибору необхідно звертатись до літературного джерела [117], що ускладнює ознайомлення з процесом вибору цільової функції.

3. На сторінці 65 після виразу (2.15) у реченні є помилкове посилання на вираз (2.1) замість (2.15).

4. На сторінці 77 роз'яснення щодо скорочення ППД (період підготовки даних про претендентів на роботу у режимі ДТГ) не можна вважати вдалим, бо голосування на виборах чи референдумах у нас не вважається роботою.

5. На сторінці 81 в одному реченні дублюється вираз «з ретельною перевіркою кожного з випромінювань», але не вказано у якому приміщенні і

як треба розміщувати технічні засоби для виявлення паразитних електромагнітних випромінювань.

6. На сторінці 89 вказано, що саме в період введення паролів для дистанційного голосування існує потреба у додаткових засобах розпізнавання осіб виборців, щоб уникнути можливої підміни особи голосуючого, але не надано додаткових роз'яснень з цього приводу.

7. На сторінках 91 і 92 використовується два різних скорочених позначень для сервера дистанційного голосування ДГ та ІГ.

8. Обране на рисунках 3.6 та 3.7 зображення сервера дистанційного голосування, що нагадує «чорний ящик», не можна вважати вдалим, бо, як бачимо з розділу 4, для цього сервера обрано міні-комп'ютер *Raspberry Pi* з відкритим монтажем, що показаний на рис. 4.11.

Слід відзначити, що наведені зауваження та недоліки суттєво не впливають на достовірність отриманих пошукачем наукових результатів та на загальне позитивне враження від роботи, не зменшують її наукової цінності та практичної значимості.

Висновки

Отримані пошукачем нові науково обґрунтовані результати, що підтверджені позитивними результатами відповідних експериментальних досліджень, а також позитивними результатами їхнього впровадження у практику суспільних відносин у повній мірі вирішують актуальне наукове завдання – забезпечити гарантії неможливості виникнення порушень цілісності результатів волевиявлення та конфіденційності персональних даних голосуючих за умов повної недовіри до всіх без винятку учасників процесу дистанційного волевиявлення, що усуває будь-які підстави для недовіри з боку голосуючих щодо можливості для реалізації вказаних порушень, а також мінімізації витрат часу голосуючими на здійснення актів волевиявлення.

В цілому, дисертаційна робота Комарницького О.О. є завершеною кваліфікаційною науковою працею, яку виконано здобувачем особисто у вигляді спеціально підготовленого рукопису, містить висунуті автором для захисту науково обґрунтовані результати, що переконливо свідчать про суттєвий особистий внесок здобувача в розвиток інформаційних технологій. Отже, вважаю, що дисертаційна робота "Методи та моделі вдосконалення транспарентної технології таємного інтернет-голосування" повністю **відповідає чинним вимогам МОН України щодо дисертаційних робіт, зокрема "Порядку присудження наукових ступенів", затвердженого Постановою КМУ від 24.03.13р. №567 (із змінами, внесеними згідно з Постановами КМУ №656 від 19.08.2015р., №1159 від 30.12.2015, №567 від 27.07.2016р.),**

відповідає паспорту обраної спеціальності, а її автор, Комарницький Олег Олександрович, гідний присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 – інформаційні технології.

Офіційний опонент

Професор кафедри автоматики та управління в технічних системах Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»,

доктор технічних наук, професор Б. Корнієнко

Підпис Корнієнка Б.Я. засвідчую