АНАЛИЗ ВОЗМОЖНОСТЕЙ ЗАЩИТЫ ОТ СИГНАЛОВ РЕВЕРБЕРАЦИИ ПРИ ГИДРОАКУСТИЧЕСКОМ СИНТЕЗЕ АПЕРТУРЫ АНТЕННЫ

ЧАН ТАЙ ЧОНГ, С.Р. ГЕЙСТЕР

В гидролокационных системах (ГЛС) при обработке принятого сигнала, кроме полезного сигнала, отраженного от дна и объектов, находящихся на нем, через приемную антенну поступают помехи. Такими помехами являются:

– сигналы, переотраженные от поверхности воды и принятые по боковым лепесткам диаграммы направленности гидроакустической антенны (ДНА);

– сигналы, отраженные от поверхности дна, лежащей вне главного лепестка ДНА, и принятые по боковым лепесткам ДНА;

– сигналы, отраженные от тел на пути распространения (например, от мельчайших частиц пыли и рыб);

– сигналы, многократно переотраженные от неровностей дна и поверхности воды.

Явление, описывающее эти переотражения, называется реверберацией.

В обычном гидролокаторе (ГЛ) построение изображения дна выполняется на основе прямого формирования узкой физической ДНА и сложного длиноимпульного сигнала. В таком ГЛ защита от помех реверберации является сложной задачей.

ГЛ с синтезом апертуры антенны (САА) обладает существенными преимуществами для защиты от помех реверберации. Это связано с тем, что основу САА составляет специальный спектральный анализ, обеспечивающий выделение из принятого сигнала только тех отраженных сигналов, для которых законы изменения задержки и фазы в ходе длительного интервала синтеза апертуры антенны соответствуют законам изменения задержки и фазы сигнала, отраженного от точки анализа. При этом сигналы реверберации из-за отличий в спектрально-временной структуре по сравнению с полезными сигналами не будут эффективно влиять на изображение.

Литература

1. *Ольшевский В.В.* Статистические свойства морской реверберации. М., 1966.
2. *Антипов В.Н.* Радиолокационные системы с цифровым синтезированием. М., 1988.

ЗАЩИТА РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ В СЕТЯХ IP-ТЕЛЕФОНИИ

И.В. ЛАГУТКО, А.А. КАСТЕРИН, Г.В. ДАВЫДОВ

Основными типами угроз, представляющих наибольшую опасность в сетях IP-телефонии, являются: подмена данных о пользователе, подслушивание, манипулирование данными, атаки типа DoS.

В целях обеспечения защиты целостности и конфиденциальности информации в сетях IP-телефонии предлагается разработать устройство активной защиты речевой информации. Основная функция устройства — шифрование с использованием криптографических алгоритмов на основе протоколов IPsec. Для поддержки целостности и конфиденциальности данных в спецификации IPsec предусмотрено применение различных протоколов и параметров аутентификации и шифрования пакетов данных, а также различных схем распределения ключей.

Шифрование передаваемой информации может производиться по стандартам ГОСТ 28147-89 и СТБ 34.101.31-2011. Шифрование обеспечит защиту от подслушивания и манипулирования данными, поддерживая конфиденциальность и неизменность передаваемой информации ограниченного распространения.

Устройство должно обеспечивать аутентификацию сторон, а также выработку сеансовых ключей связи при построении защищенных туннелей согласно группе протоколов IPSec. Процесс аутентификации защищает данные пользователя от подмены, что позволяет