Науково-технічний семінар
"Синтез, обробка та відображення інформаційних моделей"
(ІнфоСинтез)
(Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України,
Харківський університет Повітряних Сил ім. І. Кожедуба)

e-mail: infosintez@hups.edu.ua

Чергове засідання 26.09.2006

1. ***Грабчак В.И.**, старший викладач Військового інституту РВ і А Сумського державного університету.* **Розробка методу забезпечення скритності передачі даних в АСУВ на основі використання каскадних кодових конструкцій.**

Перспективним напрямом розвитку теорії захисту інформації є побудова секретних систем теоретичної стійкості, заснованих на зведенні задачі злому ключових даних до рішення теоретіко-складної задачі декодування випадкового коду.

Практичне використання секретних систем на основі кодів дозволяє реалізувати комплексний захист інформації і забезпечити крім інформаційної скритності ефективний контроль виникаючих помилок, тобто виконати вимогу достовірності передачі даних.

Основним недоліком існуючих схем, заснованих на використанні перешкодостійких кодів, є великі обсяги ключових даних і висока, в порівнянні з блоково-симетричними алгоритмами, складність алгоритмів формування і декодування кодограм. Перспективним напрямом їх подальшого розвитку є побудова каскадних кодових конструкцій і обґрунтування режимів їх функціонування.

У роботі показано, що каскадні кодові схеми захисту інформації із замаскованими алгеброгеометрічними кодами на зовнішньому рівні узагальненого каскадного коду, дозволяють побудувати потенційно стійку каскадну кодову схему захисту інформації із високими конструктивними показниками при низькій складності її реалізації.

В результаті проведених досліджень розроблені алгоритми формування і декодування кодограм з використанням каскадних кодових конструкцій, вироблені практичні рекомендації за процедурою реалізації режимів їх функціонування для забезпечення інформаційної скритності і достовірності передачі даних в АСУВ. Оцінені часова і ємнісна складнощі розроблених алгоритмів, вироблені практичні рекомендації по їх реалізації.

Показано, що практичне використання запропонованих рішень дозволяє забезпечити необхідні імовірнісно-тимчасові показники інформаційної скритності (безпечний час ТБ| > 200 років, ймовірність розкриття ключових даних РК < 10^{-25} – 10^{-35}) і достовірності передачі даних (ймовірність помилкового прийому символів повідомлення ($P_{ош} < 10^{-9}$) в каналах із незалежними помилками, що групуються.

2. ***Вовк А.И.**, адъюнкт Харьковского университета Воздушных Сил им. И. Кожедуба.* **Экспериментальное исследование возможности применения фрактальной обработки сигналов при обнаружении объектов на поверхности земли рлс сантиметрвого диапазона.**

Представляет интерес исследование флуктуаций радиолокационных сигналов методами фрактального анализа при обнаружении объектов на поверхности Земли. С этой целью проводились экспериментальные исследования радиолокационных сигналов при дистанционном зондировании земной поверхности маломощной импульсной РЛС сантиметрового диапазона длин волн. В результате измерений был сформирован массив данных, содержащий выборки принятых сигналов для различных азимутальных направлений и углов места. Полученные со всего интервала дальности выборки анализировались методами фрактального анализа с использованием «скачущего окна». Длина «окна» определялась как произведение длительности импульса станции на целое число, что соответствует анализу сигналов на определенной дальности. При длине равной десяти импульсам станции в «окне» анализировалось рассеяние радиоволн километровым отрезком поверхности Земли.

Расчет размерности в пределах «окна» осуществлялся путем покрытия выборок сигнала элементами (клетками) различных размеров и построения логарифмических зависимостей числа элементов покрытия от их размера, т.е. определялась клеточная размерность. Прохождение «окна» по всей длине выборки позволяет получить распределение клеточной размерности для перекрывающихся и не перекрывающихся «окон». Такими методами для некоторых азимутальных направлений получены следующие результаты: объектам антропогенного характера соответствовали размерности наиболее близкие к единице из всех в данном направлении.

Таким образом, проведенные исследования позволяют сделать вывод о том, что для некоторых объектов на поверхности Земли можно осуществить обнаружение сигналов рассеянных ими по величине фрактальной размерности. Для оценки показателей качества обнаружения сигналов при использовании фрактального анализа целесообразно провести дальнейшие экспериментальные исследования по обнаружению объектов с заданными отношениями сигнал/фон.

Наступне засідання семінару відбудеться 31.10.2006 у аудиторії 102 ГНК
(програма засідання буде доведена додатково)