ПОВЫШЕНИЕ ЧУВСТВИТЕЛЬНОСТИ НЕЛИНЕЙНОГО РАДИОЛОКАТОРА

М.М. Иванов

Стремительное развитие микро- и наноэлектроники ставит задачу улучшения чувствительности нелинейного радиолокатора (НРЛ) к закладным устройствам с малыми габаритами.

В традиционной радиолокации применение сложных сигналов разрешает противоречие между энергетическим потенциалом и чувствительностью [1]. В нелинейной радиолокации применение сложных сигналов имеет несколько иной характер [2]: применение сложных сигналов приводит к ухудшению чувствительности и точности измерения дальности, а повышение зондирующей частоты — к ухудшению проникающей способности сигнала.

Решение данной задачи — применение сверхширокоплосных импульсов. При облучении нелинейного объекта одновременно высокочастотным гармоническим сигналом и сверхширокополосными импульсами наблюдается эффект взаимной модуляции [3]. С помощью приемника НРЛ, регистрирующего сигнал, который получен в результате взаимной модуляции, происходит обнаружение нелинейного объекта. Сверхмалая длительность импульсов позволяет достичь разрешения порядка единиц миллиметров. Программная модель подтверждает работоспособность метода.

Литература

1. Лезин Ю.С. Оптимальные фильтры и накопители импульсных сигналов. М., 1969.

2. Горбачев А.А. // Нелинейная радиолокация. Сб. статей № 2. М., 2006.

3. Якубов В.П., Шипилов С.Э., Сатаров Р.Н., Юрченко А.В. // Журнал технической физики. 2015. Т. 85, Вып. 2. С. 122–125.

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ СКРЫТЫХ КРИПТОКОНТЕЙНЕРОВ ПРИ СОКРЫТИИ ДАННЫХ

А.М. Кадан, И.А. Сазановец

Один из широко распространенных способов защиты цифровых данных – использование зашифрованных виртуальных жёстких дисков, так называемых криптоконтейнеров.

Традиционно, пользователь авторизуется для работы с файлом криптоконтейнера, и криптоконтейнер монтируется как локальный диск. Однако некоторые программы (VeraCrypt, Jetico BestCrypt Container Encryption) позволяют также создавать скрытые криптоконтейнеры в уже готовых контейнерах. Скрытый образ внутреннего контейнера лежит на незанятом пространстве внешнего контейнера.

В работе ставилась задача исследования особенностей использования скрытых криптоконтейнеров при сокрытии данных. Дело в том, что скрыть информацию с помощью таких криптоконтейнеров не сложно, но если допустить некоторые типичные ошибки, то, как минимум, обнаружить факт существования скрытой информации становится возможным, что является весьма значимой угрозой. С этой точки зрения, основное внимание должно быть уделено дополнительным мерам и методам противодействия детектированию наличия факта сокрытия информации.

В работе предложены методы распределения информации по блокам криптоконтейнера в зависимости от уровня ее конфиденциальности, предлагаются методы «отвлечения внимания» злоумышленника от возможного наличия скрытого внутреннего содержимого, которые бы минимизировали возможные потери в случае оказания неприемлемого воздействия на владельца информации.

Методы основаны на стеганографии и учете психологического портрета злоумышленника. Проведенный эксперимент подтвердил, что предложенные методы позволили повысить надёжность сокрытия информации в скрытом криптоконтейнере при попытке детектирования ее наличия специалистами достаточно высокого уровня.

СИНТЕЗАТОР РЕЧЕПОДОБНЫХ СИГНАЛОВ НА КИТАЙСКОМ ЯЗЫКЕ

А.А. Казека, Г.В. Давыдов, В.А. Попов, А.В. Потапович

Синтезатор речеподобных сигналов предназначен для защиты от утечки информации по акустическому каналу. Данное устройство формирует акустические речеподобные сигналы на китайском языке и применяется совместно с генератором акустического белого шума.