67-72-05/2
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

Зі збільшенням числа обчислювальних пристроїв, підключених до мережі, та розвитком інформаційних технологій проблема мережевої безпеки стає все більш актуальною. Не тільки компанії витрачають все більше і більше грошей, щоб захистити свої цінні активи (фізичні та цифрові), приватні користувачі також потребують посилених заходів безпеки для збереження конфіденційності особистої інформації. Враховуючи значне зростання обчислювальних потужностей, використання традиційних методів захисту інформації на основі паролів, які базуються виключно на послідовності символів, є недостатньо ефективним, так як вони є вразливими до атак методом грубої сили (brute force attacks). В даний час основна увага приділяється розробці методів автентифікації з використанням біометричної інформації. За останні кілька років використання біометричної автентифікації в якості елементу захисту комп'ютерних систем значно збільшилося, що пояснюється їх високою надійністю при ідентифікації і досягнутим останнім часом значним зниженням їх вартості. Біометричні методи автентифікації, такі як пристрій для зчитування відбитків пальців і / або вбудовані камери, масово впроваджуються в мобільних пристроях (а саме ноутбуках та смартфонах). На ринку доступний ряд систем, які використовують переваги біометрії, але це, як правило, замкнуті системи, які важко інтегрувати з існуючою мережевою інфраструктурою та грід - системами.

Отже, тема дисертаційної роботи **Ігнатовича А.О.**, яка присвячена розробці та дослідженню методів підвищення ефективності компонентів безпеки комп'ютерних систем із використанням маскуючих елементів текстових та біометричних даних, є важливою та актуальною.

Зв'язок роботи із науковими програмами, темами

Дисертаційна робота виконувалася відповідно до плану науково-дослідних робіт 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 кіберфізичних систем" та науково-дослідної роботи "Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем", шифр ДБ/КІБЕР, (номер державної реєстрації 0115U000446).

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації, їх достовірність

Отримані результати є обґрунтованими та достовірними, це підтверджується поданим теоретичним та експериментальним матеріалом, його науковою інтерпретацією, практичним використанням запропонованих розробок та апробацією на наукових конференціях і семінарах.

У роботі коректно застосовано основні положення обчислювальної та дискретної математики, теорії алгоритмів, теорії ймовірності, теорії статистичного аналізу.

Достовірність висновків та рекомендацій підкріплена результатами моделювання, а також відповідними публікаціями.

Наукова новизна отриманих результатів

Наукова новизна дисертаційної роботи **Ігнатовича А.О.** полягає у вирішенні важливої і актуальної науково-прикладної задачі розробки та дослідження методів підвищення ефективності компонентів безпеки

комп'ютерних систем із використанням маскуючих елементів текстових та біометричних даних. Основними науковими результатами є:

1. Вперше запропоновано 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.

2. Вперше запропоновано 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 покращити ефективність компонентів безпеки.

3. Вперше розроблено критерій оцінювання ефективності компонентів безпеки комп'ютерних систем із використанням маскуючих елементів текстових та біометричних даних, яких враховує сукупність основних показників ефективності, що дозволяє отримати узагальнену оцінку ефективності компонентів безпеки.

4. Отримав подальший розвиток модифікований метод автентифікації користувачів в комп'ютерних мережах, 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 підвищити ефективність при використанні за схемою "відкритий ключ користувача – закритий ключ користувача".

Практичне значення отриманих результатів

1. Визначені основні напрямки покращення ефективності компонентів безпеки комп'ютерних систем та мереж з використанням маскуючих елементів текстових та біометричних даних.

2. Розроблений метод автентифікації користувачів у комп'ютерних системах та мережах на основі біометричних даних за відбитками пальців з маскуючими елементами за схемою "відкритий ключ користувача – закритий ключ користувача" дозволив розширити 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.

Основні результати теоретичних досліджень дисертації впроваджено в навчальний процес Національного університету "Львівська політехніка" для студентів спеціальності "Комп'ютерна інженерія" у лабораторні практикуми з курсів "Захист інформації в комп'ютерних системах", "Комп'ютерні системи"; при виконанні науково-дослідницького проекту "Удосконалення та розвиток ґрід-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"; при розробці програмного забезпечення компонентів безпеки в міжнародній аутсорсинговій компанії "KindGeek (ТзОВ "КайндГік")".

Повнота викладу результатів в опублікованих працях, апробація роботи

Основні результати дисертації відображено у 18 друкованих працях, з яких 9 статей у фахових наукових виданнях, 1 патент України на корисну модель. Результати апробовано на науково-технічних конференціях, що зафіксовано в 8 опублікованих тезах та доповідях конференцій. Опубліковані роботи в повній мірі охоплюють основні результати дисертаційних досліджень.

Аналіз внеску автора в публікації по питаннях, висвітлених в дисертації, показав, що внесок Ігнатовича А.О. *є вирішальним*.

Автореферат повною мірою відображає зміст і основні положення дисертаційної роботи.

Зміст дисертації відповідає паспорту спеціальності 05.13.05 – комп'ютерні системи і компоненти.

Недоліки та зауваження

До недоліків та зауважень дисертаційної роботи можна віднести:

1. Аналіз відомих рішень захисту користувачів в комп'ютерних мережах на основі біометричних даних наведений в підрозділі 2.1 доцільно було привести в розділі 1.

2. В підрозділі 2.2 недостатньо обґрунтовано вибір елементів поля $GF(251^2)$ при виконанні алгоритму декодування коду Ріда-Соломона. Доцільно було розглянути поле $GF(2^{16})$, яке б включало всю область сканування.

3. В підрозділі 2.5 некоректно використаний термін "багатопараметричне" застосування біометричних даних, оскільки мова йде фактично про двопараметричне застосування.

4. В підрозділі 3.3 "Адаптивні методи вставлення маскуючих елементів" недостатньо деталізовано адаптивність методу вставлення маскуючих елементів.

5. Недостатньо уваги приділено результатам використання результатів роботи у кіберфізичних системах, зокрема не описано, на яких рівнях базової платформи кіберфізичних систем використовуються запропоновані рішення.

6. В роботі відсутня структура захисту для грід-кластеру Фізико-механічного інституту ім. Г.В. Карпенка Національної академії наук України.

Незважаючи на вказані зауваження та недоліки, загалом оцінка дисертації позитивна.

ВИСНОВОК

Дисертаційна робота **Ігнатовича А.О.** на тему **"Методи підвищення ефективності компонентів безпеки комп'ютерних систем з використанням маскуючих елементів текстових та біометричних даних"** є завершеною, самостійно підготовленою кваліфікаційною науковою працею, в якій отримані нові науково обґрунтовані та практично цінні результати, що вирішують важливу науково-прикладну задачу підвищення ефективності компонентів безпеки комп'ютерних систем із використанням маскуючих елементів текстових та біометричних даних.

Вважаю, що актуальність обраної теми дисертації, ступінь обґрунтованості наукових положень, висновків і рекомендацій, новизна та повнота викладу в опублікованих працях відповідають вимогам п.п. 9, 11, 12 "Порядку присудження наукових ступенів", затвердженого постановою Кабінету Міністрів України № 567 від 24.07.2013 р. (зі змінами), а її автор – **Ігнатович Анатолій Олександрович**, заслуговує присудження йому наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент,
доцент кафедри інформаційно-обчислювальних
систем і управління Тернопільського національного
економічного університету
д.т.н., доцент **В.В. Яцків**