Голові спеціалізованої вченої ради
Д26.062.17
Національного авіаційного університету
03680, м. Київ, проспект
Космонавта Комарова,1

ВІДГУК

офіційного опонента

професора кафедри кібербезпеки та математичного моделювання
Чернігівського національного університету,
доктора технічних наук, професора Шелеста Михайла Євгеновича
на дисертацію Пригари Михайла Петровича
на тему
"Захищена система технічної підтримки процесів дистанційного волевиявлення",
що представлена на здобуття наукового ступеня кандидата технічних наук
за спеціальністю 05.13.21 "Системи захисту інформації"

Актуальність теми дисертаційного дослідження

Дисертаційна робота Пригари Михайла Петровича присвячена вирішенню актуальної задачі технічної підтримки систем дистанційного волевиявлення з використанням Інтернету. Такі системи, з одного боку, надають виборцям переваги щодо зручності, мобільності та економії часу на волевиявлення, але, з другого боку, бракує впевненості у тому, що результати дистанційного волевиявлення не будуть замінені, а таємницю голосів не буде порушено. Хоч в низці країн світу системи дистанційні волевиявлення вже впроваджено на державному рівні, але в жодній з цих систем не надаються в достатній мірі докази неможливості підробки результатів і гарантії щодо збереження таємниці голосів. Через те в країнах з тоталітарним минулим, де не має стійких демократичних традицій, процедура голосування через Інтернет повинна враховувати специфічні особливості менталітету виборців і конкретні умови здійснення виборчого процесу. Зокрема, слід враховувати тотальну недовіру основної маси виборців до будь-яких суб'єктів, які пов'язані з організацією виборів, або існуюча можливість підкупу, адміністративного або навіть силового тиску на виборців. Досконалість систем волевиявлення с точки зору прозорості і усунення причин для проявів недовіри, є фактором, який в значній мірі сприяє демократичним принципам розвитку суспільства та Е-демократії. Чим більше прозорості у системі волевиявлення, тим менше залишається причин для недовіри з боку виборців.

В даній дисертаційній роботі вперше зроблена спроба вирішити проблему недовіри в системах дистанційного волевиявлення методами, що лежать у сфері технічного захисту інформації, бо саме у цій сфері, як показано в даній роботі, лежать корені обґрунтованої недовіри громадян до «чесності» роботи систем

волевиявлення. Обраний здобувачем підхід до побудови системи волевиявлення здатен надати не тільки кожному виборцю, але й будь-якому користувачеві Інтернету, змогу добути достатні докази того, що в цій системі неможливе розкриття таємниці голосів та/або фальсифікування результатів волевиявлення.

Тому дослідження в цьому науковому напрямку є актуальними та на часі.

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

В Україні існує потреба вдосконалення системи волевиявлення, яка є важливою складовою частиною Е-демократії, про що свідчать документи ВРУ, наприклад http://euinfocenter.rada.gov.ua/uploads/documents/28784.pdf. Тому слід вважати, що обраний здобувачем напрямок дослідження відповідає сучасним потребам розвитку науки і техніки в Україні.

Оцінка змісту дисертації та її завершеності як єдиного цілого

Дисертаційна робота складається з вступу, чотирьох розділів, які містять основні наукові результати, списку літератури та додатків.

Вступ розкриває сутність і стан наукового завдання, що вирішується в роботі, та її значущість, обґрунтовує необхідність проведення дисертаційних досліджень. В ньому подана загальна характеристика роботи у відповідності з діючими вимогами ВАК України до дисертацій. Також визначений особистий внесок автора дисертації в одержані наукові результати.

В ***першому розділі*** виконано аналіз існуючих систем технічної підтримки процесів дистанційного волевиявлення з позицій захисту інформації. Обґрунтовано існуюче протиріччя між зацікавленістю в достовірності виборів спільноти виборців в цілому та існуючої недовіри в процесі волевиявлення до окремого громадянина або будь-яких їх об'єднань, що задіяні в організації та проведені виборів. Показано, що ця недовіра є наслідком недосконалості методів та засобів ТЗІ, що знайшли застосування в існуючих СДВ. Тому в даній роботі зроблена спроба вирішити це протиріччя (проблему недовіри) методами, що лежать у сфері ТЗІ.

У результаті проведеного аналізу визначено інформаційні потоки й об'єкти, що потребують захисту, виявлено загрози для інформації, відсутність протидії яким підриває довіру до того, що результати волевиявлення будуть об'єктивно відображати волю виборців, та запропоновано можливі методи їхньої нейтралізації.

У ***другому розділі*** побудовано модель СДВ, основу якої складає сукупність концептуальної моделі захисту інформації в СДВ та логічної моделі взаємодії користувачів із сервером СДВ. Основна умова реалізації моделі СДВ - відкритість програмного забезпечення сервера та відсутність обмежень щодо процедур контролю. Згідно з концептуальною моделлю функціональність СДВ має забезпечити: логічну ізоляцію процесів прикладної програми від шкідливих проникнень; імпорт даних, що є об'єктами захисту, до обчислювальних процесів прикладної програми; створення умов для використання шифрування для захисту даних, що імпортуються в домен об'єктів захисту; контроль за роботою сервера з боку необмеженого кола будь-яких користувачів Інтернету.

Розроблена логічна модель СДВ за умов відкритості ПЗ забезпечує: доско-

налий захист критичних даних при зберіганні на сервері і при обміні через середовище Інтернет; перебування критичних даних виключно в оперативній пам'яті діючої програми; конфіденційність та неможливість непомічених фальсифікацій за умови повної недовіри до всіх без винятку учасників процесу волевиявлення; можливість застосування методів протидії незаконному впливу на виборців.

Розроблено метод дистанційного спостереження в режимі реального часу за станом сервера з боку необмеженого кола користувачів Інтернету з метою протидії загрозам, що пов'язані із можливими зловмисними діями персоналу, який обслуговує СДВ. Розроблений метод базується на спостереженні за станом активних процесів (діючих програм) і всіх файлів на сервері з боку необмеженої кількості будь-яких осіб із будь-яких вузлів Інтернету, що унеможливлює створення непомічених загроз на сервері за умов використання відкритого ПЗ. Метод створює умови, за яких будь-яке зловживання щодо роботи сервера не може залишитись непоміченим.

В ***третьому розділі*** запропоновано метод захищеного обміну даними через Інтернет між клієнтами та сервером СДВ у класі симетричних систем шифрування. В основі методу - відома схема, яка полягає в тому, що спочатку здійснюється генерування випадкових бітових послідовностей як на боці клієнта, так і на сервері та виконується обмін ключами за алгоритмом Диффі-Хеллмана, а потім здійснюється обмін конфіденційною інформацією через відкритий канал шляхом з використанням шифру Вернама. Конкретизовано діапазони оптимальних значень параметрів цих криптографічних методів, визначено обмежувальні умови застосування та розроблено засоби забезпечення виконання цих умов, а саме визначено:

- тривалість обслуговування запитів клієнтів для різних значень якості обслуговування (що визначається у даному випадку ймовірною тривалістю очікування у черзі до сервера);
- довжини ключів шифру, що безпосередньо пов'язано з вибором методу шифрування та визначенням кількості конфіденційних даних, які мають бути передані через канал протягом одного сеансу зв'язку;
- параметри алгоритму Диффі-Хеллмана, зокрема варіанту мультиплікативної групи для реалізації цього алгоритму, за яких злом системи захисту є гарантовано неможливим;
- метод отримання випадкових бітових послідовностей, який базується на використанні нестабільності частоти кварцових резонаторів, що є невід'ємними частинами будь-якого комп'ютера масового виробництва.

Запропоновано також метод протидії загрозам, що пов'язані з моральним або іншим тиском на суб'єктів процесу ДВ. Головна ідея, яку покладено в розробку методу наступна. Система має надавати виборцю абсолютно ідентичні повідомлення в разі голосування як із правильним паролем, так і з деякою множиною неправильних паролів, наприклад, тих, що мають ту ж саму довжину, що й правильний пароль. При цьому зараховується тільки один результат із правильним паролем. Це забезпечує можливість усунення будь-якого впливу на власне рішення виборця з боку інших осіб шляхом забезпечення імітації процесу голосування з метою уведення в оману зловмисника.

Четвертий розділ присвячено натурному моделюванню усіх засобів СДВ, у складі якої функціонує розроблена система ТЗІ. Для моделювання обрано типову організаційно-технічну модель проведення загальнонаціональних виборів в Україні, принципи її функціонування сформульовано у вигляді технічних вимог. Розкрито програмні механізми реалізації всіх запропонованих методів захисту та надано відповідні фрагменти комп'ютерних програм на мові *JavaScript*.

У ***висновках*** викладено найважливіші наукові та практичні результати, що отримані в дисертації. В ***додатках*** містяться тексти програм для реалізації системи дистанційного волевиявлення та акт впровадження отриманих автором результатів. ***Список використаних джерел*** оформлений, в основному, коректно та складається з 84 найменувань наукової літератури по темі дисертації.

Зміст роботи відповідає науковому завданню та сформульованим задачам. Їх рішення є суттю та змістом виконання дослідження. Дисертація оформлена у відповідності з прийнятими стандартами, а стиль викладення в ній матеріалу забезпечує доступність та легкість його сприйняття.

Наукова цінність результатів роботи полягає у наступному:

1) вперше побудовано модель СДВ, 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 СДВ;

2) здійснено подальший розвиток методу дистанційного спостереження за роботою СДВ, 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 СДВ;

3) здійснено подальший розвиток методу захищеного обміну даними через Інтернет, в якому завдяки сумісного застосування шифру Вернама і алгоритму Діффі-Хеллмана із параметрами, що забезпечують стійкий захист даних, формально обґрунтовується неможливість порушення конфіденційності даних волевиявлення 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 шифрування. Метод дозволяє на типовому клієнтському обладнанні без додаткових програмних або апаратних засобів реалізувати запропонований удосконалений метод захищеного обміну даними через Інтернет.

Достовірність отриманих в дисертації результатів підтверджується експериментальними дослідженнями на натурних моделях.

Значення результатів для практики полягає в тому, що побудована мо-

дель СДВ в сукупності з розробленими методами надає можливість гарантувати відсутність порушень таємниці голосів та істинність результатів волевиявлення під час проведення виборів, конкурсів та опитувань в умовах повної недовіри до всіх без винятку учасників процесу волевиявлення.

Використання запропонованого методу дистанційного спостереження за роботою сервера СДВ з боку необмеженої кількості користувачів мережі Інтернет за рахунок усунення підстав для недовіри щодо істинності результатів волевиявлення та збереження таємниці голосів стимулює до участі в масових опитуваннях, виборах та референдумах.

Можливості приховування інформації про результати особистого волевиявлення від зловмисників усуває доцільність незаконного впливу на виборців методами підкупу, залякування або силового тиску.

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).

Оцінка обґрунтованості та достовірності наукових положень, висновків та рекомендацій

У роботі розглянуто широке коло питань, які пов'язані між собою єдиною метою. Ступінь обґрунтованості наукових результатів дисертації та їх достовірність підтверджується коректним аналізом із залученням методів побудови комплексних систем захисту, що знайшли своє відображення у чинних нормативних документах ТЗІ. Розробка методів, що гарантують контрольованість середовища функціонування СДВ, 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. Синтез джерела випадкових бітових послідовностей здійснено на основі результатів математичного моделювання пакетного трафіка. Статистичні параметри побудованої СДВ оцінювалися з використанням результатів теорії телетрафіка.

Висновки та рекомендації, сформульовані в дисертаційній роботі, враховують сутність та актуальність науково-технічної задачі роботи та її мету. Представляється, що вони є придатними для практичного використання.

Ідентичність змісту автореферату й основних положень дисертації

Проаналізувавши автореферат і дисертацію здобувача, можна зробити висновки, що в авторефераті з необхідною повнотою відображено загальну характеристику, основній зміст та висновки дисертаційної роботи. Для основних положень дисертації та змісту автореферату характерна ідентичність.

Стиль викладення автореферату в цілому забезпечує повноту та доступність сприйняття. Наукові завдання дослідження та шляхи їх вирішення викладені чітко і лаконічно. З тексту зрозуміла наукова і практична значущість роботи та особистий внесок здобувача.

Автореферат і дисертація Пригари М.П., відповідно до вимог МОН України, були розміщені в електронному депозитарії Національного авіаційного університе-

ту за місяць до захисту.

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

Тема дисертації та її зміст відповідають формулі й галузі досліджень відповідно до положень, що викладені у паспорті спеціальності 05.13.21 – системи захисту інформації.

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

Основні результати дисертації достатньо повно опубліковані в наукових фахових виданнях України, профіль яких відповідає спеціальності за якою дисертація подана на захист. За темою дисертаційної роботи опубліковано 10 наукових праць, в тому числі 5 із яких у фахових науково-технічних спеціалізованих виданнях. Крім того, зазначені положення дисертаційної роботи пройшли обов'язкову і достатню апробацію на міжнародних науково-практичних конференціях та семінарах в Україні та закордоном. В авторефераті і дисертації наведені дані щодо конкретного особистого вкладу здобувача.

Таким чином, 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 в якості базової операційної системи для СДВ слушно пропонується обрати операційну систему *OpenBSD* у мінімальній конфігурації, оскільки серед ОС з відкритим програмним кодом вона є найбільш простою і надійно захищеною. При впровадженні СДВ такі операційні системи повинні проходити державну сертифікацію. В Україні на базі *OpenBSD* вже давно розроблена національна операційна система *BBOS*, яка пройшла в ДССЗЗІ відповідну сертифікацію в сфері ТЗІ та КЗІ. Тому бажано було би при проведенні дисертаційних досліджень провести критичний аналіз можливості її використання в СДВ, у тому числі вбудованих сертифікованих засобів КЗІ.

2. В першому науковому результаті можливість виявлення всіх порушень політики безпеки щодо цілісності результатів волевиявлення та конфіденційності голосів базується на введені необмеженої кількості користувачів з правами доступу на ознайомлення з усіма файлами і процесами на сервері, але без прав на будь-яку їх модифікацію. Це потребує від таких користувачів-контролерів безперервної уваги, щоб жодне з порушень не мало шансів залишитись невиявленим. На практиці, в реальних умовах через неуважність таких осіб, можливі проміжки часу без їх нагляду. Незрозуміло, чому автор не дослідив питання можливої автоматизації контролю сервера СДВ, яка б не тільки дозволяла виявляти порушення, як це пропонується в роботі, але й фіксувала виявлені порушення і проводила оповіщення користувачів.

3. Недоліком другого наукового результату, який полягає у дистанційному спостереженні за роботою СДВ, що, як вважає здобувач, повинно усунути підстави для недовіри з боку виборчої спільноти, є значна складність реалізації запропонованого процесу спостереження. Таке спостереження можуть виконувати тільки кваліфіковані фахівці. В цьому напрямку можливо проведення додаткових досліджень з метою пошуку методів, які б дозволяли кожному корис-

тувачеві мережі Інтернет без особливих зусиль впевнитись у тому, що цій системі дійсно можна довіряти.

4. В роботі взагалі не розглянуто питання стійкості системи дистанційного волевиявлення до можливих хакерських атак. Саме такий вид загроз в теперішній час є найбільш ймовірним та може суттєво вплинути на довіру виборців до СДВ.

5. В розділі 2 роботи для розрахунку проценту статистичної похибки оцінки результатів виборів при голосуванні в межах одномандатного округу запропоновано використовувати вираз (2.9), в якому введено значення ймовірності p. Далі по тексту в таблиці 2.6 наведено результати розрахунку залежності відсотку статистичної похибки оцінки результатів виборів від відсотка виборців, що голосують дистанційно, для значень p=50, при якому вираз (2.9) не є дійсним.

6. В підрозділі 3.2.6. автор обґрунтовує метод отримання дійсно випадкових бітових послідовностей. Для їх генерації автор пропонується використовувати таке природне явище як нестабільність частоти кварцових резонаторів, що є невід'ємними частинами будь-якого комп'ютера. Далі йде теоретичне обґрунтування запропонованого методу, базуючись на дослідженнях Смагіна О.Г. та Ярославського М.І., де припускається, що потік запитів до серверу має ознаки фрактального процесу. Зрозуміло, що вирази (3.10)-(3.11), що наведені в роботі, не є оригінальними, але посилання на джерело відсутнє. До того ж деякі параметри цих виразів не пояснені, що теж слід розглядати як недолік. Посилаючись на вираз (3.11), стверджується, що значення параметру Херста можливо оцінити по кутовому коефіцієнту нахилу цієї прямої лінії, а якої цієї прямої лінії – не вказано.

7. В перелік публікацій здобувача за темою дисертації включена робота «Подбор оптимального набора строительных обьектов при планировании инвестиционной деятельности в строительстве», яка не в повній мірі відповідає питанням, що досліджуються в дисертаційній роботі.

Слід відзначити, що наведені зауваження та недоліки не є принциповими щодо вирішення науково-прикладного завдання, яке є суттю дослідження, суттєво не впливають на загальне позитивне враження від роботи, не зменшують її якості, а також наукової цінності та практичної значимості.

Висновки

Нові науково обґрунтовані результати, що отримані в роботі, та їх практична реалізація в сукупності розв'язує актуальне наукове завдання – забезпечення 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.

В цілому, дисертаційна робота Пригари М. П. є завершеною кваліфікаційною науковою працею, яку виконано здобувачем особисто у вигляді спеціально підготовленого рукопису, містить висунуті автором для захисту науково обґрунтовані результати, що вичерпно свідчать про особистий внесок здобувача в науці. Отже, вважаю, що дисертаційна робота "Захищена система технічної підтримки процесів дистанційного волевиявлення" 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, Пригара Михайло Петрович, гідний присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент

професор кафедри кібербезпеки та математичного моделювання Чернігівського національного університету

доктор технічних наук, професор М.Шелест

Підпис Шелеста М.С. засвідчую

вчений секретар Г.М. Олійченко