АИС КАК ОБЪЕКТ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ ВОЗДЕЙСТВИЙ

AIS AS AN OBJECT OF INFORMATIONAL AND TECHNICAL INFLUENCES

K. Klimov

Summary. Information and technical effects (ITV) on radio electronic means (RES) by means of simulating interference are the most effective. The formation of false signals (LS) used in the automatic identification system (AIS) of ships containing distorted information can lead to navigation accidents.

The aim of the article is to study the AIS signals as an object of intentional interference, the approaches to solving the problem of determining the structure of the AIS signals by means of technical analysis of radio signals.

Keywords: Information and technical effects, AIS, false AIS signals, technical analysis of radio signals.

Климов Кирилл Сергеевич
Специалист по информационной безопасности телекоммуникационных Систем, специалист по тестированию, АО «Лаборатория Касперского»
kirik-klim@mail.ru

Аннотация. Информационно-технические воздействия (ИТВ) на радиоэлектронные средства (РЭС) с помощью имитирующих помех являются наиболее эффективными. Формирование ложных сигналов (ЛС), используемых в автоматической идентификационной системе (АИС) судов, содержащих искаженную информацию, может привести к навигационным происшествиям.

Целью статьи является исследование сигналов АИС как объекта воздействия преднамеренных помех, рассмотрены подходы к решению задачи определения структуры сигналов АИС методами технического анализа радиосигналов.

Ключевые слова: Информационно-технические воздействия, АИС, ложные сигналы АИС, технический анализ радиосигналов.

Введение

Информационно-технические воздействия (ИТВ) на радиоэлектронные средства (РЭС), являются одним наиболее эффективных методов радиоэлектронного противоборства, предусматривают создание преднамеренных помех, маскирующих и подавляющих полезные сигналы или же несущих дезинформацию.

Автоматическая идентификационная система [1] (АИС) судов предназначена для обеспечения безопасности судоходства и предупреждения столкновений. Суда, оборудованные станциями (транспондерами) АИС, передают сообщения, которые содержат в себе наименование судна, данные о курсе, скорости движения и текущем навигационном статусе. В АИС применяется открытый протокол передачи данных с излучением сигналов на известных международных частотах [3], вследствие чего возможно использование имитирующих помех или ложных сигналов (ЛС) АИС (Рисунок 1–6). Для формирования подобных ЛС необходимо знать сигнально-кодовую конструкцию (СКК) сигналов АИС для последующей их имитации.

Выявление СКК возможно с помощью методов технического анализа радиосигналов, которые приведены в статье.

Виды помех

Помехи делятся на два больших класса: маскирующие и имитирующие [2]. Маскирующие помехи — это прямые радиоизлучения, нарушающие работу РЭС путем маскирования полезных сигналов. Слово «маскирование» при этом понимается в широком смысле, т.е. включает как подавление полезного сигнала помехой, например, за счет нелинейных каскадов приемника, или отдельных узлов приемника путем нарушения их нормального функционирования. Примером маскирующих помех могут служить шумовые помехи, прицельные по частоте и спектру помехи, в частности, хаотические импульсные помехи или просто импульсные помехи с полосой частот, равной полосе частот принимаемого сигнала и др.

Имитирующие (дезинформирующие) помехи — это помехи, трудно отличимые от полезных сигналов, но несущие дезинформацию. Имитирующие помехи не создают сплошного маскирующего и подавляющего фона полезным сигнала, и поэтому реализуются при меньших средних мощностях излучения, чем маскирующие помехи. Характер дезинформации зависит от назначения и специфики подавляемой радиоэлектронной аппаратуры. Применительно к НАП GPS это могут быть автономные уводящие по дальности и скорости помехи, ретрансляционные помехи с последующим уводом по дальности и скорости, ложные спутники.

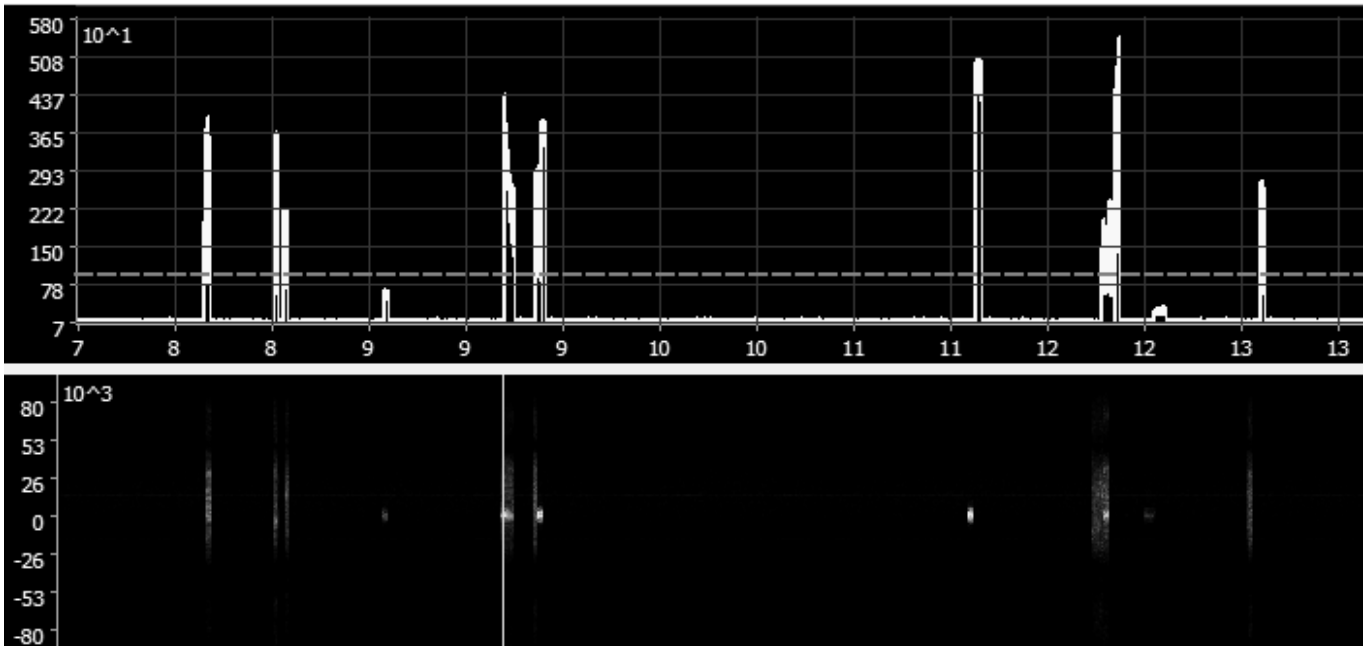
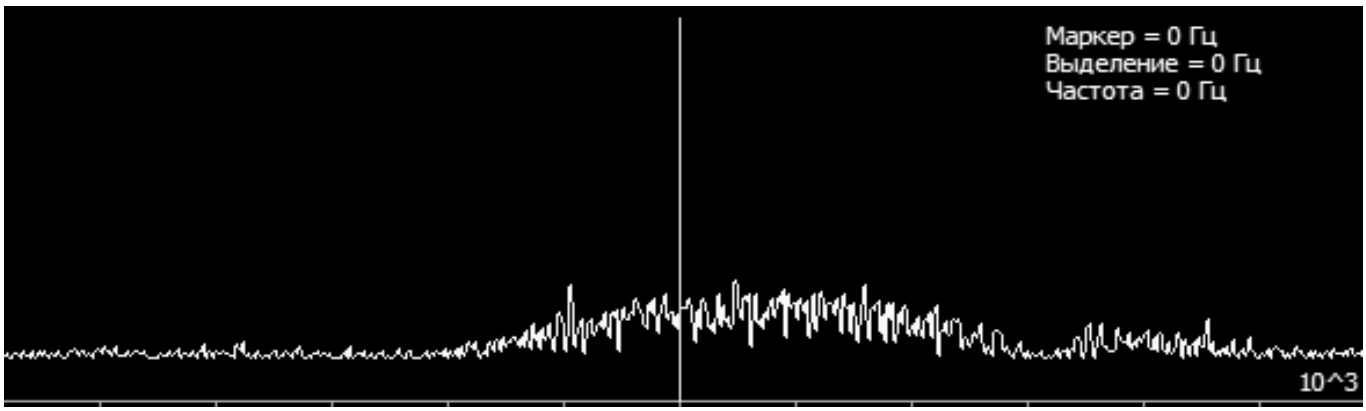


Рис. 1. Сигналы АИС в координатах амплитуда/время и частота/ время



Рисинок 2. Спектр сигналов АИС

В данной работе рассматриваются информационно-технические воздействия, создаваемые на основе имитирующих помех или ложных сигналов.

Активные имитирующие помехи обычно предназнача ются для внесения ложной информации в подавляемое ра диоэлектронное устройство. Под действием имити рующей помехи происходит перегрузка информационных каналов, что может при вести к работе радиоэлектронного устройства не только на пределе пропускной способности, но и к ее ограничению, не обеспечивая передачу полезной информации в полном объеме.

Чтобы исключить возможность фильтрации, ложный сигнал не должен значительно отличаться от реального сигнала по техническим параметрам. Например, в радиолокации при имитации ложной цели, находя щейся на одном пеленге с действительной целью, но на иной дальности, помеховый сигнал должен иметь, по крайней мере, одинаковую с полезным сигналом поляризацию и не сущую частоту. Однако по информационному параметру он отличается от полезного, т.е. помеховые сигналы излучаются по отношению к полезным с некоторой задерж кой.

Информационные и сопутствующие параметры помехового и полезного сигналов имеют между собой ста-

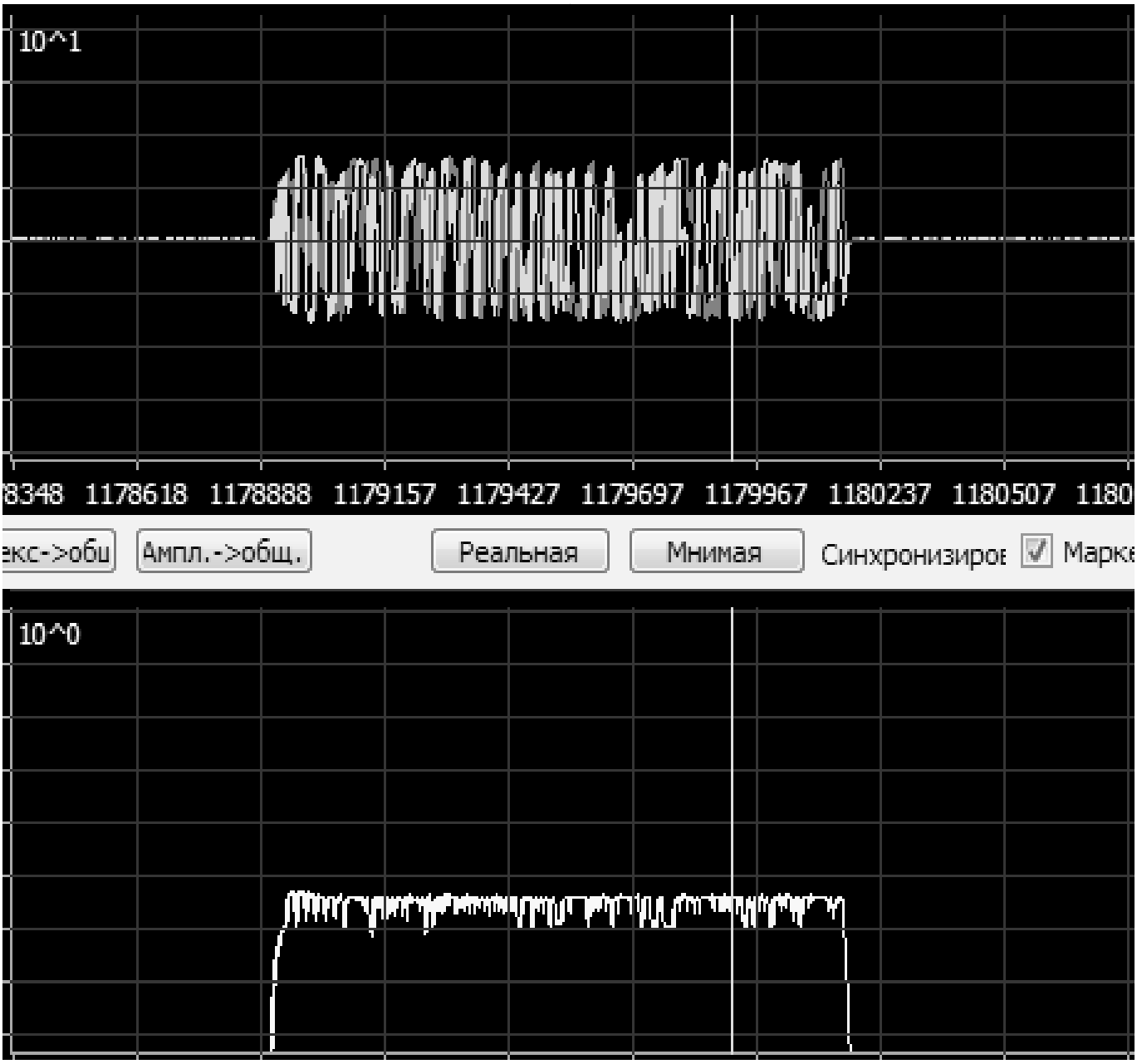


Рис. 3. Пакет (квадратуры, огибающая)

тистиче скую связь, которая в ряде случаев может переходить в функциональную зависимость.

В соответствии с назначением подавляемого РЭС различают имитирующие помехи для противодействия РЛС, линиям радиосвязи, командным радиолиниям управления, системам радионавигации и др.

Будем рассматривать постановку ЛС применительно к системам связи (СС), обеспечивающим автоматизированный обмен информацией между мобильными абонентами.

Примером таких систем могут служить сотовые системы (GSM, 3G. 4G), однако по ним разработано достаточно много средств противодействия.

В отличие от вышеприведенных методов формирования ЛС, предлагается формирование ЛС не только в виде имитирующей помехи, схожей с исходным по техническим параметрам (частота, вид модуляции и кодирования, информационная скорость …) статической информации, но и внесением после семантического анализа сообщения дополнительной информации, искажающей сообщение.

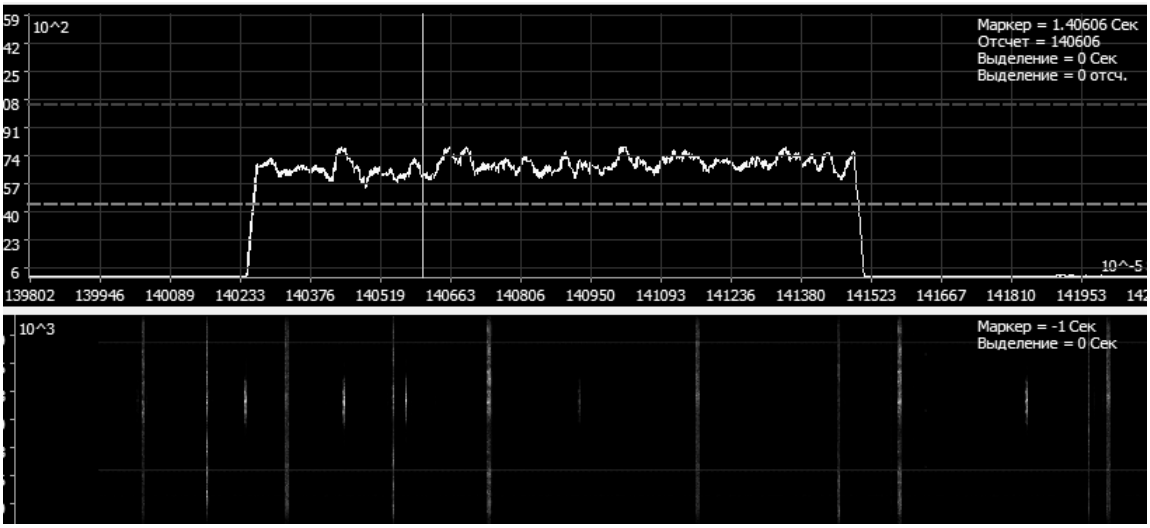


Рис. 4. Выделенный пакет

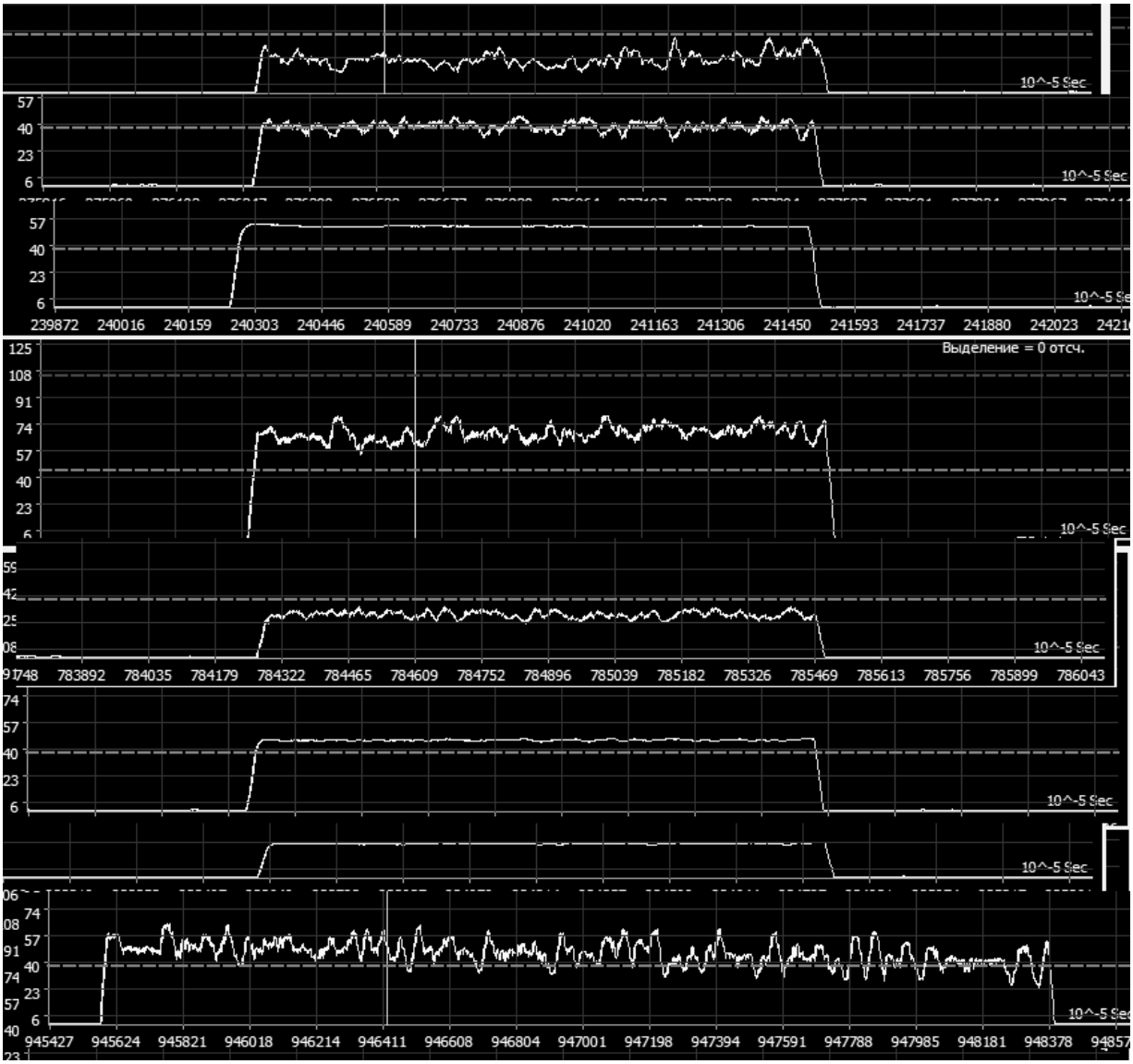


Рис. 5. Вид выделенного пакета в комплексе технического анализа радиосигнала

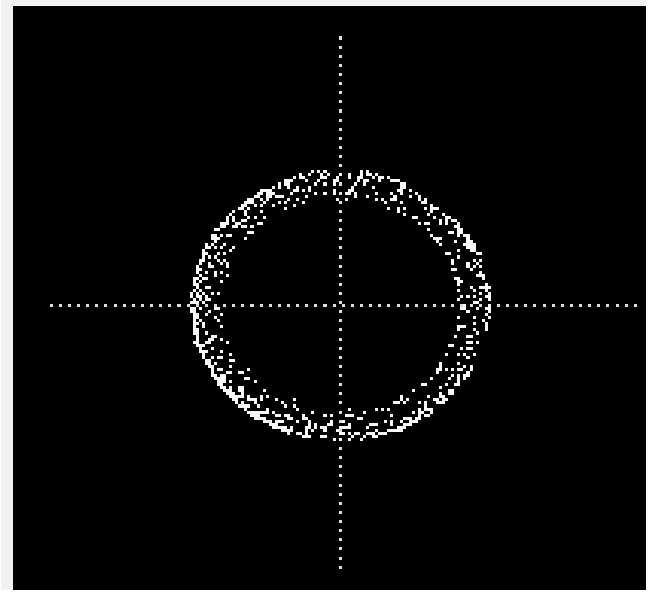


Рис. 6. Фазовое созвездие

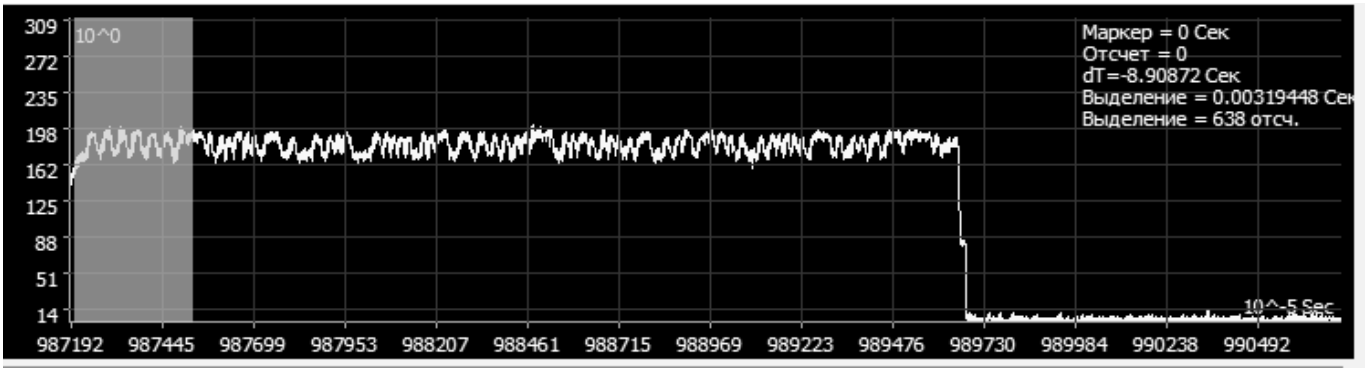


Рис. 7. Посылка (пакет) сигналов АИС, на которой выделен участок синхронизации.

Методы технического анализа сигналов АИС

Классический метод технического анализа цифровой записи сигналов АИС показывает совпадение с априорными данными по их структуре[3]:

- излучения с модуляцией MSK (GMSK) производятся на двух частотах: 161,975 МГц и 162,625 МГц пакетами со скоростью 9600 бит/с Сообщения передаются 8-битовым кодом,
- в каждом частотном канале применяется временное разделение передаваемых сообщений в кадре сигнала[4]. Длительность кадра 60 с, кадр делится на 2250 слотов (временных окон). Длительность слота — 26,67 мс, пакет передаваемой информации в слоте содержит 256 бит. В конце каждого слота имеется буферная зона из 12 бит, обеспечивающая автоматический прием сообщений, задержанных во времени.

После демодуляции и декодирования сообщение АИС имеет вид:

Lat; Lon; MMSI; Speed; Course; Name; Time; Accuracy; Code

34.2669333333333;-120.091348333333;636091237; 19.5;286; ;2016-05-07 07:39:33;1;19NWsl@033oJ@ w<CVq8;;8u404rL

33.7402466666667;-118.278068333333; 366760650;0;238.9; LEADER;2016-05-07 07:39:33; 1;15MiBjP000oRT><CCVe9E@C604rL

30.1217716666667; -122.2397;636013351; 7.4;131;2016-05-07 07:39:33;0;19NS; 9h01:G@KUVA?5qm7Sv60<01

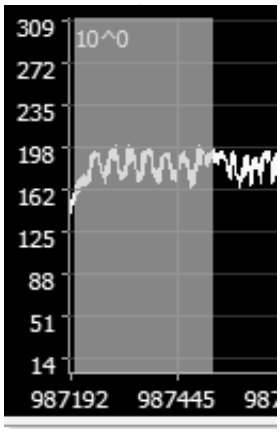


Рис. 8. Участок синхронизации

В приведенном сообщении возможна замена элементов ложными, например, идентификатора 636091237 на другой и передача ЛС, из которого участниками судоходства будет получаться и отображаться искаженная информация с ложными целями.

Большинство корпоративных и специальных СС технически или криптографически закрыты, поэтому как доступ к сообщениям, так и возможность имитации ложных сообщений отсутствует. Но вместе с тем с помощью методов технического анализа радиоизлучений можно выявить открытые служебные участки сообщений, используемые для точной настройки приемников на сигналы, синхронизация модемов, шифраторов и т.д. ЛС с имитацией пакетов сообщений с подобными служебными участками будет восприниматься в СС как полезный сигнал, однако может быть достигнута избыточность сигнального потока, что не позволит принимать полезную информацию, а также технический сбой модемов и шифраторов.

На примере с сигналом АИС определяющим структуру является выделенный участок синхронизации (Рисунок 7–8), который может быть сформирован как ЛС, а в дальнейшем восприниматься в СС всеми приемниками. Интенсивная передача указанного ЛС может привести к перегрузке приемников и блокировке приема полезной информации.

Таким образом, основой для формирования ЛС в закрытых СС является выявление служебных участков пакетов, которые могут быть сымитированы и восприняты абонентами СС.

Таким образом, задача информационного обеспечения постановки ЛС разбивается на этапы:

- Дальний загоризонтный прием пакетных сигналов УКВ-диапазона БЛА и ретрансляция на наземный комплекс мониторинга.
- Анализ принятых сигналов, определение структуры сообщений и участков, которые могут быть использованы для формирования ЛС.
- Подготовка исходных данных для формирования ЛС в цифровом виде, которые могут быть введены в комплекс постановки помех.

Методика

формирования ЛС на основе дальнего обнаружения сигналов АИС и анализа их структуры может быть распространена на другие пакетные сигналы УКВ-диапазона. Данная задача также актуальна в городских условиях при наличии большого числа экранирующих зданий.

Наибольшее применение в УКВ-диапазоне имеют пакетные ФМ (фазомодулированные) передачи, характерной особенностью которых является наличие в структуре многочастотных синхронизирующих составляющих, необходимых для правильной настройки приемной аппаратуры и модемов. Имитация подобных пакетов сводится к их запоминанию аппаратурой мониторинга, с дальнейшим переизлучением. Приемная аппаратура абонентов будет вынуждена синхронизироваться по ложному сигналу, принимать ложную информацию, вносящую сбои в сообщения.

Примеры 2, 3 сигналов УКВ приведены ниже (Рисунок 9–13).

Заключение

В данной статье показана методика формирования ЛС АИС с использованием маскирующих и имитирующих помех. Анализ сигнала осуществлялся с использованием комплекса технического анализа.

Пример 2

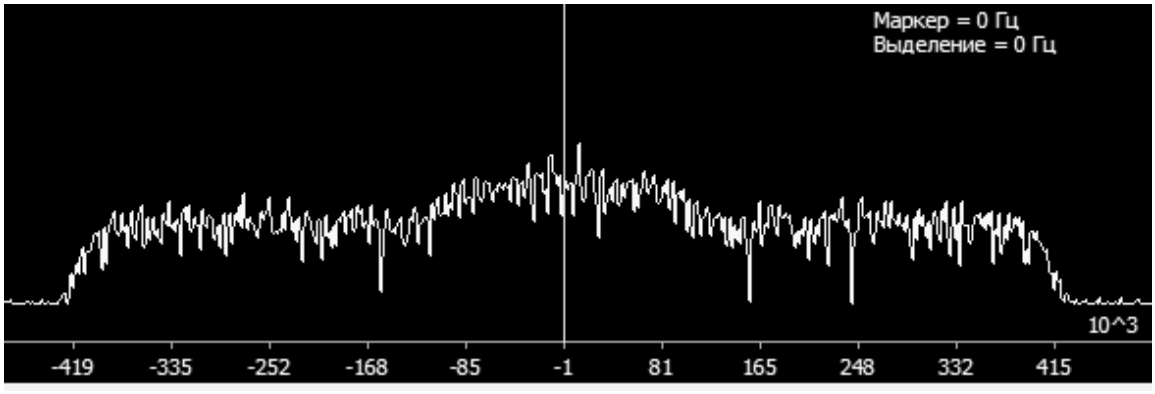


Рисунок 9. Спектр пакетного УКВ-сигнала

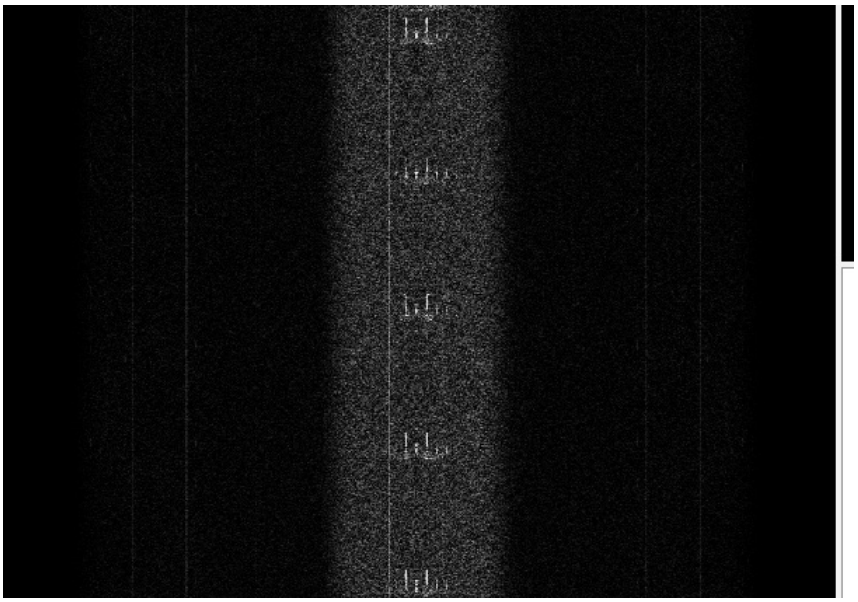


Рисунок 10. Сонограмма пакетного УКВ-сигнала

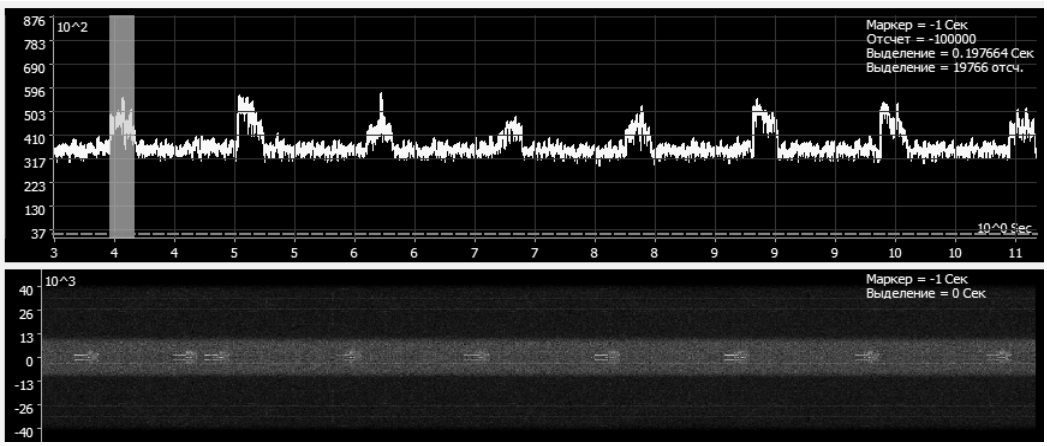


Рисунок 11. Осциллограмма/Сонограмма пакетного УКВ-сигнала

Пример 3

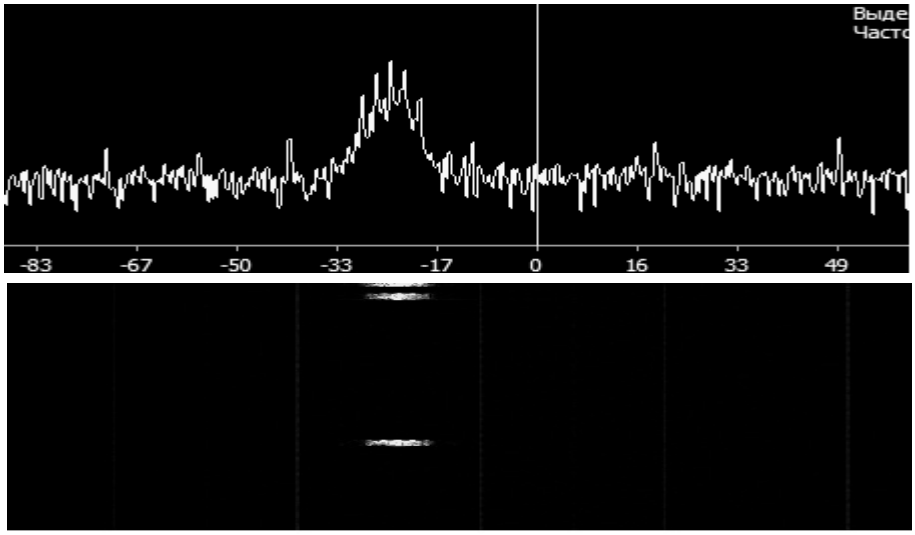


Рис. 12.Спектр и сонограмма пакетного УКВ-сигнала

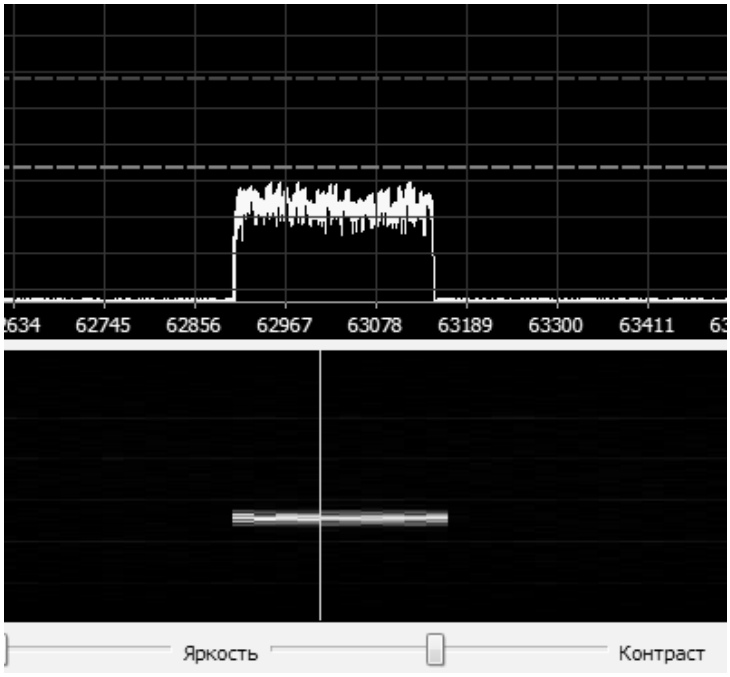


Рис. 13.Осциллограмма/ Сонограмма пакетного УКВ-сигнала

ЛИТЕРАУРА

1. IEC62320–1:2009 Оборудование и системы морской навигации и радиосвязи. Автоматические системы идентификации (AIS).
2. М. В. Максимов, М. П. Бобнев, Б. Х. Кривицкий и др. Защита от радиопомех. Под ред. Максимова М. В. М., «Сов. радио», 1976,— 496 с.
3. Резолюция ИМО MSC.43(64) «Руководство и критерии к системам судовых сообщений».
4. Резолюция ИМО MSC.74(69) «Эксплуатационные требования к комбинированному судовому приёмному оборудованию системы ГЛОНАСС/GPS»

Журнал «Современная наука: актуальные проблемы теории и практики»