Міністерство освіти і науки, молоді та спорту України
Вінницький національний технічний університет
Харківський національний економічний університет
Об'єднаний інститут проблем інформатики НАН Білорусі
Азербайджанська державна нафтова академія
Бєлгородський державний університет, Росія
Гірничо-металургійна академія AGH, Польща
Новий університет Лісабона, Португалія
Університет ЛІОН 2 ім. Люм'єра, Франція
Інститут інженерів з електротехніки та електроніки (IEEE), Українська секція

Тези доповідей Тертьої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації»

м. Вінниця, Україна
20-22 квітня 2011 року

Тезисы докладов Третьей Международной научно-практической конференции «Методы и средства кодирования, защиты и сжатия информации»

г. Винница, Украина
20-22 апреля 2011 года

ВНТУ 2011

УДК 004+681.3+621.3
М54

Відповідальний редактор В. А. Лужецький

Матеріали статей опубліковані в авторській редакції

Методи та засоби кодування, захисту й ущільнення
М54 інформації. Тези доповідей Третьої Міжнародної науково-практичної конференції. м. Вінниця, 20-22 квітня 2011 року. – Вінниця: ВНТУ, 2011. – 231 с.
ISBN 978-966-641-406-2

Збірка містить матеріали доповідей третьої Міжнародної науково-практичної конференції з сучасних проблем кодування, захисту й ущільнення інформації за п'ятьма основними напрямками: методи та засоби кодування інформації; методи та засоби криптографічного захисту інформації; інформаційна безпека комп'ютерних систем; методи та засоби ущільнення інформації; методи та засоби перетворення форм інформації.

УДК 004+681.3+621.3

ISBN 978-966-641-406-2

УДК 621.391

МЕТОД СТЕГАНОГРАФІЧНОГО ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ

П. В. Козлюк, асистент
Вінницький національний технічний університет
kozluk@svitonline.com

Контроль телефонних розмов залишається одним з найбільш поширених видів промислового шпигунства і дій злочинних елементів. Причини очевидні – малі витрати і ризик реалізації загроз, необов'язковість заходу в контрольоване приміщення, різноманітність способів і місць знімання інформації і т.п. Сучасні системи захисту мовної інформації в основному базуються на використанні методів закриття повідомлень, які роблять мову нерозбірливою або невпізнанною для зловмисника. В свою чергу, методи закриття мовних повідомлень поділяються по способу передачі інформації по каналам зв'язку на методи аналогового скремблювання та методи шифрування. Основна частина апаратури закриття мовних повідомлень використовує методи аналогового скремблювання завдяки їх відносній простоті та можливості використання в стандартних телефонних каналах. При цьому, рівень захисту мовних повідомлень зростає із ростом складності використовуваного алгоритму скремблювання.

Найбільшу ступінь захисту мовних повідомлень забезпечують динамічні скремблери зі змінними в часі параметрами використовуваних перетворень в частотній області. Методи шифрування мовних сигналів в цифровій формі забезпечують більш високий рівень захисту, але вимагають широкосмугових каналів зв'язку і відповідних модемів. Крім того, необхідно відмітити, що як методи аналогового скремблювання,

так і методи шифрування вносять суттєві спотворення в відновлений мовний сигнал.

В цифрових системах для захисту інформації поруч із методами криптографії почали широко застосовуватись методи цифрової стеганографії, які дозволяють приховати сам факт передачі конфіденційної інформації. В якості носія конфіденційної інформації (контейнера) може бути використаний довільний файл, в тому числі й оцифрований мовний сигнал.

В доповіді пропонується стеганографічний метод захисту мовної інформації, при якому конфіденційна інформація вбудовується в звичайну телефонну розмову, тобто контейнером виступає відкритий мовний сигнал сторони, яка передає конфіденційну інформацію. Для забезпечення необхідної стійкості захисту вбудова конфіденційної інформації відбувається в області коефіцієнтів спектрального перетворення фрагментів контейнера. Кофіденційна мовна інформація може вводитися безпосередньо під час розмови з другого мікрофону передаючої сторони, або з пристрою попереднього запису.

Особливістю такого стеганографічного методу захисту телефонних розмов є потоковий характер контейнера і робота в реальному масштабі часу. Тому однією з головних вимог до застосовуваного дискретного перетворення є його обчислювальна складність та величина внесеної затримки. Крім того, суттєві обмеження накладаються на затримку мовного сигналу в результаті дискретних перетворень.

В пропонованому методі стеганографічного захисту мовної інформації використовується дискретне q-перетворення, орієнтоване на ефективну потокову обробку. Для забезпечення максимальної пропускної спроможності вбудова конфіденційної мовної інформації відбувається в молодші розряди спектральних коефіцієнтів для вибраного фрагменту контейнера. Ключовою інформацією є параметр q перетворення та розмірність оброблювальних фрагментів сигналу-контейнера.