67-72-05/1
13.02.17

ВІДГУК

офіційного опонента на дисертаційну роботу

Ігнатовича Анатолія Олександровича

"Методи підвищення ефективності компонентів безпеки комп'ютерних систем з використанням маскуючих елементів текстових та біометричних даних", подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

Актуальність теми дисертації

Розвиток комп'ютерних систем та мереж в світі вийшов на такий рівень, що складно уявити хаос в різних сферах діяльності людства при відключенні комп'ютерів і мереж хоча б на короткотривалий період. На особливе місце виходить боротьба великих фірм, корпорацій у кібер-просторі. Необхідно звернути увагу на те, що ми стаємо свідками започаткування гібридних війн у кібер-просторі, –останні десятиліття розгортаються справжні протистояння кібер-дивізій ряду країн. Такі змагання у кібер-просторі приносять одним державам чималі втрати, іншим – шалений вплив на багато соціальних і економічних процесів в певних країнах. Для прикладу, одним із наглядних фактів втручання кібер-дивізій є кібератаки на інфраструктуру США під час проведення президентських виборів, що підтверджене офіційним звітом трьох американських спецслужб – Федерального бюро розслідувань, Центрального розвідувального управління та Агентства з національної безпеки.

Науково-технічний розвиток кібер-фізичних систем неможливо уявити без постійного розвитку питань безпеки при експлуатації таких систем. Захист інформації є одним із важливих векторів розвитку комп'ютерних технологій. Інформаційна безпека забезпечується при проектуванні комп'ютерних систем та мереж на системному рівні, відповідними апаратними та програмними засобами. Очевидно рівень безпеки залежить від всіх складових, інакше через одну із слабих ланок можливо буде реалізоване "вікно" для зловмисників, кібер-злочинців. З одного боку методи захисту інформації розроблялися століттями, з другого боку методи злому інформації також неперервно розробляються і будуть розроблятися. Тому думки про те, що основні рішення вже відкриті – цей постулат є хибним як для захисту, так і для злому елементів захисту. Незважаючи на те, що в галузі проектування систем інформаційної безпеки працює велика кількість спеціалістів високого рівня, на практиці використовуються обмежена кількість методів захисту. В залежності від потрібного рівня захисту інформації використовуються засоби відповідної ефективності. Процес розробки нових методів захисту інформації відбувається постійно. Новий напрямок підвищення ефективності компонентів безпеки комп'ютерних систем та мереж з використанням маскуючих елементів текстових та біометричних даних є мало дослідженим і, вірогідно, перспективним. Тому розвиток та вдосконалення методів та засобів підвищення ефективності компонентів безпеки комп'ютерних систем та мереж з

використанням маскуючих елементів текстових та біометричних даних є актуальним.

Дисертаційна робота відповідає науковому напряму кафедри електронних обчислювальних машин Національного університету "Львівська політехніка": "Питання теорії, проектування та реалізації комп'ютерних систем та мереж, а також комп'ютерних засобів, вузлів, приладів і пристроїв вимірювальних, інформаційних, керуючих, телекомунікаційних та кібер-фізичних систем" та науково-дослідної роботи "Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем", шифр ДБ/КІБЕР, реєстраційний номер 0115U000446.

Ступінь обґрунтованості наукових положень і рекомендацій, які сформульовані у дисертації, та їх достовірність

Аналіз змісту дисертаційної роботи та методів дослідження дозволяє стверджувати, що наукові результати та висновки достатньо обґрунтовані з наукової та технічної точок зору. Наукові положення та висновки базуються на аналізі літературних джерел в предметній області дисертаційного дослідження. Перевірка достовірності запропонованих методів підвищення ефективності компонентів безпеки комп'ютерних систем та мереж з використанням маскуючих елементів текстових та біометричних даних виконана на основі моделювання реалізованих засобів захисту, апробацій результатів та впроваджень.

Основні результати досліджень та наукова новизна отриманих результатів.

Основними науковими результатами, які одержані здобувачем є:

1. Запропоновано модифікований метод автентифікації користувачів в комп'ютерних мережах як подальший розвиток засобів управління доступом, який полягає у використанні маскуючих елементів біометричних даних за відбитками пальців, та у порівнянні із відомими розширює функціональні можливості методів та засобів автентифікації, що дозволяє поліпшити їх ефективність при використанні за схемою "відкритий ключ користувача – закритий ключ користувача".

2. Вперше запропоновано вдосконалений метод шифрування інформації в компонентах безпеки комп'ютерних систем, який полягає у статичному використанні маскуючих елементів у відкритому тексті повідомлення з наступним перетворенням інформації блоковими криптографічними засобами, та на відміну від відомих покращує частотний розподіл символів у шифрованому тексті, що дає можливість підвищити ефективність компонентів безпеки;

3. Вперше запропоновано вдосконалений метод шифрування інформації в компонентах безпеки комп'ютерних систем, який полягає у динамічному використанні маскуючих елементів у відкритому тексті повідомлення з

наступним перетворенням інформації блоковими криптографічними засобами, який на відміну від відомих покращує частотний розподіл символів у шифрованому тексті та наближує до рівноймовірного, що дає можливість поліпшити ефективність компонентів безпеки;

4. Вперше розроблено та апробовано критерій оцінювання ефективності компонентів безпеки комп'ютерних систем із використанням маскуючих елементів текстових та біометричних даних, яких враховує сукупність важливих показників ефективності та у порівнянні із відомими не вимагає значного збільшення обчислювальних ресурсів, що дозволяє отримати узагальнену оцінку ефективності компонентів безпеки.

Практичне значення результатів дисертаційної роботи.

Отримані в дисертаційній роботі результати мають як наукове, так і практичне значення. Практичну цінність отриманих наукових результатів підтверджують акти використання результатів дисертаційної роботи в наукових практичних роботах. Практична цінність роботи полягає в наступному.

1. На основі аналізу сучасного стану компонентів безпеки комп'ютерних систем та мереж визначені основні напрямки покращення їх ефективності з використанням маскуючих елементів текстових та біометричних даних.

2. Використання запропонованого методу автентифікації користувачів в комп'ютерних системах та мережах на основі біометричних даних за відбитками пальців з маскуючими елементами за схемою "відкритий ключ користувача – закритий ключ користувача" розширює функціональні можливості компонентів безпеки.

3. Шифрування інформації на основі статичного чи динамічного використання маскуючих елементів у відкритому тексті повідомлення з наступним перетворенням інформації з допомогою блокової криптографічної системи покращує частотний розподіл символів у шифрованому тексті та ефективність компонентів безпеки.

4. Запропонований критерій оцінювання ефективності компонентів безпеки комп'ютерних систем та мереж на основі блокових шифрів із використанням маскуючих елементів дозволяє отримати узагальнену кількісну оцінку їх ефективності.

5. Основні результати теоретичних досліджень дисертації впроваджено в навчальний процес студентів базового напряму "Комп'ютерна інженерія" Національного університету "Львівська політехніка" у лабораторні практикуми з курсів "Захист інформації в комп'ютерних системах", "Комп'ютерні системи"; при виконанні науково-дослідницького проекту "Удосконалення та розвиток грід-кластеру Фізико-механічного інституту ім. Г.В. Карпенка НАН України"; при виконанні науково-дослідницької роботи "Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем", шифр ДБ/КІБЕР; при розробці програмного

забезпечення компонентів безпеки в міжнародній аутсорсинговій компанії "KindGeek (ТзОВ "КайндГік")".

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

Аналіз отриманих наукових результатів Ігнатовича А.О. дає можливість зробити висновок про їх цілісність і підтверджує особистий внесок здобувача в науку стосовно підвищення ефективності компонентів безпеки комп'ютерних систем з використанням маскуючих елементів.

Основні положення та результати дисертаційного дослідження викладено в 17 наукових працях, зокрема: 9 статтях в періодичних наукових виданнях (в тому числі 7 статтях у фахових виданнях та 2 статтях в іноземних виданнях), 8 тезах доповідей на конференціях та семінарах. Отримано 1 патент на корисну модель на новий спосіб шифрування інформації.

Обсяг друкованих робіт та їх кількість відповідають вимогам МОН України щодо публікацій основного змісту дисертації на здобуття наукового ступеня кандидата технічних наук.

Відповідність теми дисертації профілю спеціальності.

Дисертаційна робота написана державною мовою. Дисертація узгоджується з її назвою, метою, предметом об'єктом та задачами досліджень. Результати дисертаційної роботи відповідають спеціальності 05.13.05 – комп'ютерні системи та компоненти , зокрема пункту формули спеціальності – "створення алгоритмічного, апаратно-програмного, контрольно-діагностичного та інформаційно-вимірювального забезпечення процесів утворення, збору, зберігання, захисту, обробки, передачі, вводу, виводу та перетворення інформації у комп'ютерних та інформаційно-вимірювальних системах і мережах".

Відповідність автореферату змісту дисертації.

Основні положення автореферату: предмет, об'єкт та методи дослідження; мета і завдання дослідження; наукова новизна одержаних результатів; практичне значення одержаних результатів; зміст розділів; основні результати і висновки роботи; список праць за темою дисертації; характеристика особистого внеску здобувача повністю відповідають аналогічним позиціям дисертаційної роботи.

Оцінка мови, змісту та оформлення дисертації й автореферату.

Дисертаційна робота складається зі вступу, чотирьох розділів, висновків наприкінці кожного з розділів, загальних висновків, списку використаних літературних джерел зі 91 найменування і чотирьох додатків. Загальний обсяг дисертації - 143 сторінки, з них 115 сторінок - основна частина.

У вступі обґрунтовано актуальність дисертаційної роботи, наведено визначення компонентів безпеки комп'ютерних систем, сформульовано мету і задачі досліджень, викладено наукову новизну та практичне значення результатів досліджень, наведено інформацію відносно зв'язку роботи з науковими програмами, планами і темами, особистого внеску здобувача, апробації отриманих результатів і публікацій.

У першому розділі дисертації проведено аналіз сучасного стану і особливостей побудови існуючих компонентів безпеки комп'ютерних систем та мереж. Показана ефективність побудови компонентів безпеки на основі біометричних даних. Наведена класифікація компонентів захисту комп'ютерних систем та мереж за класифікаційною ознакою, що визначає рівень очікуваного ефекту захищеності. Аналіз сучасного стану досліджень ефективності компонентів безпеки комп'ютерних систем та мереж показав, що актуальними та доцільними є дослідження методів підвищення ефективності компонентів безпеки комп'ютерних систем та мереж з використанням маскуючих елементів текстових та біометричних даних.

У другому розділі запропоновано метод автентифікації та алгоритм захисту інформації в комп'ютерних мережах на основі біометричних даних з використанням маскуючих елементів. Запропоновано вдосконалений метод автентифікації користувача за біометричними даними із вставленням маскуючих елементів з використанням моделі та алгоритму взаємодії між користувачем та засобами криптографічного захисту. Використовується деякий криптографічний примітив, який зв'язує закриті (приватні) ключі користувача мережі з фрагментами даних відбитків пальців. Необхідно створити певний масив даних, які в певний спосіб блокують закриті ключі. Такий процес формування необхідного масиву даних відбувається під час реєстрації нового користувача, або коли існуючий користувач змінює ключ. Основна особливість криптографічних систем з біометричним захистом є створення ланок біометричного блокування (розблокування) ключів подібно до ланок парольного захисту ключів. Аналіз алгоритму автентифікації користувачів в комп'ютерних системах та мережах на основі біометричних даних за відбитками пальців з маскуючими елементами дозволяє зробити такі висновки. В процесі реєстрації біометричною системою зберігається не сам біометричний сигнал w, а його відображення $h(w, K)$, де K – це криптографічний ключ, який захищається системою. Для ефективного використання біометричних даних у блоках захисту біометричних ключів пропонується розширити модель випадкового визначника до нової моделі біометричного визначника, яка, на відміну від моделі визначника випадкових величин, дозволить зв'язати криптографічні ключі з нечіткими нерівномірно розподіленими біометричними даними і, тим самим, змоделювати безпосередньо взаємодію користувача із системою захисту. Біометричний визначник враховує проблему стабільності біометричних даних, а саме дозволяє поставити у відповідність до біометричних даних один або більше випадково вибраних ключів.

Біометричний визначник при заданих умовах зводиться до "чіткого". Для врахування проблеми нечіткості введено поняття біометричного ідентифікатора. Біометричний ідентифікатор відображає вхідні біометричні дані у певну структуру, яка нечутлива до визначеного рівня змін у біометричних даних. Відповідно біометричний визначник це складена конструкція - побудована з біометричного ідентифікатора та чіткого визначника.

У третьому розділі отримали подальший розвиток методи шифрування інформації із використанням маскуючих елементів на основі блокових шифрів. Використання блокових шифрів є одним з перспективним напрямком підвищення ефективності компонентів безпеки комп'ютерних систем. Запропоновано і досліджено на графічних моделях статичний і динамічний метод вставлення маскуючих елементів в текстові блоки. Запропоновано обраховувати середнє інтегральне відхилення частотного розподілу символів у шифрованому тексті для визначення якості запропонованих методів шифрування.

У четвертому розділі наведені практичні результати досліджень методів та моделей покращення ефективності компонентів безпеки в комп'ютерних системах та мережах. Запропонований модифікований метод автентифікації користувачів в комп'ютерних мережах із використанням маскуючих елементів в біометричних даних за відбитками пальців досліджено на грід-кластері Фізико-механічного інституту. Використано модель та алгоритм взаємодії між користувачем та засобами криптографічного захисту. Запропонований метод автентифікації у порівнянні із відомими розширює функціональні можливості засобів автентифікації, що дозволяє поліпшити їх ефективність при використанні за схемою "відкритий ключ користувача – закритий ключ користувача".

Ефективність запропонованих методів шифрування текстових даних із використанням маскуючих елементів досліджена тестовими засобами. Якість шифрованого за запропонованими методами одного із прикладів відкритого тексту досліджена тестами NIST USA. Успішне проходження чотирьох основних тестів NIST вказує на високі показники ефективності методів шифрування текстових даних із вставленням маскуючих елементів.

Досліджені графічні моделі статичного та динамічного методу вставлення маскуючих елементів. Результати підтверджують основні переваги запропонованого способу шифрування текстової інформації у порівнянні з аналогами – згладжується частотна характеристика вживання символів у шифрованому тексті і суттєво збільшується інтервали повторень фрагментів шифрованого тексту.

Запропоновано критерій оцінювання показників ефективності компонентів безпеки на основі багатопараметричного порівняльного аналізу з нормуванням порівняльних величин з врахуванням пріоритетів замовника.

У додатках подано чотири акти впровадження, лістинг програми тестування шифрів з допомогою тестів NIST USA, коди шифрованого тексту при його перевірці з допомогою тестів NIST USA.

Зауваження до дисертаційної роботи.

1. В дисертації запропоновано декілька показників для визначення ефективності застосування маскуючих елементів. Не наведено достатнього обґрунтування, в яких випадках користуватися цими показниками.

2. Недостатньо деталізований алгоритм використання маскуючих елементів біометричних даних за відбитками пальців щодо їх кількості та рекомендацій їх розташування.

3. Не наведено кількісних показників зміни продуктивності роботи криптографа при використанні маскуючих елементів біометричних і текстових даних у порівнянні з аналогами.

4. Не описані рекомендації щодо максимально допустимих термінів використання однієї конфігурації маскуючих елементів без суттєвого зниження ефективності компонентів безпеки комп'ютерних систем та мереж як для біометричних, так і для текстових даних.

5. В дисертації не наведено кількісного взаємозв'язку між стійкістю шифрів і зміною інтегрального відхилення частотного розподілу символів у шифрованому тексті.

6. Доцільно було б навести загальні особливості та порівняння методів криптоаналізу запропонованих засобів шифрування та аналогів.

7. В дисертації недостатньо уваги приділено апаратній реалізації запропонованої процедури використання маскуючих елементів біометричних і текстових даних, що обмежує сферу практичного використання запропонованих рішень.

8. Наявні окремі невідповідності математичних виразів автореферату та дисертації.

9. Наявні деякі помилки комп'ютерного набору.

Висновок про відповідність дисертації встановленим вимогам.

1. Дисертаційна робота Ігнатовича Анатолія Олександровича "Методи підвищення ефективності компонентів безпеки комп'ютерних систем з використанням маскуючих елементів текстових та біометричних даних" є завершеним науковим дослідженням. В дисертації отримано нові науково обґрунтовані теоретичні та практичні результати, що в сукупності розв'язують наукову задачу підвищення ефективності компонентів безпеки комп'ютерних систем із використанням маскуючих елементів текстових та біометричних даних.

Дисертаційна робота відповідає паспорту спеціальності 05.13.05 – комп'ютерні системи та компоненти у частині формули спеціальності за напрямками: створення алгоритмічного, апаратно-програмного, контрольно-

діагностичного та інформаційно-вимірювального забезпечення процесів утворення, збору, зберігання, захисту, обробки, передачі, вводу, виводу та перетворення інформації у комп'ютерних та інформаційно-вимірювальних системах і мережах

2. Основні результати роботи достатньо повно опубліковані, пройшли належну апробацію на наукових конференціях та семінарах.

3. Автореферат відповідає змісту дисертації та повністю його відображає. Дисертаційну роботу виконано на доволі високому науковому рівні, вона відповідає вимогам, які висуваються до робіт на здобуття наукового ступеня кандидата наук, зокрема пп. 9, 11, 12 "Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника", а автор, Ігнатович Анатолій Олександрович, заслуговує присвоєння наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент:
Проректор з науково-дослідної роботи Львівського державного університету безпеки життєдіяльності, д.т.н., доцент **Т.Є. Рак**