Симулятор сигналов GNSS как инструмент для контроля устойчивости навигационного оборудования к джаммингу и спуфингу

Статья адресована специалистам, ответственным за оценку и управление рисками при работе с системами, использующими сигналы спутниковой навигации. Перечислены основные факторы, влияющие на сигналы глобальных спутниковых систем (GNSS), и методы защиты сигналов. Рассказано о разработке компанией ЮНИТЕСС мер по снижению рисков.

Компания ЮНИТЕСС, г. Москва

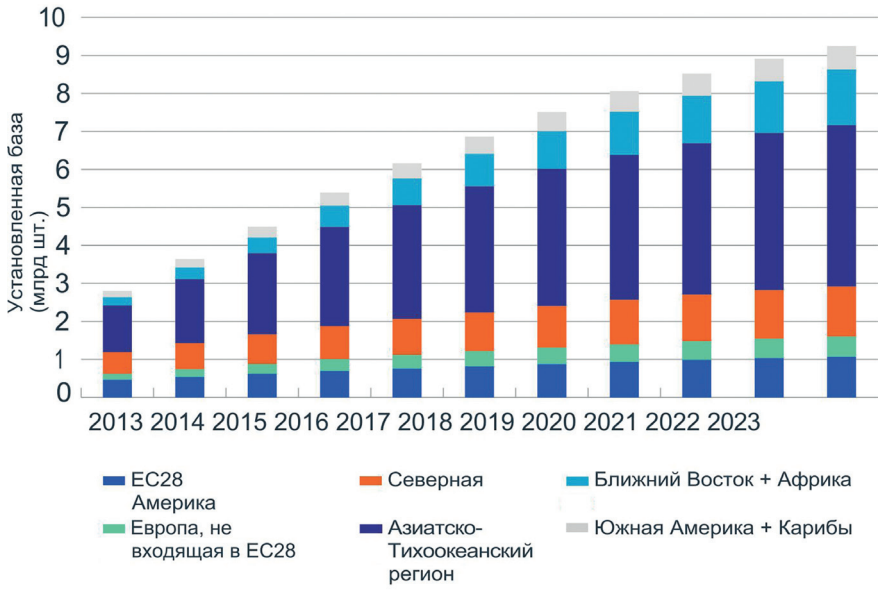
GPS или GNSS? Раньше единственной глобальной навигационной спутниковой системой была американская GPS, обеспечивающая точные координаты и время для военных и гражданских нужд. Сегодня существуют и другие глобальные системы, включая российскую ГЛОНАСС, китайскую BeiDou и европейскую Galileo, а также несколько региональных систем навигации. В совокупности их называют глобальными навигационными спутниковыми системами, или GNSS.

Данная статья адресована специалистам, ответственным за оценку и управление рисками в системах, работающих на основе GNSS, с акцентом на разработку мер по снижению этих рисков. В статье вы найдете:

- исследование уязвимостей сигналов GNSS перед растущим числом угроз;
- обзор основных угроз для GNSS и современных методов их устранения;
- описание наиболее эффективных методик для минимизации риска сбоев, ошибок и кибератак на критически важные системы;
- обзор услуг компании ЮНИТЕСС, направленных на оценку и снижение угроз для GNSS.

Растущая зависимость от GNSS

Глобальные навигационные спутниковые системы (GNSS) стали неотъемлемой частью современной инфраструктуры и повседневной жизни, оказывая колоссальное влияние на многие отрасли. Наш мир все больше зависит от точных данных о времени и местоположении, предоставляемых GPS и другими GNSS. Сегодня мно-



Источник: GSA GNSS Market Report

Рис. 1. Установленная база устройств GNSS по регионам

жество систем и устройств критически зависят от этих технологий, обеспечивая сервисы, на которые мы привыкли полагаться.

Круг областей применения GNSS постоянно расширяется (рис. 1), что объясняет прогнозируемый рост мирового рынка GNSS до 500 млрд евро в ближайшее десятилетие. Широкое распространение навигационных технологий ожидается в транспорте, мобильных устройствах, сети и автоматизированных системах управления, что приведет к еще более тесной интеграции GNSS с нашей жизнью.

Основные угрозы для сигналов GNSS

Влияние растущих угроз на сигналы спутниковой навигации может существенно сказаться на стабильности и безопасности критически важных систем, использующих GPS. Нарушения в работе навигационных сигналов приводят к потере точности координат, ошибкам синхронизации и даже полной недоступности данных, что особенно опасно для систем, требующих высокой надежности. Перечень основных факторов влияния включает:

- солнечную активность. Высокая активность солнца вызывает радиопомехи, которые затрудняют передачу и обработку сигналов. В периоды усиленной солнечной активности возрастает вероятность перебоев в работе навигации;
- техногенные помехи. Радиоизлучение от земных передатчиков, таких как мобильные вышки и радиопередатчики, может блокировать или искажать сигналы GNSS, вызывая задержки и ошибки в определении местоположения;
- злонамеренные вмешательства (спуфинг и джамминг). Злоумышленники могут намеренно глушить (джамминг) или подменять (спуфинг) сигналы GNSS. Спуфинг – это подмена сигнала с целью передачи ложной информации, а джамминг направлен на блокировку сигнала, делает его недоступным для приемников;
- манипуляции с данными о времени и местоположении. Поскольку многие критически важные системы зависят от точного времени, любое нарушение в передаче временных данных может создать каскадные ошибки, влияющие на целые сети и цепочки поставок.

Обзор методов защиты сигналов GNSS

Для большинства пользователей GNSS является невидимым инструментом, который ежедневно помогает с навигацией, управляет транспортом и обеспечивает выполнение важных функций в нужном месте и в нужное время. Однако инженерам и специалистам, которые отвечают за стабильную работу этих систем, очевидно, что сигналы GNSS, исходящие от спутников, обладают высокой уязвимостью. Они слабые и легко подвержены влиянию множества факторов, которые могут нарушить или скомпрометировать их работу.

Возможные методы защиты:

- **от глушения сигналов (джамминга)** – блокировки сигналов GPS посредством мощного излучения. *Решение:* установка фильтров и систем обнаружения глушения;
- **от подмены сигналов (спуфинга)** – подделки GPS-сигнала с целью передачи ложных данных о местоположении. *Решение:* внедрение многополосных GNSS-приемников и использование вспомогательных технологий, таких как инерциальная навигация;
- **от кибератак** – попыток злоумышленников получить доступ к системам, работающим на GPS. *Решение:* усиленная кибербезопасность и регулярное обновление протоколов безопасности;
- **для исключения зависимости от одной навигационной системы** – использование только GPS делает системы уязвимыми к единственной точке сбоя. *Решение:* интеграция других GNSS (например, ГЛОНАСС, Galileo, BeiDou) для создания устойчивой многоуровневой навигации.

Эти угрозы требуют комплексного подхода к безопасности, включающего передовые защитные технологии, непрерывный мониторинг возможных угроз и регулярные тестирования оборудования и процессов. Такой подход позволяет не только предотвратить потенциальные атаки, но и своевременно реагировать на изменяющиеся условия внешней среды и технологические риски.

При разработке надежной защиты GNSS-систем важно не только учитывать профиль угроз, но и обеспечить внедрение адекватных мер для минимизации рисков. Уровень защиты подбирается с учетом особенностей устройства, системы и требований к точности. Применение требует комплексного подхода, начиная от устойчивых приемников и заканчивая альтернативными источниками данных. К основным методам относятся:

- **многочастотные приемники.** Использование приемников, способных принимать сигналы на нескольких частотах (например, L1, L2, L5 для GPS), существенно повышает устойчивость к глушению и спуфингу, поскольку злоумышленнику становится значительно сложнее заблокировать или подделать многоканальный сигнал. Также приемники с функцией перекрестной проверки частот могут более точно определять местоположение и устранять многопутевые искажения;
- **многосистемные GNSS-приемники.** Современные многосистемные приемники, поддерживающие одновременно GPS, ГЛОНАСС, Galileo и BeiDou, более устойчивы к внешним помехам, так как сбой в одной системе не приводит к потере навигации. Эти приемники минимизируют риск затухания сигнала, глушения и подделки, что особенно важно для критически важных систем;
- **улучшенные антенны.** Правильно подобранная антенна может значительно повысить качество сигнала GNSS. Например, антенны с высоким коэффициентом усиления и подавлением боковых лепестков минимизируют помехи, а некоторые модели способны отфильтровывать сигналы, приходящие под углом, нехарактерным для спутниковой связи. Антенны с защитой от спуфинга, такие как многоэлементные или фазированные решетки, еще более эффективны, так как способны использовать формирование луча для адаптации к условиям окружающей среды и максимизации точности;
- **альтернативные и резервные источники данных.** Использование дополнительных систем для получения данных о положении, навигации и времени (PNT) может компенсировать временные нарушения GNSS. Варианты включают инерциальные измерительные системы (IMU), позиционирование по Wi-Fi или сотовой связи, вспомогательные GNSS-системы и наземные резервные системы, такие как eLoran (для морских приложений) и WAAS или EGNOS (для авиации). Эти системы способны

обеспечить точное позиционирование и синхронизацию в случае временного выхода GNSS из строя;

‣ **дифференциальные системы и RTK.** Применение наземных корректирующих станций, таких как DGPS (дифференциальная GPS) и системы кинематического позиционирования в реальном времени (RTK), помогает обнаруживать аномалии и компенсировать ошибки, связанные с потерей сигнала или его подделкой. Такие системы активно используются в профессиональных приложениях, требующих высокой точности;

‣ **автономные методы контроля целостности приемников (RAIM).** RAIM-приемники могут самостоятельно обнаруживать и исключать ложные сигналы, оценивая целостность данных от спутников. Этот метод позволяет улучшить устойчивость к сбоям и защите от спуфинга и ложных сигналов;

‣ **технологии подавления многопутевых помех.** Многопутевые помехи, возникающие от отраженных сигналов, могут снизить точность и облегчить захват приемника спуфером. Применение усовершенствованных алгоритмов обработки сигнала помогает различать прямые и отраженные сигналы, повышая устойчивость к спуфингу и помехам;

‣ **зашифрованные сигналы GNSS.** Для стратегически важных объектов доступ к зашифрованным сигналам, таким как GPS PPS (Precise Positioning Service) для военных США или PRS (Public Regulated Service) от Galileo для европейской критической инфраструктуры, существенно повышает защиту. Зашифрованные сигналы гораздо сложнее подделать, и их использование становится все более востребованным для критически важных приложений.

При выборе методов защиты следует учитывать, что угрозы GNSS эволюционируют. Технологические улучшения требуют регулярного пересмотра применяемых мер защиты и своевременного обновления для обеспечения их актуальности и устойчивости к новым типам атак и помех.

Разработки компании ЮНИТЕСС: имитаторы сигналов GNSS

Компания ЮНИТЕСС была основана в 2011 году и в настоящее время включает три компании, зарегистрированные в России и Беларуси. Основное направление деятельности – разработка автоматизированных рабочих мест (АРМ) и стендов для поверочных и испытательных лабораторий. Среди клиентов – ведущие предприятия в области измерений, которым компания предоставляет решения, соответствующие самым высоким стандартам качества: China Academy of Information and Communications Technology (Китай), Qualcomm (Индия), CETECOM (Германия), ФБУ «Ростест-Москва», МТС, УЗГА (АО «Уральский завод гражданской авиации»), НПП «ИТЭЛМА» (Российская Федерация).

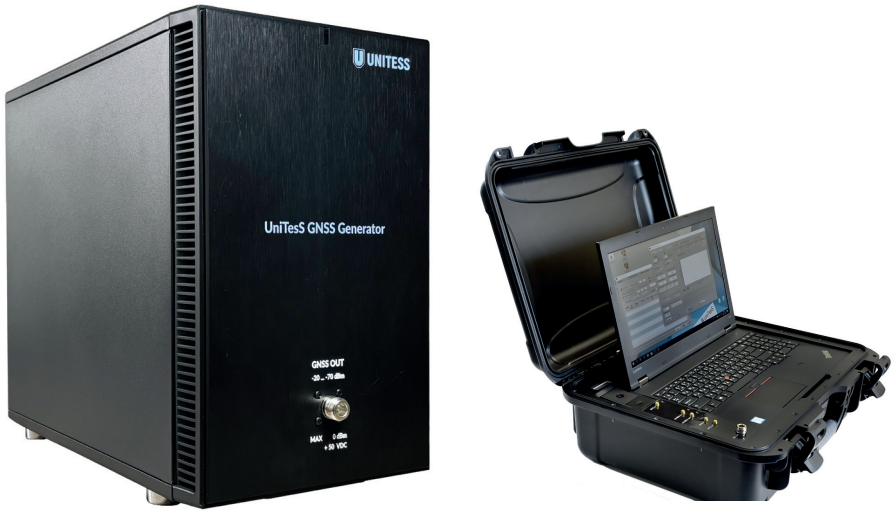
Таблица 1. Технические характеристики имитатора сигналов глобальных навигационных спутниковых систем ГЛОНАСС/GPS

Характеристика	Значение
Количество спутников GPS	12
Количество спутников ГЛОНАСС	12
Режимы имитации	Точка, сценарий
Динамический диапазон, дБВт	–20…–150
Погрешность: • по уровню, дБ, не более • по частоте • формирования	 ±1,0 1×10^{-9} псевдодальности по фазе дальномерного кода ⩽0,5 м; псевдоскорости ⩽0,01 м/с

Одной из последних разработок компании ЮНИТЕСС является имитатор сигналов глобальных навигационных спутниковых систем ГЛОНАСС/GPS. Данная модель выпускается в двух вариантах: стационарном (имитатор GNSS 1030Д) и переносном (имитатор GNSS 1030М с защитой IP67).

Оба варианта включают лицензию на генерацию сигналов одной из систем GNSS. В стационарном варианте предоставляется возможность генерации сигналов ГЛОНАСС с дальномерными кодами стандартной точности СТ (OF) в частотном диапазоне L1 либо сигналов GPS с дальномерным кодом стандартной точности C/A в частотном диапазоне L1. Подробные технические характеристики имитатора приведены в табл. 1.

Имитатор сигналов GNSS, получивший название UNITESS GNSS GENERATOR (рис. 2), предназначен для автоматизированного проведения испытаний и поверки навигационных приемников GPS и ГЛОНАСС. Устройство поддерживает как проводное, так и беспроводное подключение, что позволяет выполнять сравнительный анализ различных моделей приемников, проверять их работу в разных географических областях путем изменения мощности имитационных



а *б*

Рис. 2. Имитатор сигналов GNSS от ЮНИТЕСС (UNITESS GNSS GENERATOR): *а* – в стационарном исполнении; *б* – в переносном исполнении

сигналов, а также тестировать компоненты системы.

Кроме того, имитатор обеспечивает возможность испытаний приемников спутниковой навигации в составе системы экстренного реагирования ЭРА-ГЛОНАСС, что позволяет проверить их соответствие требованиям ГОСТ 55534.

Технические особенности UNITESS GNSS GENERATOR

Имитатор сигналов оснащен 24 каналами, каждый из которых формирует полный навигационный радиосигнал одного навигационного космического аппарата (НКА) в своем частотном диапазоне. Устройство суммирует сигналы со всех каналов для создания комплексного навигационного сигнала на выходе.

Синхронизация работы всех узлов блока имитации осуществляется с помощью встроенного опорного генератора, который также поддерживает синхронизацию от реальных сигналов СНС GPS с частотой 10 МГц. Все каналы имитации синхронизируются по импульсу 1 PPS (Pulse Per Second).

Имитатор управляется операционной системой Windows 10 и программным обеспечением UNITESS GNSS GENERATOR, что гарантирует высокую точность и надежность выполнения тестов.

Моделирование помех в имитаторе сигналов GNSS: расширенные возможности тестирования

Одной из ключевых особенностей имитатора сигналов GNSS от компании ЮНИТЕСС является возможность моделирования помех в одном или нескольких каналах. Эта функция позволяет проводить более глубокий анализ и тестирование навигационных систем в условиях, приближенных к реальным. Для использования этой функции требуется приобретение дополнительных лицензий:

- ЮГС1030 «Спуфинг GNSS» – лицензия на одновременную генерацию «настоящего» и «поддельного» сигналов на двух каналах имитации. Предназначена для лабораторных испытаний приемников на устойчивость к различным сценариям спуфинга. Требует наличия второго канала GNSS «ЮГС1030: 2-й GNSS-канал»;
- ЮГС1030 «Синхронный спуфинг GNSS» – лицензия на программную опцию синхронного спуфинга GPS. Позволяет проводить испытания на устойчивость к спуфингу в реальных (полевых) условиях. Генерирует поддельный сигнал, полностью идентичный настоящему, с возможностью последующего «увода» (искажения) координат или времени. Требует наличия аппаратной опции «ЮГС103: опорный GNSS-приемник»;
- ЮГС1030 «Библиотека GNSS-помех» – лицензия на библиотеку помех GNSS. Содержит адаптированные/квазиоптимальные помехи для спутниковых систем ГЛОНАСС, GPS, Beidou, Galileo. Поддерживает все диапазоны L1, L2, L5. Требует наличия хотя бы одного аппаратного канала «ЮГС1030: канал генерации помех»;
- ЮГС1030 «Расширенная библиотека помех» – лицензия на расширенную библиотеку помех для сетей связи 2G, 3G, 4G, Wi-Fi, Bluetooth, каналов управления, телеметрии и передачи видео для дронов. Требует наличия хотя бы одного аппаратного канала «ЮГС1030: канал генерации помех».

Тестирование приемников с помощью имитатора сигналов GNSS на устойчивость к спуфингу и джаммингу обеспечивает надежную защиту и гарантирует корректную работу GNSS-приемников даже в условиях потенциальных атак со стороны злоумышленников. Наличие полного комплекта программного обеспечения, а также опционального СВЧ-тракта для подключения навигационных приемников позволяет быстро и экономично создать полноценное автоматизированное рабочее место для испытаний и поверки.

Для производителей устройств и систем, зависящих от GNSS, своевременная реакция на возникающие угрозы – обязательное условие для снижения рисков и повышения надежности продуктов. ЮНИТЕСС предлагает консультации по всем аспектам защиты: от выявления и тестирования уязвимостей до комплексного устранения рисков. Специалисты компании помогут вам обеспечить безопасность и устойчивость ваших решений.

Компания ЮНИТЕСС, г. Москва,
тел.: +7 (495) 975-7283,
e-mail: sales@unitess.ru,
сайт: www.unitess.ru