ВІДГУК

офіційного опонента
кандидата технічних наук Цуркана Василя Васильовича
на дисертацію Пригари Михайла Петровича
«Захищена система технічної підтримки процесів дистанційного волевиявлення»,
представлену на здобуття наукового ступеня кандидата технічних наук
за спеціальністю 05.13.21 – системи захисту інформації

Актуальність обраної теми. Ключову роль у забезпеченні економічного та соціального прогресу України відіграє розвиток демократичних процесів, застосування загальновизнаної системи демократичних цінностей. Це дозволяє громадянам та інститутам громадянського суспільства брати участь у процесах державотворення та державного управління. Така участь розширяється завдяки розвитку інформаційно-телекомунікаційних технологій і, як наслідок, застосування інструментів електронної демократії.

Формування електронної демократії в Україні розпочалося прийняттям законів «Про електронні документи та електронний документообіг», «Про електронний цифровий підпис». Так, 2017 року Кабінетом міністрів України схвалено Концепцію розвитку електронної демократії в Україні. Цим документом затверджується План заходів щодо долучення громадян до комунікації, співпраці з органами державної влади, контролю за ними, участі у виробленні політики, розвитку самоорганізації та самоврядування.

Одним із основних завдань другого етапу (2019-2020 роки) реалізації Концепції розвитку електронної демократії в Україні є впровадження електронного голосування, електронного виборчого процесу, електронних референдумів. Завдяки цьому, здійснюватиметься дистанційне волевиявлення громадян через мережу Інтернет, що призведе до необхідності забезпечення їх довіри до результатів голосування.

Таким чином, дисертаційна робота Пригари Михайла Петровича, виконання якої направлене на забезпечення довіри до всіх учасників виборчого процесу через мережу Інтернет шляхом створення захищеної системи технічної підтримки процесів дистанційного волевиявлення, є актуальною та має практичне значення.

Обґрунтованість і достовірність наукових положень, висновків і рекомендацій, сформульованих у дисертації, підтверджується коректною постановкою завдань, науковою обґрунтованістю теоретичних положень, використанням апробованого математичного апарату, узгодженістю теоретичних положень з результатами експериментальних досліджень, опублікованими науковими працями у фахових виданнях та відповідними впровадження у діяльності Національного авіаційного університету, Київського національного університету будівництва і архітектури, Національному університеті ім. Т.Г. Шевченка, Державному науково-дослідному інституті автоматизованих систем в будівництві; навчальному процесі Національного авіаційного університету.

Новизна наукових положень. На основі аналізу результатів дослідницької кваліфікаційної роботи, яка виконана Пригарою М.П., можна зробити висновок, що найбільш суттєвими новими науковими результатами є такі:

1. Вперше побудовано модель системи дистанційного волевиявлення, у якій за допомогою введення необмеженої кількості користувачів мережі з правами доступу виключно на ознайомлення з усіма файлами і процесами на сервері, але без прав на будь-яку модифікацію, можливе виявлення всіх порушень політики безпеки щодо цілісності результатів волевиявлення та конфіденційності голосів в умовах недовіри до всіх без винятку осіб, що беруть участь у розробці, створенні та обслуговуванні системи дистанційного волевиявлення.

2. Дістав подальший розвиток метод дистанційного спостереження за роботою системи дистанційного волевиявлення, використання якого за рахунок виконання визначеної послідовності контрольних дій та за умов повністю відкритого програмного забезпечення, унеможливлює виникнення непомічених порушень прийнятої політики безпеки, що усуває підстави для недовіри до системи дистанційного волевиявлення.

3. Удосконалено метод захищеного обміну даними через Інтернет, який завдяки використанню випадкових бітових послідовностей та сумісного застосування шифру Вернама і алгоритму Діффі-Хелмана із параметрами, що забезпечують стійкий захист даних, і завдяки збереженню відстані єдиності згідно з К. Шенноном, формально обґрунтовують неможливість порушення конфіденційності даних у каналі зв'язку.

4. Удосконалено метод отримання випадкових бітових послідовностей, який завдяки комбінованому використанню природної нестабільності кварцових резонаторів, що входять до складу типового клієнтського обладнання, та непередбачуваності моментів появи та тривалості переривань, що виникають під час обробки випадкових мережевих запитів, забезпечує можливість коректної реалізації шифру Вернама в сукупності з алгоритмом Діффі-Хелмана. Метод дозволяє на типовому клієнтському обладнанні без додаткових програмних або апаратних засобів реалізувати запропонований удосконалений метод захищеного обміну даними через Інтернет.

Теоретичне та практичне значення роботи. Представлені в роботі модель і методи захисту дистанційного волевиявлення громадян, є важливим теоретичним внеском у наукову спеціальність 05.13.21 – системи захисту інформації. Практичне значення отриманих результатів полягає у розробленні алгоритму функціонування та прикладних програм формування бази виборців, виборчої дільниці, введення паролів, голосування і отримання довідок. Завдяки цьому стане можливим стимулювання громадян до участі в опитуваннях, виборах, референдумах через мережу Інтернет, з одного боку. Тоді як з іншого, гарантування відсутності порушень та об'єктивності результатів такої участі. В кінцевому випадку це дозволить унеможливити підривання довіри громадян до електронного голосування завдяки використанню моделі та методів захисту інформації у процесі дистанційного волевиявлення.

Рекомендації щодо використання у дисертації результатів, одержаних автором. Теоретичні та практичні результати дисертаційної роботи доцільно використовувати в організаціях як приватного, так і державного секторів, а також в науково-дослідних та навчальних установах України, які займаються теоретичними та практичними питаннями, пов'язаними з вирішенням проблем дистанційного волевиявлення і захисту інформації, зокрема. Крім цього при виконанні другого етапу плану заходів реалізації Концепції розвитку електронної демократії в Україні (2019-2020 роки).

Повнота викладення наукових положень дисертації в опублікованих працях. Результати за темою дисертації автором викладено в опублікованих 9 наукових працях, які представлені у списку використаних джерел дисертаційної роботи. Зокрема, 4 – у наукових фахових виданнях України, що включені до міжнародних науково-метричних баз, та 4 тез доповідей на вітчизняних і міжнародних конференціях.

За своїм змістом та отриманими результатами дисертаційна робота відповідає формулі та пунктам напрямів досліджень паспорту спеціальності 05.13.21 – системи захисту інформації, а саме: пункту 1 в частині «теоретичних, методологічних, технічних <…> й організаційних основ створення комплексних систем захисту інформації, зокрема інформації, що зберігається, оброблюється і передається в комп'ютерних системах і мережа»; пункту 2 у в частині «організація <…> функціонування систем захисту інформації»; пункту 3 у в частині «шифри, <…> та способи вибору систем криптозахисту, адекватних прийнятій політиці безпеки інформації». Вона є завершеною кваліфікаційною працею з науковими положеннями, що надані автором для публічного захисту, характеризується внутрішньою єдністю та доводить особистий внесок автора в науку.

При цьому зміст автореферату повністю відображає основні положення дисертаційної роботи.

Зауваження до дисертації. Незважаючи на достатній рівень виконаних наукових досліджень до дисертаційної роботи є такі зауваження:

1. Узагальненість формулювання теми дисертаційної роботи, зокрема, її визначення доцільно було б уточнити з огляду на отримані наукові результати. Наприклад: «Модель і методи захисту …».
2. Неузгодженість використання окремих понять і положень. Наприклад: формулювання об'єкта дослідження на с. 13 і 20 дисертації; «*Наразі* у Америці йде підготовка до Інтернет-голосування на виборах президента *у 2016 році*», див. с 22; «слабке місце» (недоцільно – «слабке місце» операційної системи), тоді як загальновживаним є поняття «уразливість» (доцільно – уразливість операційної системи), див. с. 29.
3. Складність реалізування окремих положень на практиці. Наприклад: контролювання виборцями усіх файлів і процесів на сервері, зокрема, з боку рядових виборців; забезпечення абсолютного захисту інформації через існування ризиків порушення її властивостей, таких як конфіденційність, цілісність, доступність.

4. Недостатність описання елементів виразу (2.9) на с. 75, зокрема, імовірності події, що досліджується. Це призводить до ускладнення інтерпретування результатів оцінювання відсотка статистичної похибки за табл. 2.6 з огляду на зміну значень величини ймовірності: 2,5; 5; 10, … та, як наслідок, визначення індексу дисперсії за виразом (3.10) на с. 106.

5. Наявність окремих стилістичних, орфографічних помилок та неточностей оформлення. Наприклад: «конфіденційність … конфіденційних даних…», доцільно – «…конфіденційність … даних…», див. с. 11; «…учбово-тренувальних…», доцільно – « …навчально (або освітньо)- тренувальних…», див. с. 24; «… Диффі-Геллмана…», доцільно «…Діффі-Хелмана…», див. с. 46; «…процент статистичної похибки…», доцільно «…відсоток статистичної похибки…», див. с. 75; діапазону сторінок джерел [80], [83] дисертації, див. с. 159; джерел [6], [9] автореферату, див. с. 17-18.

Висновки. Зазначені у відгуку зауваження не зменшують теоретичної та практичної цінності дисертаційної роботи Пригари Михайла Петровича. Загалом, вона характеризується внутрішньою єдністю, виконана на достатньому науковому рівні та є завершеною працею. У ній отримано нові науково обґрунтовані результати, що в сукупності вирішують наукове завдання зі створення захищеної системи технічної підтримки процесів дистанційного волевиявлення для забезпечення довіри до всіх учасників виборчого процесу через мережу Інтернет.

Дисертаційна робота Пригари М.П. відповідає вимогам Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24.07.2013 № 567 (зі змінами). Тому її автор заслуговує на присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент
доцент кафедри кібербезпеки та застосування
автоматизованих інформаційних систем та технологій
ІСЗЗІ КПІ ім. Ігоря Сікорського
кандидат технічних наук В.В. Цуркан

Підпис кандидата технічних наук Цуркана Василя Васильовича засвідчую.

Начальник відділу кадрової роботи
ІСЗЗІ КПІ ім. Ігоря Сікорського В.М. Грищук