УДК 007.2

Практика тестирования навигационного оборудования в условиях активного радиоэлектронного противодействия

Солдатов О. А., технический директор ООО «ЮНИТЕСС», 117218 Москва, Нахимовский пр-т, д. 24 стр.9, помещ.I, эт.4, ком.22,23, тел. +375 29 248-62-90, os@unitess.ru

Мазаник А.В., генеральный директор ООО «ЮНИТЕСС», 117218 Москва, Нахимовский пр-т, д. 24 стр.9, помещ.I, эт.4, ком.22,23, тел. +7 909 918-42-50, mazanik.aleksandr@unitess.ru

Аннотация

В статье рассматривается практика тестирования навигационного оборудования на подверженность атакам с подменой или подавления навигационного сигнала. Показана актуальность проблемы в связи с ростом зависимости критически важных инфраструктур от данных ГНСС. Описаны основные типы атак — глушение, когерентный и некогерентный спуфинг, а также влияние на приёмники промышленного и гражданского назначения. Представлена архитектура автоматизированного комплекса испытаний на базе имитатора ГНСС, разработанного автором. Приведены примеры сценариев атак, зарегистрированные отклонения координат и времени, а также сравнительный анализ поведения приёмников разных производителей. Сделаны выводы о необходимости включения устойчивости к РЭБ-воздействию в цикл приёмки оборудования и предложено использовать комплекс в качестве средства технического контроля и сертификации.

Abstract

The article examines the practice of testing navigation equipment for vulnerability to spoofing and jamming of GNSS signals. The relevance of the issue is highlighted in the context of increasing dependence of critical infrastructure on GNSS-derived data. The main types of attacks—jamming, coherent and non-coherent spoofing—are described, along with their impact on both industrial and civilian-grade receivers. The architecture of an automated test system based on a custom-developed GNSS simulator is presented. The article provides examples of attack scenarios, recorded deviations in position and time, as well as a comparative analysis of receiver behavior across different manufacturers. The study concludes with recommendations to include resistance to electronic countermeasures in the equipment acceptance process and proposes using the test system as a tool for technical control and certification.

1. Актуальность проблемы

Современная инфраструктура — от энергетики и телекоммуникаций до финансовых систем и объектов оборонного значения — критически зависит от точных координат и времени, предоставляемых системами ГНСС. Такие данные лежат в основе синхронизации вычислительных процессов, расчётов в биржевых и банковских системах, позиционирования мобильных и стационарных объектов.

Однако открытость навигационного сигнала делает его уязвимым к целенаправленным атакам — глушению (джаминг) и подмене сигнала (спуфингу). Применение подобных атак зафиксировано как в военных конфликтах, так и в инцидентах с гражданской инфраструктурой. Это создаёт необходимость в испытании оборудования на устойчивость к радиоэлектронному противодействию.

2. Типы атак

В рамках испытаний исследовались следующие типы воздействий:

- Широкополосные помехи (jamming): создание сигнала в диапазоне 1575–1602 МГц с регулируемой мощностью от -120 дБм до -50 дБм, блокирующего приём легитимных ГНСС-сигналов.
- Некогерентный спуфинг: резкая подмена сигнала ложной навигационной информацией без предварительной синхронизации с текущим положением.
- Когерентный спуфинг: синхронизированная подмена сигнала с плавным отклонением координат и/или времени, часто не вызывающая тревог у приёмников.
- Комбинированные сценарии: атаки, совмещающие подавление и подмену сигнала, в том числе с искажением временной шкалы.

3. Поведение и реакция приёмников

Испытания проводились на оборудовании производителей u-blox и Septentrio, а также на серверах времени, используемых в промышленности, дата-центрах, на судах и в других критических системах. Все приёмники поддерживают приём 4 типов навигационных сигналов: GPS, ГЛОНАСС, Galileo, BeiDou.

Зафиксированные реакции:

- При некогерентном спуфинге устройства u-blox в большинстве случаев теряли возможность определения координат и через некоторое время переключались на имитационный сигнал. Встроенный в приемники u-blox механизм обнаружения спуфинга не сигнализировал о подмене сигнала. При когерентной атаке в 100% случаях переключались на имитационный сигнал.
- При некогерентной атаке модели Septentrio случаев теряли возможность определения координат и редко переключались на подменный сигнал до перезапуска. При когерентной атаке приемники принимали ложные координаты без тревожных флагов.
- Сервера времени продемонстрировали отклонение при некогерентной атаке и смещение временной метки при когерентной, если сдвиги были не резкими. Некоторые устройства переходили в режим "hold" или "no fix", полное восстановление сигнала происходило через 15 минут после снятия воздействия.

4. Методика испытаний

Испытания проводились с использованием разработанного автоматизированного комплекса на основе имитатора ГНСС ЮНИТЕСС, как в лабораторных условиях, так и на открытых площадках (в т.ч. в городской среде).

Архитектура комплекса:

- Генератор ГНСС (с возможностью программного задания динамики, мощности, числа спутников и параметров отклонения);
- ПК управления для настройки ложного сигнала;
- Логирование (фиксация координат и временных отклонений, реакций приёмников, сообщений о сбоях);

Комплекс позволяет создавать сценарии, специфичные для области применения, включая возможность имитации перемещающегося источника или изменения условий радиообстановки.

5. Результаты тестирования

Примеры сценариев:

- Сценарий 1 (когерентный спуфинг): плавное смещение координат на 500 м в течение 100 секунд.
- Сценарий 2 (некогерентный спуфинг): подавление оригинального сигнала имитационным сигналом мощностью -80 дБм. Момент потери слежения зависит

от дальности до приемника, при кондуктивном подключении начинается при -100 дБм.

- Сценарий 3 (временной сдвиг): подмена временной метки на 10 мс каждую минуту.

6. Выводы и предложения

1. Устойчивость приёмников и серверов времени варьируется в разы, что подтверждает необходимость проведения целевых испытаний перед развертыванием оборудования в критических объектах.
2. Рекомендуется включать испытания на устойчивость к радиоэлектронному противодействию в процедуры приёмки поставляемого оборудования, особенно в госсекторе и энергетике.
3. Разработанный комплекс может применяться:
    - как инструмент сертификации;
    - как средство контроля качества приёмников;
    - для регулярного технического контроля в эксплуатации.

Библиографические ссылки

1. Wang H., Yang L., Zhang X., Wu J. Recent advances on jamming and spoofing detection in GNSS [Текст] / англ. // Sensors. – 2024. – Vol. 24, № 13. – P. 4210.
2. Liu Y., Li Z., Xu J., et al. A survey of GNSS spoofing and anti-spoofing technology [Текст] / англ. // Remote Sensing. – 2022. – Vol. 14, № 19. – P. 4826.
3. Alghamdi A., Zhang W., Singh R. GNSS/GPS spoofing and jamming identification using machine learning and deep learning [Электронный ресурс]. – Режим доступа: https://example.com. – Дата обращения: 30.06.2025. – 2025.
4. Rao D., McCarthy B., Bernstein J. UnReference: analysis of the effect of spoofing on RTK reference stations for connected rovers [Электронный ресурс]. – Режим доступа: https://example.com. – Дата обращения: 30.06.2025. – 2025.