Вченому секретарю спеціалізованої вченої ради Д 26.062.17
Національний авіаційний університет
03680, м. Київ,
просп. Космонавта Комарова, 1

ВІДГУК

на автореферат дисертації Смірнова Олексія Анатолійовича на тему: «Методи та засоби цифрової стеганографії з використанням складних дискретних сигналів для захисту інформаційних ресурсів», яка подається на здобуття наукового ступеня доктора технічних наук за спеціальністю 21.05.01 – інформаційна безпека держави

На сьогодні, завдяки бурхливому розвитку телекомунікаційних та мультимедіа технологій, активно розвиваються методи та засоби цифрової стеганографії. Дані мультимедіа-файлів, як правило, не потребують збереження абсолютної точності: вони можуть за рахунок стиснення незначно спотворюватися як при зберіганні, так і при передачі за рахунок впливу шумів, наявних у каналі зв'язку. Можливість внесення незначних змін без втрати функціональності зміненого файлу можна використати для прихованої передачі повідомлень. Органи відчуттів людини не здатні надійно розрізняти такі зміни, а спеціальне програмне забезпечення для виявлення та аналізу можливих незначних змін, або не дає можливості їх виділення, або не може бути побудоване за сучасного рівня розвитку стеганографічного аналізу, або ж не може бути побудованим взагалі. Це призводить до виникнення нових загроз інформаційній безпеці держави.

Як слідує з автореферату, дисертаційна робота О.А.Смірнова присвячена вирішенню важливої науково-прикладної проблеми, яка полягає у розробці методів та засобів цифрової стеганографії з використанням складних дискретних сигналів і технології прямого розширення спектру для захисту інформаційних ресурсів.

У результаті проведених у дисертаційній роботі досліджень отримано такі наукові результати:

– Вперше сформований принцип передачі інформаційних даних стеганоканалами, що організовуються, який полягає в введенні додаткових обмежень на кореляційні властивості дискретних сигналів при побудові стеганографічних засобів захисту інформації, що дозволяє підвищити вірогідність даних, які приховуються у стеганографічній системі, для захисту інформаційних ресурсів держави.

– Вперше розроблені стеганографічні методи захисту інформації з адаптивним формуванням дискретних сигналів, які враховують кореляційні властивості використовуваних контейнерів. Застосування розроблених методів при побудові стеганографічних засобів захисту інформації дозволяє підвищити ймовірність правильного вилучення повідомлень на прийомній стороні стеганосистеми.

– Вперше запропонована інформаційна технологія обміну ключами й передачі даних у закритій стеганосистемі, що враховує особливості адаптивного формування дискретних сигналів і дозволяє, за рахунок збереження у таємниці від зловмисника секретного правила вилучення інформаційних повідомлень, приховати факт передачі даних та забезпечити, таким чином, побудову стеганографічної системи для захисту інформаційних ресурсів

– Вперше розроблені методи синтезу великих ансамблів дискретних сигналів з багаторівневими функціями авто- і взаємної кореляції, які відрізняються від відомих використанням розроблених процедур перетину орбіт групового коду, що дозволяє формувати псевдовипадкові дискретні послідовності, бокові викиди функцій кореляції яких приймають кінцеве заздалегідь задане значення.

– Одержала подальший розвиток математична модель стеганографічних систем захисту інформації, яка відрізняється від відомих застосуванням абстрактного визначення процедур стеганокодування й декодування у вигляді відображень відповідних множин контейнерів, інформаційних даних і стеганограм, що дозволило формалізувати стеганоперетворення для різних класів систем (робастних, крихких і напівкрихких).

– Удосконалено методи цифрової стеганографії, які відрізняються від відомих використанням сформованих великих ансамблів дискретних сигналів з особливими кореляційними властивостями, що дозволяє підвищити пропускну здатність стеганоканалів з необхідними показниками безпеки (стеганографічної стійкості) та вірогідності даних, які приховуються, без внесення критичних спотворень застосованих стеганоконтейнерів.

При аналізі автореферату, були виявлені наступні недоліки:

1. В авторефераті, в таблиці 3, використовується значення ≈0 (для показника втрати вірогідності). Дане математичне позначення є некоректним та призводить до деякої плутанини в розумінні одержаних результатів.

2. В авторефераті немає рекомендацій щодо підбору зображення контейнера.

Втім, слід зазанчити, що зауваження, які виявлені при аналізі автореферату, не мають суттєвого впливу на отримані наукові результати.

Вважаю, що дисертаційна робота має визначену актуальність, наукову новизну та практичну значимість, і являє собою закінчену науково-дослідну роботу, яка відповідає паспорту спеціальності 21.05.01 – інформаційна безпека держави, а також вимогам «Порядку присудження наукових ступенів і присвоєння вчених звань», а її автор, Смірнов Олексій Анатолійович, заслуговує присудження наукового ступеня доктора технічних наук.

Відгук розглянутий та затверджений на засіданні кафедри інформаційних систем в економіці, протокол № 02 від 07 жовтня 2013 року.

Завідувач кафедри Інформаційних систем в економіці
Одеського національного економічного університету

доктор технічних наук
за спеціальністю 05.13.21 – системи захисту інформації **О.О. Скопа**

Підпис: Скопа О.О.
Засвідчую:
Нач. відділу кадрів
"26" 09 2013 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ * ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ * 02071079