# Исследование спуфинг воздействий на навигационные приемники с использованием SDR-трансивера

А. В. Фомин, С. П. Леонтьев, Д. М. Самойлов
Военно-космическая академия имени А.Ф. Можайского
vka@mil.ru

***Аннотация*. В работе представлены исследования спуфинг воздействий имитирующими помехами на навигационную аппаратуру ГНСС GPS, представлены результаты экспериментов по исследованию воздействий помех с различными параметрами при использовании современных программно-определяющих радиосистем, способных формировать широкополосные сигналы.**

***Ключевые слова: спуфинг GPS; программно-определяемая радиосистема; навигация; навигационная аппаратура***

## I. Введение

В современном мире особо важную роль играет навигация и навигационные системы, поскольку данные комплексы обеспечивают потребителей не только навигационной информацией, но и опорным временем, используемым для синхронизации работы сложных систем. Открытость структуры навигационных сообщений, структуры и сигналообразования создает возможность формирования ложных имитирующих навигационных сигналов и реализацию спуфинга или спуфинг-атак.

Спуфинг – (от англ. spoofing – подмена) это умышленная подмена истинной информации ложной для достижения определенных целей. Возможность реализации GPS спуфинга или спуфинг-атаки (далее спуфинг), то есть подмены навигационного сигнала показывает необходимость изучения данного вопроса, изучения особенностей реализации спуфинга и формулировки выводов.

Спуфинг, как правило, реализуется с помощью программно-определяемых радиосистем – радиосистем, в которых все функции физического уровня (фильтрация, модуляция/демодуляция, преобразование спектра, усиление) реализуются программными средствами без непосредственного вмешательства в схему устройства.

Для проведения экспериментов по исследованию спуфинг воздействий на навигационную аппаратуру был разработан программно-аппаратный комплекс (ПАК), позволяющий осуществлять формирование группового навигационного сигнала с заданными параметрами (координатами, временем, мощностью и др.) и излучать его в эфир.

## II. Структура и принцип работы ПАК

Внешний вид разработанного ПАК представлен на рис. 1.


Рис. 1. ПАК для исследования спуфинг воздействий на навигационные приемники с использованием SDR-трансивера

Программно-аппаратный комплекс включает в себя:

- передающую часть, состоящую из ПЭВМ со специализированным программным обеспечением (ПО) и подключенным SDR-трансивером «Hack RF One»;
- навигационные приемники «Garmin Nuvi 710» и «Mystery MNS-440MP»;
- анализатор спектра, который используется для контроля радиоэлектронной обстановки.

### *A. Описание передающей части ПАК*

Передающая часть ПАК предназначена для формирования группового навигационного сигнала в соответствии со структурой, описанной в интерфейсном контрольном документе системы GPS.

В навигационном сообщении содержится информация об эфемеридах навигационных космических аппаратов (НКА), альманах созвездия спутников, частотно-временные поправки, метки времени, параметры

ионосферной модели, сведения о работоспособности бортовой аппаратуры НКА и др. Эта информация используется в аппаратуре потребителя при решении навигационной задачи по определению координат, скорости и временной поправки к местной шкале времени. Информационная последовательность передается кадрами емкостью 1500 бит и длительностью 30 с. Структура кадра представлена на рис. 2.

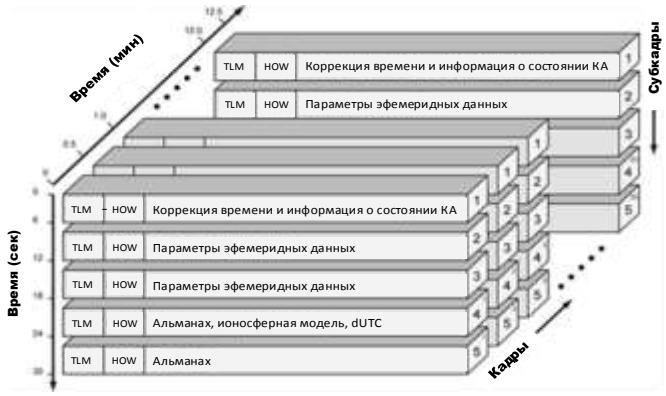


Рис. 2. Структура кадра навигационного сообщения

Эфемеридная информация, используемая при формировании навигационного сообщения, представляется в формате RINEX, который имеет следующую структуру рис. 3.

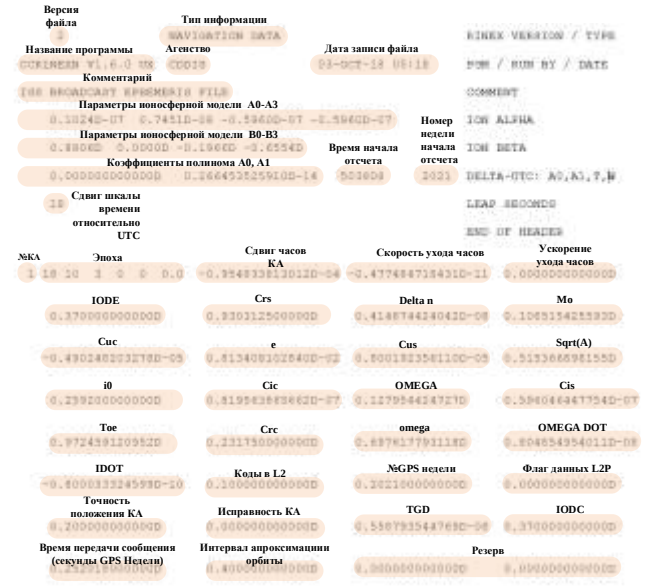


Рис. 3. Структура RINEX-файла с эфемеридной информацией

Для реализации спуфинга, кроме структуры навигационного сообщения необходимо знать структуру (вид, параметры модуляции и т. д.) излучаемого высокочастотного сигнала. Навигационный сигнал L1C/A системы GPS получается путем модуляции несущей дальномерным кодом и информационным сообщением. При этом используется двоичная фазовая манипуляция. Структура навигационного радиосигнала, а также его спектр представлены на рис. 4, 5.

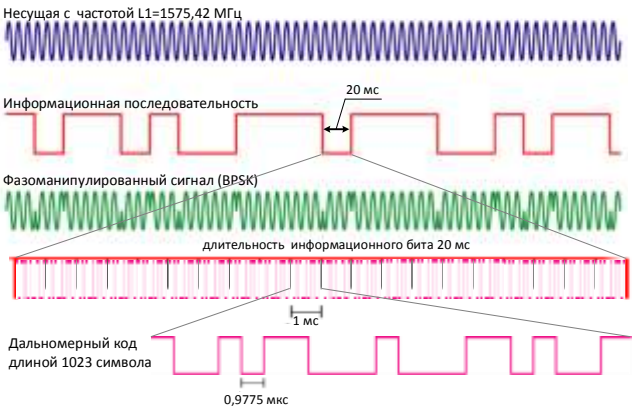


Рис. 4. Структура навигационного сигнала


Рис. 5. Спектр формируемого навигационного сигнала

### *B. Навигационные приемники*

Для проведения экспериментов по исследованию спуфинга было задействовано 2 навигационных устройства «Garmin Nuvi 710», «Mystery MNS-440MP».

Основной задачей этих устройств является поиск сигнала, слежение за сигналом, выделение навигационной информации и решение навигационной задачи.

Основными режимами работы НАП являются:

- Холодный старт – выполнение первого навигационного определения при отсутствии исходных данных.
- Теплый старт – выполнение первого навигационного определения при наличии исходных данных, включающих: достоверный альманах, плановые координаты, текущую дату и время, устаревших не более чем на 60 мин.
- Горячий старт – выполнение первого навигационного определения при наличии исходных данных и эфемеридной информации.

Устройства, используемые в исследованиях, помимо основных функций обеспечивают возможность просмотра уровней навигационных сигналов, а также текущего орбитального созвездия НКА.

На основе знания содержания навигационного сообщения, структуры навигационного сигнала, а также рассчитанных задержек от каждого НКА до имитируемой позиции формируются отсчёты группового навигационного сигнала с учетом частоты дискретизации SDR трансивера HackRF One, которая составляет 2,6 МГц. Полученные отсчеты записываются в файл, содержимое которого затем используется для формирования высокочастотного группового навигационного сигнала. При этом задержки сигналов внутри группового сигнала выстраиваются следующим образом: первым идёт навигационный сигнал с наименьшей задержкой и его дальномерный код начинается с первого символа, за ним сигнал со значением задержки больше первого, но меньше остальных и его дальномерный код задерживается относительно первого на требуемую величину и т. д. рис. 6.

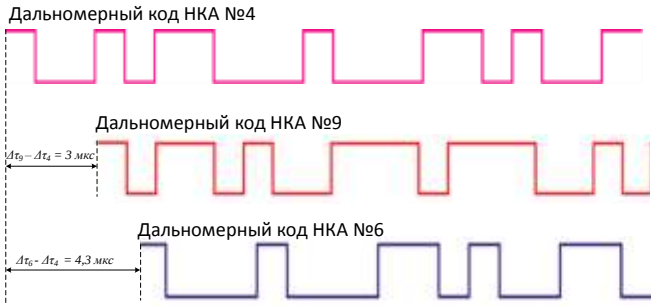


Рис. 6. Задержки дальномерных кодов друг относительно друга

## III. Результаты проведенных исследований

Для исследования эффективности спуфинг воздействий на навигационные приемники провести ряд различных экспериментов:

- Определение времени захвата навигационным приемником имитирующей помехи при различных уровнях помехи.
- Мощность излучения на выходе передающего устройства: 5,15,25,35 дБ.
- Определение времени захвата навигационным приемником имитирующей помехи при различной удаленности имитируемого местоположения от истинного.

Имитируемые координаты:

59,954992 30,285127 (100 м от исходного, СПб);
59,946015 30,285433 (1 км от исходного, СПб);
59,870461 30,379171 (10 км от исходного, СПб);
60,219995 31,972460 (100 км, с.Дубно Лен.обл.);
52,590068 39,616071 (1000 км, г. Липецк).

- Определение времени захвата навигационным приемником имитирующей помехи при различном рассогласовании по времени между истинным и ложным сигналами.

Сдвиг по времени: 1, 5, 10, 30, 60, 180, 360 мин

Следует отметить, что эксперименты проводились для одного из вариантов спуфинга, при котором сам ложный навигационный сигнал, обеспечивает срыв слежения за истинным сигналом (за счет большей мощности).

Данные, полученные в результате экспериментов, для повышения наглядности и упрощения анализа сведены в следующие графики и диаграммы рис. 7–10.

### *A. Эксперимент №1*

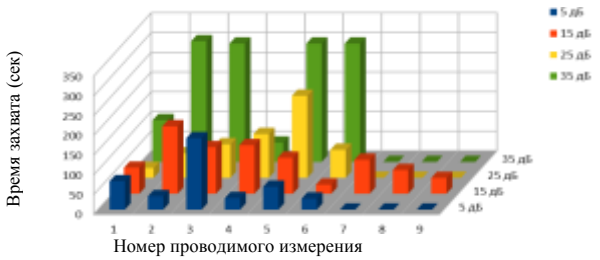


Рис. 7. Диаграмма времени захвата навигационным приемником имитирующей помехи при различных уровнях помехи

### *B. Эксперимент №2*

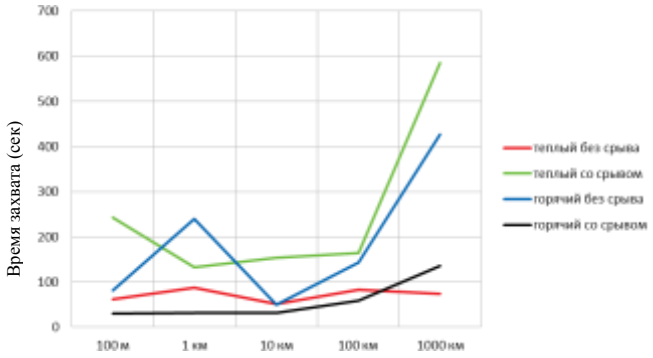


Рис. 8. График зависимости времени захвата имитирующей помехи от расстояния между истинными и ложными координатами (Garmin Nuvi 710)

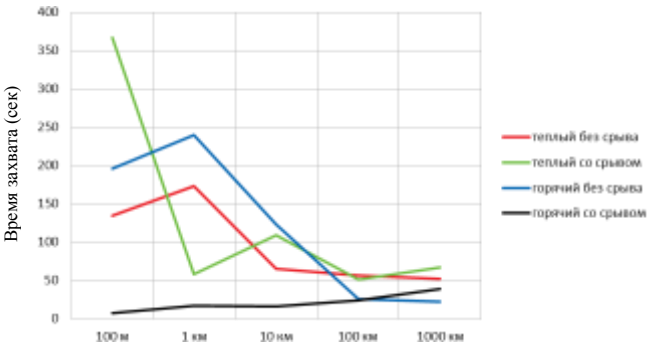


Рис. 9. График зависимости времени захвата имитирующей помехи от расстояния между истинными и ложными координатами (Mystery MNS-440MP)

### C. Эксперимент №3

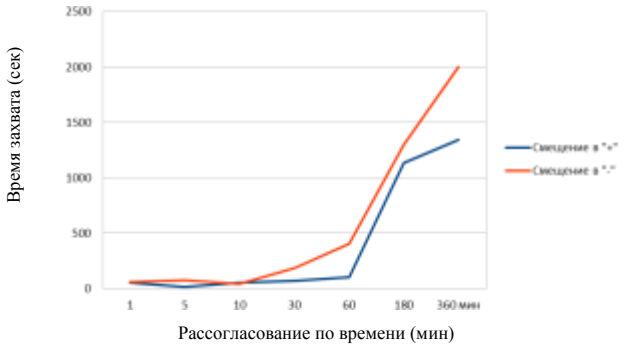


Рис. 10.График зависимости времени захвата имитирующей помехи от рассогласования по времени между истинным и ложным сигналами

Анализ результатов экспериментов показал, что для навигационных приемников наиболее опасным является спуфинг, при котором параметры формируемого ложного навигационного сигнала максимально близки к параметрам истинного сигнала.

Также стоит отметить, что разные навигационные приемники используют разные алгоритмы обработки сигналов, вследствие чего результаты по реакции на спуфинг воздействия, для разных приемников могут существенно отличаться рис. 8–9.

Самый быстрый перезахват сигнала с истинного на ложный происходит при минимальной мощности излучения на выходе передающего устройства, при минимальной расстройке ложного и истинного сигнала по расстоянию, а также при минимальной расстройке между временем на навигационном приемнике и опорным временем на КА в навигационном сигнале.

## IV. Заключение

Разработанный ПАК обеспечил возможность проведения исследований по воздействию имитирующих помех на навигационные приемники системы GPS. Полученные результаты позволили определить максимально опасные, для навигационных приемников, условия, при которых происходит навязывание ложного навигационного сигнала.

Дальнейшим направлением исследований станет совершенствование ПАК для формирования уводящей имитирующей помехи (спуфинг без срыва слежения) и исследования особенностей её реализации.

## Список литературы


[1] Фомин А.В., Вознюк В.В., Маслаков П.А. Исследование помехоустойчивости аппаратуры потребителей глобальной навигационной спутниковой системы GPS на основе технологии программного приема // Труды Военно-космической академии имени А.Ф.Можайского. Вып.№650. СПб.: ВКА, 2016. С. 33-40.

[2] Посохин Н.И., Сонников В.Г., Максимов Ю.Н. Радиоэлектронная борьба. СПб: ВКА имени А.Ф. Можайского, 2004. 522 с.

[3] Конин В.В. Спутниковые навигационные системы. Киев, 2008. 249 с.

[4] ГОСТ Р 52928-2010. Система спутниковая навигационная глобальная. Термины и определения. М.: Стандартинформ, 2011. 16 с.

[5] Джейм Бао-Йен Тсуи. Общая информация о приемниках глобальной навигационной системы. Глава 2 «Принципы GPS: Программный подход.»

[6] Interface specification. IS-GPS-200L. Navstar GPS Space Segment/Navigation User Interface / Global positioning systems directorate. Systems engineering & integration, 2020.

[7] Официальная информация правительства США о Глобальной системе позиционирования (GPS) и связанных темах [Электронный ресурс]. – Режим доступа: https://www.gps.gov/multimedia/presentations/2020/IGNSS/auerbach.pdf, свободный – (14.08.2020).

[8] Московский авиационный институт (Государственный технический университет) Каф. № 401 «Радиолокация и радионавигация» [Электронный ресурс]. – Режим доступа: http://kaf401.rloc.ru/files/GPS_signals.pdf-, свободный – (18.08.2020).

[9] Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки [Электронный ресурс] – Режим доступа: https://github.com/osqzss/gps-sdr-sim, - свободный – (14.08.2020).

[10] RINEX v2.11 (The Receiver Independent Exchange Format) 27 октября 2008 г.