[Методы РЭБ в области космической навигации и обеспечение безопасности КА]

ДОКЛАДЧИК: [l1th1um]

Whoami

- technician (electronics repair engineer)
- bachelor (telecommunications and theoretical radiophysics)
- HW dev
- engineer researcher
- young master of information security ☺

Немного теории

Основным элементом радиоэлектронной борьбы является нарушение радиообмена между радиоэлектронными средствами передачи информации путем постановки помех и фальшцелей.

Классификация помех и радиосигналов

С информационной точки зрения сигналы делят на:

- детерминированные
- случайные

Наряду с полезными случайными сигналами в теории и практике приходится иметь дело со случайными помехами — **шумами**.

Подразделение радиосигналов в зависимости от их природы:

- управляющие
- информационные

Непрерывные и цифровые.

В связи с этим применяемые в современной радиоэлектронике сигналы можно разделить на следующие классы:

- о произвольные по величине и непрерывные по времени (рис. 1а);
- о произвольные по величине и дискретные по времени (рис. 1б);
- о квантованные по величине и непрерывные по времени (рис. 1в);
- о квантованные по величине и дискретные по времени (рис. 1г).

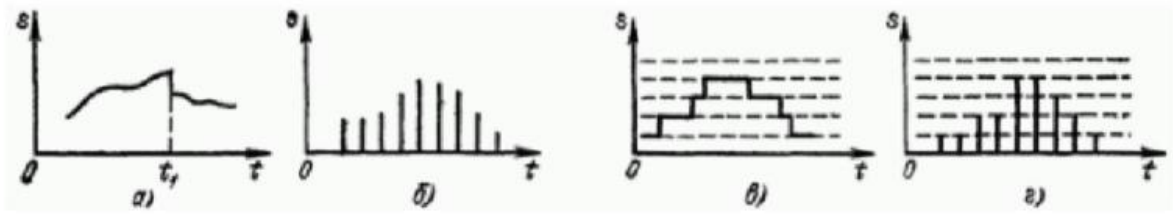


Рисунок 1. Виды радиосигналов

Разновидности помех

- пассивные:
  - атмосферные;
  - индустриальные; межсистемные;
- активные:
  - преднамеренные;

В зависимости от способа наведения помех:

- заградительные помехи;
- прицельные помехи.

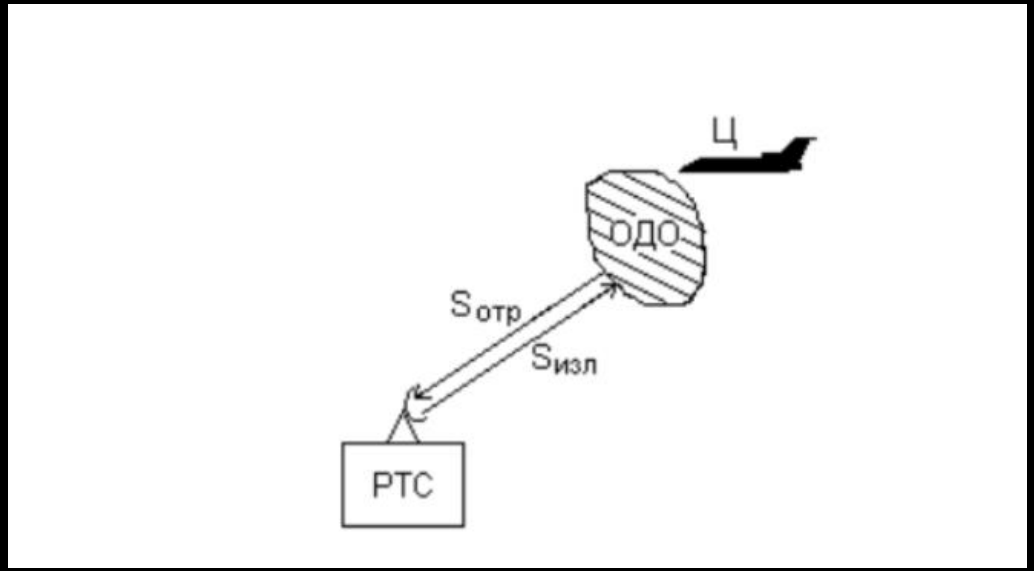
По временной структуре:

- непрерывные;
- импульсные.

Разновидности помех

- неорганизованные (естественные, неумышленные)
- организованные (искусственные, умышленные)

Сильнее всего на работу НАП (навигационной аппаратуры потребителя) могут влиять **пассивные организованные помехи.**



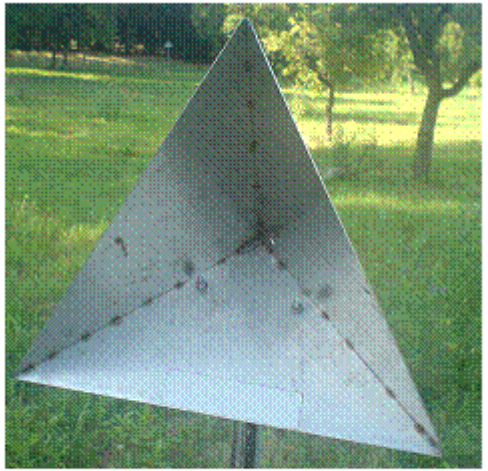


Рис.5 Уголковый отражатель радиодиапазона.

Разновидности помех по характеру (эффекту) воздействия:

- маскирующие
  - сильные - превышают по уровню полезный сигнал, что исключает РЭС выполнение боевых задач),
  - о средние (соизмеримые с полезным сигналом, их воздействие вызывает потерю информации не менее 50%.),
  - о слабые (по энергетическому уровню не превышают потерю до 15% информации).
- имитирующие
- подавляющие

Преимущества имитационных помех:

1. При воздействии ИП противник не подозревает о том, что подвергся нападению, и, следовательно, не предпринимает ответных действий. В отличие от этого при выявлении МП (маскирующих помех) у него есть возможность прибегнуть к целому ряду защитных действий:

- отказаться от навигации по глобальным спутниковым навигационным системам и использовать автономные навигационные системы, такие как инерциальная навигационная система или магнитный компас;
- осуществлять подавление широкополосных МП с помощью адаптивной антенной решетки (ААР), узкополосных МП на основе алгоритмов спектральной режекции, импульсных МП – временной режекцией;
- принять организационные меры по физическому уничтожению источников помех.

Преимущества имитационных помех:

2. Мощность принимаемой ИП принципиально должна не слишком отличаться от мощности принимаемого навигационного сигнала S.

3. Основным средством защиты от помех в НАП является ААР, которая осуществляет подавление помех, мощность которых превышает уровень внутренних шумов приемника. Так как мощность ИП сопоставима с мощностью реального сигнала (уровень шумов), то ИП проходит через ААР без ослабления.

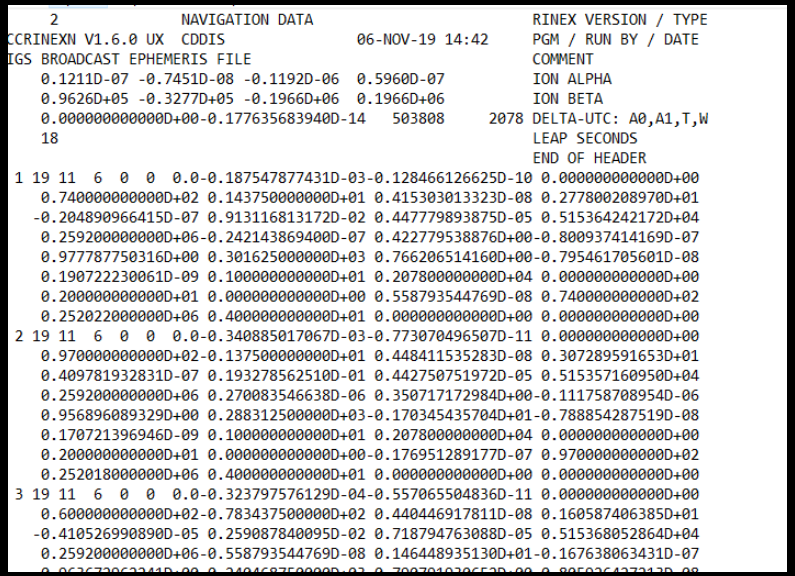
Преимущества ИП относительно МП, приведенные выше, столь значительны, что вызывают постоянный интерес к возможностям и методам создания и применения ИП. Пристальное внимание к ИП особенно обострилось в последнее время в связи с целой серией публикаций в отечественной и зарубежной прессе, впрямую посвященных применению ИП.

Имитирующие помехи для НАП for InfoSec dummies = GPS Spoofing

Зачем?

- угон яхт
- браконьерство
- военные операциии
- угон дронов
- угон автомобилей
- угон беспилотников
- угон военных беспилотников

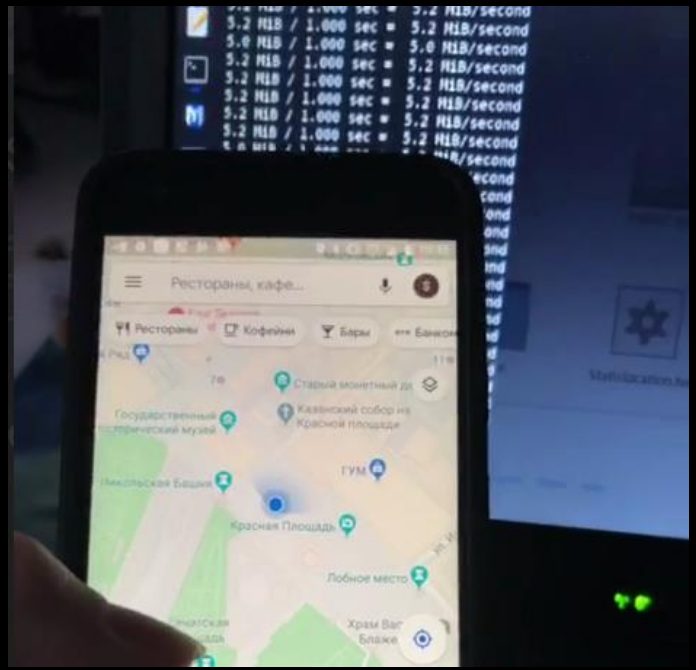
GPS Spoofing with HackRF in 4 steps

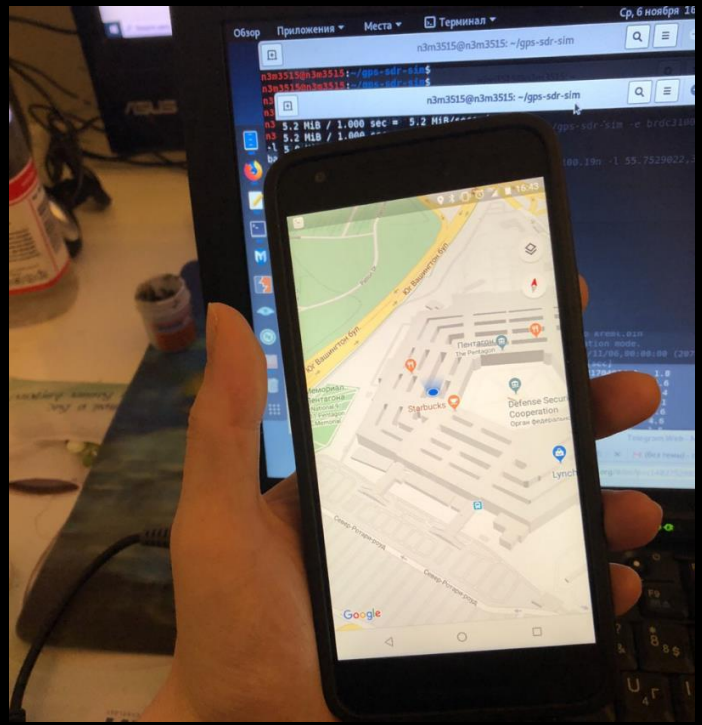


```
     2             NAVIGATION DATA                         RINEX VERSION / TYPE
CCRINEXN V1.6.0 UX  CDDIS               06-NOV-19 14:42     PGM / RUN BY / DATE
IGS BROADCAST EPHEMERIS FILE                                COMMENT
    0.1211D-07 -0.7451D-08 -0.1192D-06  0.5960D-07          ION ALPHA
    0.9626D+05 -0.3277D+05 -0.1966D+06  0.1966D+06          ION BETA
    0.000000000000D+00-0.177635683940D-14   503808     2078 DELTA-UTC: A0,A1,T,W
    18                                                      LEAP SECONDS
                                                            END OF HEADER
 1 19 11  6  0  0  0.0-0.187547877431D-03-0.128466126625D-10 0.000000000000D+00
    0.740000000000D+02 0.143750000000D+01 0.415303013323D-08 0.277800208970D+01
   -0.204890966415D-07 0.913116813172D-02 0.447779893875D-05 0.515364242172D+04
    0.259200000000D+06-0.242143869400D-07 0.422779538876D+00-0.800937414169D-07
    0.977787750316D+00 0.301625000000D+03 0.766206514160D+00-0.795461705601D-08
    0.190722230061D-09 0.100000000000D+01 0.207800000000D+04 0.000000000000D+00
    0.200000000000D+01 0.000000000000D+00 0.558793544769D-08 0.740000000000D+02
    0.252022000000D+06 0.400000000000D+01 0.000000000000D+00 0.000000000000D+00
 2 19 11  6  0  0  0.0-0.340885017067D-03-0.773070496507D-11 0.000000000000D+00
    0.970000000000D+02-0.137500000000D+01 0.448411535283D-08 0.307289591653D+01
    0.409781932831D-07 0.193278562510D-01 0.442750751972D-05 0.515357160950D+04
    0.259200000000D+06 0.270083546638D-06 0.350717172984D+00-0.111758708954D-06
    0.956896089329D+00 0.288312500000D+03-0.170345435704D+01-0.788854287519D-08
    0.170721396946D-09 0.100000000000D+01 0.207800000000D+04 0.000000000000D+00
    0.200000000000D+01 0.000000000000D+00-0.176951289177D-07 0.970000000000D+02
    0.252018000000D+06 0.400000000000D+01 0.000000000000D+00 0.000000000000D+00
 3 19 11  6  0  0  0.0-0.323797576129D-04-0.557065504836D-11 0.000000000000D+00
    0.600000000000D+02-0.783437500000D+02 0.440446917811D-08 0.160587406385D+01
   -0.410526990890D-05 0.259087840095D-02 0.718794763088D-05 0.515368052864D+04
    0.259200000000D+06-0.558793544769D-08 0.146448935130D+01-0.167638063431D-07
```

1. https://github.com/n3m351d4/gps-sdr-sim
2. ftp://cddis.gsfc.nasa.gov/gnss/data/daily/2019/brdc/
3. ./gps-sdr-sim -e brdc3100.19n -l 38.8710298,-77.0573827, **17 -b 8** -o file.bin
4. hackrf_transfer -t gpssim.bin -f 1575420000 -s 2600000 -a 1 -x 0

Android


Рестораны, кафе...
Рестораны
Кофейни
Бары
Красная Площадь
ГУМ
Лобное место


Обзор
Приложения
Места
Терминал
n3m3515@n3m3515: ~/gps-sdr-sim
Starbucks
Google

Проектирование устройства генерации ИП для НАП

Если атакующая сторона имеет возможность передавать ИП НАП, то она может сфальсифицировать для этого приёмника любую конфигурацию спутников и, в общем случае, приёмник не сможет отличить виртуальные координаты от подлинных.

Существует возможность генерировать ИП с опережением по времени.

НС спроектирован таким образом, чтобы сделать возможным приём на слабом уровне, ниже шумов. НАП используют тот или иной коррелятор, позволяющий получить достаточное соотношение сигнал/шум. Это, с одной стороны, означает, что сигнал ИП может совсем незначительно превышать мощность подлинного сигнала – коррелятор всё равно «переключится» именно за него (другими словами: обнаружить факт наличия ИП по возросшей мощности сигнала – не выйдет).

Военные диапазоны – код доступа есть? А если найду?

Аутентификация в военной навигационной системе реализована с использованием кода доступа, который засекречивается и изменяется через некоторое время. Он, предположительно, передается лично в руки и используется для расшифровки сигнала спутника.

Так как коды доступа в реальном времени получить будет сложно, то отличным выходом из данной ситуации будет являться подмена сигнала заранее записанным сигналом военного диапазона. Путем трансляции военного навигационного сигнала с небольшой задержкой по времени, данный вектор атаки на военные навигационные протоколы становится вполне реальным.

Подробнее здесь (Ctrl+F military):
https://www.cs.ox.ac.uk/files/6489/gps.pdf

Обнаружение ИП, принятых НАП

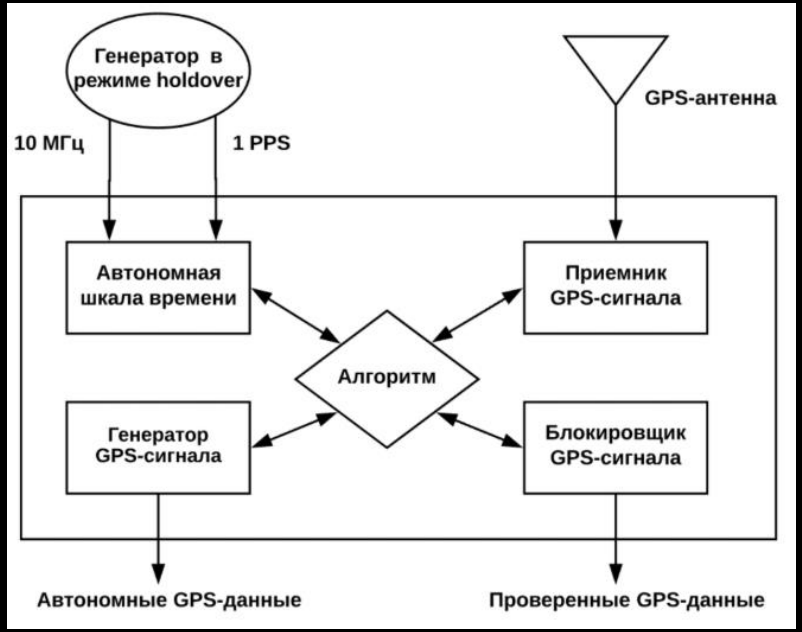
Статичная ИП будет определяться по потере сигнала, с последующим восстановлением в совсем другой (имитируемой) точке пространства.

При наличии трех НАП, находящихся на расстоянии нескольких сотен метров друг от друга, с известными расстояниями между ними известны. В случае обычной постановки ИП, после того, как приёмники захватят ложный сигнал, они «переместятся» в одну точку.

Структурная схема системы обнаружения ИП в НАП, данное устройство выступает в качестве буфера между антенной и НАП.

В данном устройстве реализованы алгоритмы, которые оценивают характеристики НС:

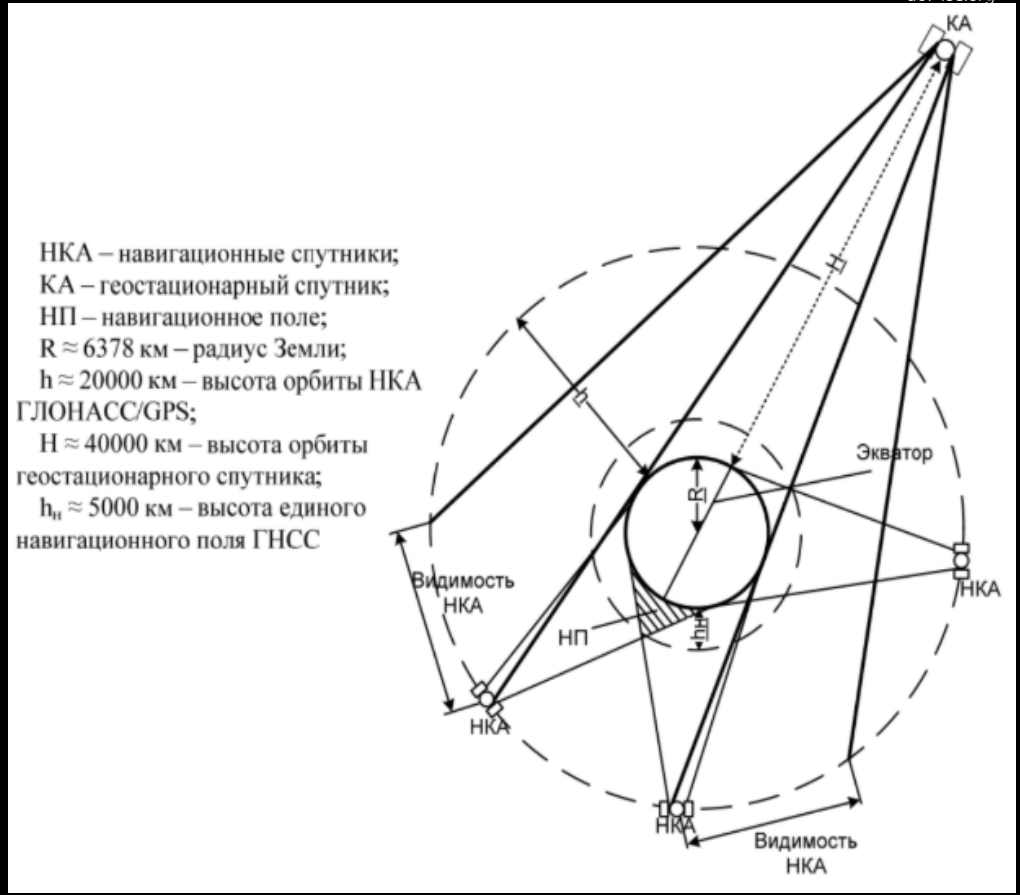
- о радиочастотную мощность,
- о корректность геоданных
- о корректность времени



КА = Потребитель?

Наличие навигационных приемников на борту КА значительно упрощает определение их местонахождения.

Так же, как и любая другая НАП, космическая НАП может быть подвержена воздействию комплексами противоспутниковой радиоэлектронной борьбы, в том числе и ИП.

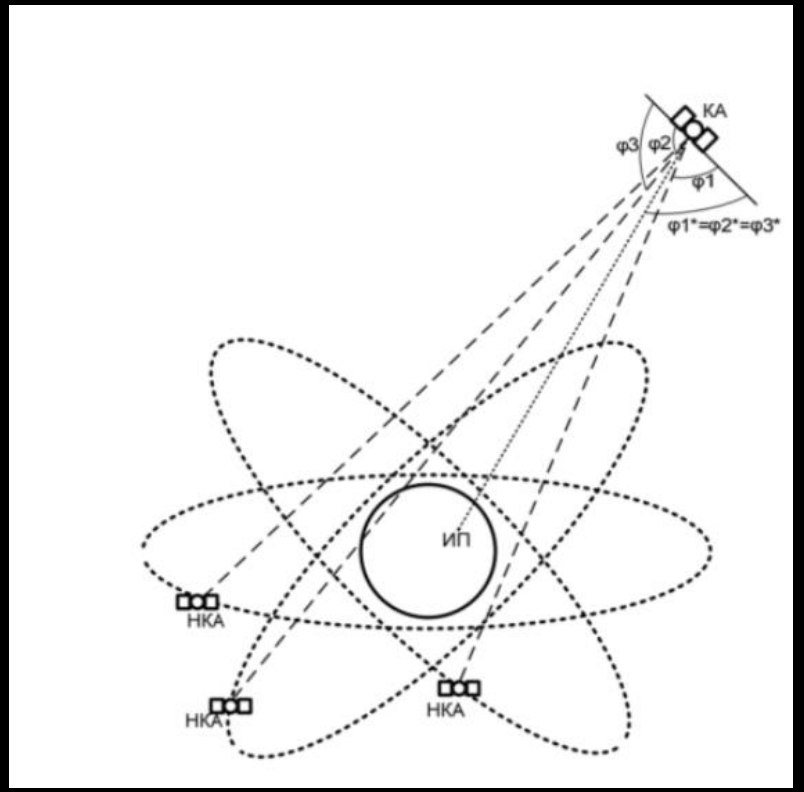


Влияние ИП на КА

Приемные антенны КА, находящегося на ГСО, направлены на Землю, так как улавливают сигналы от НКА перед их заходом и выходом из-за Земли.

Это значит, что бортовая НАП такого КА легко подвергается наведению ложного сигнала с поверхности Земли.

Средний срок жизни спутника на орбите 10 лет, а некоторые “доживают” до 15 лет (в основном спутники иностранного производства). 190-230 млн. долларов стоит постройка и вывод спутника на геостационарную орбиту.



Еще немного векторов

В отношении многих спутников, разработчики никогда не предполагали, что люди на земле будут пытаться перехватить, либо подменить сигнал. При ограниченном объеме памяти и вычислительной мощности многие спутники даже не используют шифрование данных.

Например, зонд Voyager 1 должен будет обрабатывать биты в течение шести дней только для того, чтобы установить соединение SSL. Об этом следует помнить инженерам, поскольку устройства с низким энергопотреблением, такие как CubeSats, становятся все более распространенными. (Extremetech: Hacking Satellites Is Surprisingly Simple)

Так же существует такой вектор, как взлом SATCOM терминалов. (Blackhat:SATCOM Terminals: Hacking by Air, Sea, and Land)

Если это ИБ, то нужен багфикс. Выявление ИП в КА

«Простые» методы выявления в НАП ложных НС:

- о слежение за абсолютной мощностью каждой несущей частоты НС;
- о слежение за скоростью изменения мощности сигнала;
- о слежение за относительными мощностями принимаемого сигнала;
- о сравнение скоростей динамики кода и фазы;
- о проверка целостности полученных данных.

Кроме указанных способов защиты можно предложить реализуемые уже сегодня относительно более сложные способы различения сигналов НКА и ИП, использующие их пространственные отличия. Они предполагают наличие вместо одной приемной антенны нескольких разнесенных в пространстве.

Contact me: Telegram: @N3M351DA

Read more: Telegram : @in51d3

Useful links & Литература

- https://www.blackhat.com/docs/eu-15/materials/eu-15-Kang-Is-Your-Timespace-Safe-Time-And-Position-Spoofing-Opensourcely-wp.pdf
- https://blog.csdn.net/OpenSourceSDR/article/details/51968678
- Source: Кафедра телекоммуникаций и теоретической радиофизики, отчёт по преддипломной практике, Тема: «Методы РЭБ в области космической навигации и обеспечение безопасности КА» (N3M351D4).
- Справочник «Радиоэлектронные системы» – Основы построения и теория. / Под ред. Я.Д. Ширмана (изд. 2-е переработанное и дополненное), М.: «Радиотехника», 2007.
- Радиотехнические системы. / Под ред. Ю.М. Казаринова, М.: «Высшая школа», 1990. – 496 с.

Useful links & Литература

- Гоноровский И. С. Радиотехнические цепи и сигналы: Учебник для вузов. — 4-е изд., перераб, и доп. — М.: Радио и связь, 1986. — 512 с.
- Никольский, Б. А. Основы теории систем и комплексов радиоэлектронной борьбы [Электронный ресурс] : электрон. учеб. пособие /Б.А.Никольский; Минобрнауки России, Самар. гос. аэрокосм. ун-т им. С. П. Королева (нац. исслед. ун-т).
- https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/
- https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf
- Чердынцев В.А. Радиотехнические системы, Минск: «Высшая школа», 1988. – 369 с.

Useful links & Литература

- https://www.cs.ox.ac.uk/files/6489/gps.pdf
- https://www.technologyreview.com/f/613912/military-satellites-are-still-worryingly-vulnerable-to-cyberattack/
- https://www.extremetech.com/extreme/287284-hacking-satellites-is-probably-easier-than-you-think
- https://www.cs.ox.ac.uk/files/6489/gps.pdf
- https://www.technologyreview.com/f/613912/military-satellites-are-still-worryingly-vulnerable-to-cyberattack/
- https://www.extremetech.com/extreme/287284-hacking-satellites-is-probably-easier-than-you-think