



ВИДЫ НАВИГАЦИОННЫХ ИМИТИРУЮЩИХ ПОМЕХ И МЕТОДЫ БОРЬБЫ С НИМИ

Проведен анализ влияния преднамеренных помех на сигналы глобальных навигационных спутниковых систем (ГНСС), принимаемых навигационной аппаратурой потребителя (НАП). Кратко рассмотрено воздействие маскирующих помех и способы повышения помехоустойчивости НАП. Дается описание типов имитирующих помех и приводится расширенное описание технологий их постановки. Выполнена классификация спуфинг-атак. Рассмотрены методы обнаружения имитирующих помех на основе временного и пространственного анализа принимаемого сигнала. Описаны методы противодействия имитирующим помехам и выполнено сравнение их эффективности в борьбе с спуфинг-атаками.

Ключевые слова: глобальная навигационная спутниковая система, маскирующие помехи, имитирующие помехи, спуфинг.

Berdiugin-Malinovskiy D. A., Shabunin S. N.

TYPES OF NAVIGATION SIMULATION INTERFERENCE AND METHODS OF DEALING WITH THEM

The analysis of the impact of intentional interference on the signals from global navigation satellite systems as received by consumer navigation equipment is conducted. The effects of masking interference and methods to enhance noise immunity are briefly discussed. A description of the types of simulated interference is provided, along with an extended overview of the technologies used to create them. Classification of spoofing attacks has also been performed. Techniques for detecting simulated interference based on the temporal and spatial characteristics of the received signal are explored. Methods to counter imitating interference are outlined, and their efficacy in combating spoofing assaults is compared.

Keywords: Global Navigation Satellite Systems, jamming, deception jamming, spoofing.

Введение

Свое развитие ГНСС начали с Глобальной системы позиционирования (GPS), созданной в США, и Глобальной навигационной спутниковой системы (ГЛОНАСС), разработанной в Советском Союзе. Современная ГНСС так же включает в себя такие системы, как Galileo – Европейский союз, BeiDou – Китайская народная республика, а также региональные навигационные спутниковые системы: индийская региональная навигационная спутниковая система (IRNSS) и квазизенитная спутниковая система (QZSS) в Японии [1]. НАП ГНСС широко востребована по всему миру, предоставляя точные данные о местоположении, скорости и времени.

Услуги предоставления ГНСС открытых высокоточных синхронизированных данных о времени нашли применение и стали незаменимы в отраслях, не связанных с навигацией, таких как энергетика, банковское дело, коммуникации. Это делает актуальным анализ уязвимостей ГНСС, связанных с помехоустойчивостью из-за крайне низкого уровня сигнала, получаемого со спутников, расположенных на высоте приблизительно в 20 000 километров, открытой структуры общедоступных гражданских навигационных сигналов (НС), используемых в навигации, которые легко подделать ложными с помощью технологии, известной как спуфинг (spoofing) [2].

При изучении уязвимости ГНСС, кроме возможных естественных помех, исследователи выделяют два основных типа преднамеренных помех НАП: маскирующие помехи (jamming) [3] и имитирующие помехи (спуфинг) [4]. Отношение мощности НС на входе приемного устройства к уровню шума обычно не превышает 30 дБ в полосе пропускания приемника. Так для ГНСС ГЛОНАСС в диапазоне L1 уровень сигнала на входе приемника может составлять – 161 дБВт, а для ГНСС GPS – 166 дБВт [1]. Для внесения помех и потери работоспособности НАП GPS достаточно передатчика с мощностью 0,25 Вт на удалении 4 км [5]. Постановщики помех (ПП) используют передатчики с широкополосным гауссовским шумом [6] или другие формы сигналов [7] на частотах работы ГНСС для снижения отношения сигнал/шум на входе приемника или полного подавления работы НАП.

Для повышения помехоустойчивости от маскирующих помех используются методы пространственной режекции сигналов помехи. Адаптивное формирование диаграммы

направленности с помощью комбинации нескольких антенн [8] или антенной решеткой (АР) осуществляется за счет подстройки фаз сигналов [9], получаемых с антенных элементов, для достижения максимального отношения сигнал / (помеха + шум) на входе приемника НС [10]. Применение цифровых антенных решеток позволяет подавить уровень множественных помех на 90–100 дБ [5]. Таким образом, методы борьбы с разными видами маскирующих помех НС ГНСС достаточно глубоко исследованы [11] и далее не рассматриваются. Основной целью работы является раскрытие и описание наиболее значимой проблемы – имитирующих помех НС.

Имитирующие помехи (спуфинг) НС ГНСС

Спуфинг НС ГНСС классифицируется как преднамеренная передача ложных НС с задачей дезинформировать НАП с целью получения ею неверных данных о положении, скорости и времени [12]. В отличие от помехи глушения цель атаки тайно заставить приемник НС отслеживать ложные сигналы ГНСС для предоставления неверного навигационного решения и получения контроля над ней. Воздействие имитирующей помехи на НАП намного опаснее маскирующей [13].

Термин «спуфинг» (имитирующая помеха) был заимствован из области информационной безопасности [12]. В области информационной безопасности целью атаки спуфинга является получение разведанных с помощью человека или программы путем маскировки под вид другого человека или программы с помощью фальсификации данных [14]. Имитирующие помехи НС ГНСС имеют сходство с информационными спуфинг-помехами, однако воздействие помехи на НАП не является главной целью. ПП рассчитывает получить полный контроль над объектом с помощью атаки. Цель ошибочно думает, что это настоящий сигнал и использует его. Чтобы добиться своего результата ПП используют различные стратегии и технологии.

Технологии имитирующих помех

При приеме навигационных сигналов со значительного удаления, возникают искажения, связанные с прохождением атмосферы, влияющие на прием [15]. Принимаемый НАП уровень НС настолько низкий, что уязвим для любого вида преднамеренных и непреднамеренных радиочастотных помех [16]. Чтобы на-

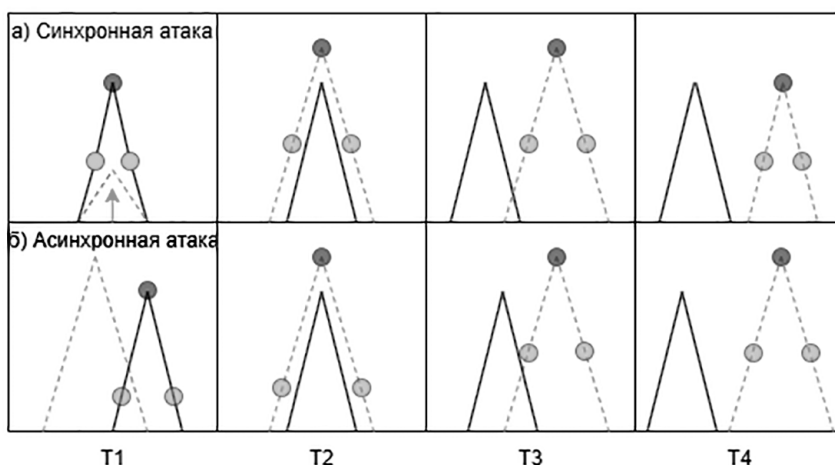


Рис. 1. Синхронная атака спунфинга (а), асинхронная атака (б) с этапами:

T1 – Выравнивание фазы спунфинг-сигнала с реальным сигналом,
T2 – Захват контроля над НАП с повышением мощности, T3 – Изменение параметров сигнала (фазы),
T4 – Контроль ПП над НАП

чать атаку, ПП сначала передает синхронизированные по фазе ложные НС, но более низкой мощности по сравнению с подлинными. На следующем этапе мощность спунфинг-сигналов увеличивается до уровня, незначительно превышающего подлинный [17]. С увеличением мощности НАП начинает отслеживать ложный сигнал вместо подлинного, получая таким образом контроль над НАП. ПП медленно изменяет параметры сигнала, уводя их от исходных. Как только ложные сигналы перемещают приемник на 2 микросекунды во времени или на 600 метров в сторону от подлинного навигационного решения, можно констатировать, что НАП подчинена ПП [18]. Описанная технология постановки имитирующих помех называется синхронной атакой (или мягкий захват), в противном случае это будет асинхронная атака [19] (или грубый захват) как показано на рис. 1.

Для синхронной атаки требуется точная синхронизация помеховых сигналов по фазе, доплеровскому сдвигу, положению и времени. Сигналы должны содержать соответствующие данные альманаха и эфемерид. Для обеспечения точности синхронизации постановщику помех необходим приемник ГНСС.

Несинхронная атака является одной из самых простых. Для нее не требуется синхронизация. Для успешной атаки уровень сигнала помехи должен превышать подлинный сигнал не менее, чем на 30 дБ. Во время атаки проис-

ходит срыв слежения за НС, после чего НАП переходит в режим поиска и захватывает более мощный спунфинг-сигнал. В случае, когда НАП находится в режиме поиска НС, для проведения атаки помеховому сигналу достаточно небольшой разницы в мощности [20].

Постановка помехи на основе генерации НС

Такие сигналы генерируются самим оборудованием ПП для передачи на НАП ложных данных [21]. Сгенерированные сигналы имеют хорошую гибкость в плане изменения навигационных параметров о местоположении и времени. В основном такие атаки выполняются после предварительного глушения сигналов ГНСС, чтобы заставить НАП захватить ложный сигнал, превышающий мощность подлинных сигналов.

Постановка помехи на основе ретрансляции НС

Источник помех на основе ретрансляции НС состоит из ретранслятора и приемника НС. Перед ретрансляцией сигналы синхронизируются с подлинными, после этого генерируются спунфинг-сигналы, усиленные по мощности относительно подлинных сигналов и с небольшой задержкой во времени, направленные на приемную антенну цели. Атаки на небольшом расстоянии от целевой НАП наиболее синхронизированы с подлинными НС [22].

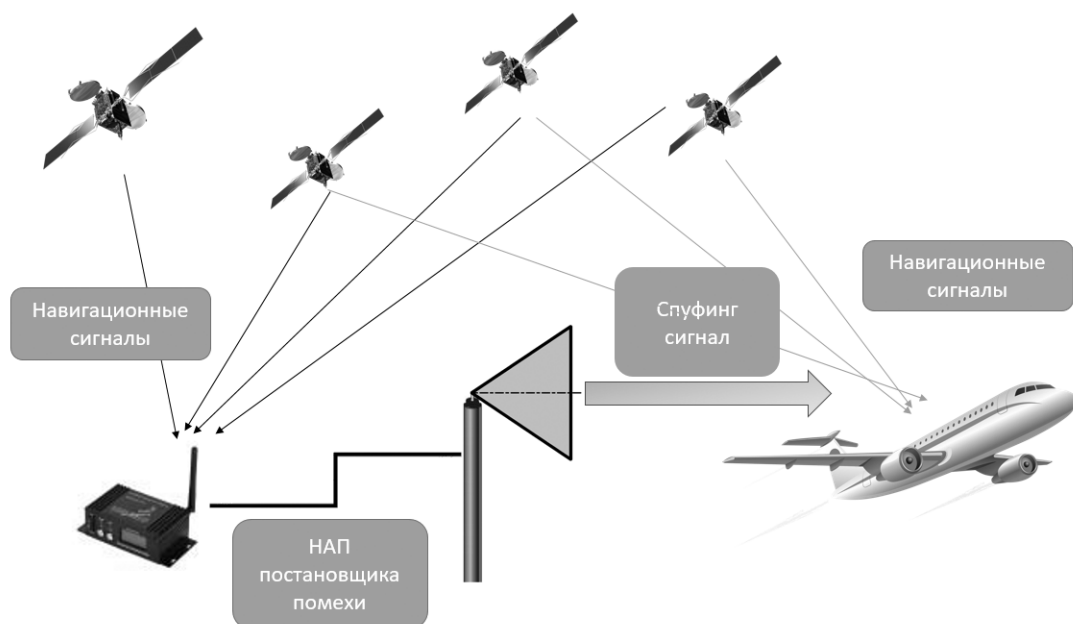


Рис. 2. Схема синхронной спуфинг-атаки на основе ретрансляции НС

На рис. 2 показана базовая схема синхронной атаки на основе ретрансляции НС.

Постановка помехи с автосинхронизацией

Как наиболее продвинутая исследователями рассматривается технология скрытной постановки имитирующей помехи с постепенной синхронизацией к подлинным НС, подстраиваемой под контур слежения НАП [23]. После обработки подлинных НС, ПП осуществляет задержку по дальности и доплеровскому сдвигу в соответствии с динамикой объекта атаки, с целью скрытного контроля задержки приема НС [24]. Особенность технологии автосинхронизации помехи заключается в эффективной скрытной подмене подлинного НС. Для общедоступных гражданских и военных НС технология постановки помех отличается [25].

Постановка помехи с использованием нескольких передатчиков

Атака с несколькими передатчиками считается наиболее сложной помехой с технологической точки зрения. На рис. 3 изображена схема атаки на основе ретрансляции НС с несколькими источниками помех. В этой технологии используется несколько передатчиков, что значительно усложняет пространственную оценку прихода сигналов для подавле-

ния таких помех [26]. Как при генерации, так и при ретрансляции НС, работа источников помех должна быть синхронизирована, что делает её сложно реализуемой [27].

Выбор технологии постановки имитирующих помех зависит от целей ПП [28], их можно разделить на несколько категорий:

- подмена информации в определении местоположения цели [29];
- подмена информации текущего времени цели [30];
- получение контроля над НАП ГНСС [31].

По отличительным признакам описанных методов и технологий, имитирующие помехи можно классифицировать в виде отдельных групп (рис. 4).

Методы детектирования имитирующих помех

Большая работа по детектированию имитирующих помех была проведена еще в 1995 году [32]. Были проанализированы технологии постановки помех, а также сформулированы методы их обнаружения:

- по амплитуде сигнала;
- по углу прихода сигнала;
- по времени прибытия сигнала;
- проверка согласованности с другим навигационным оборудованием;
- аутентификация шифрования сигнала;

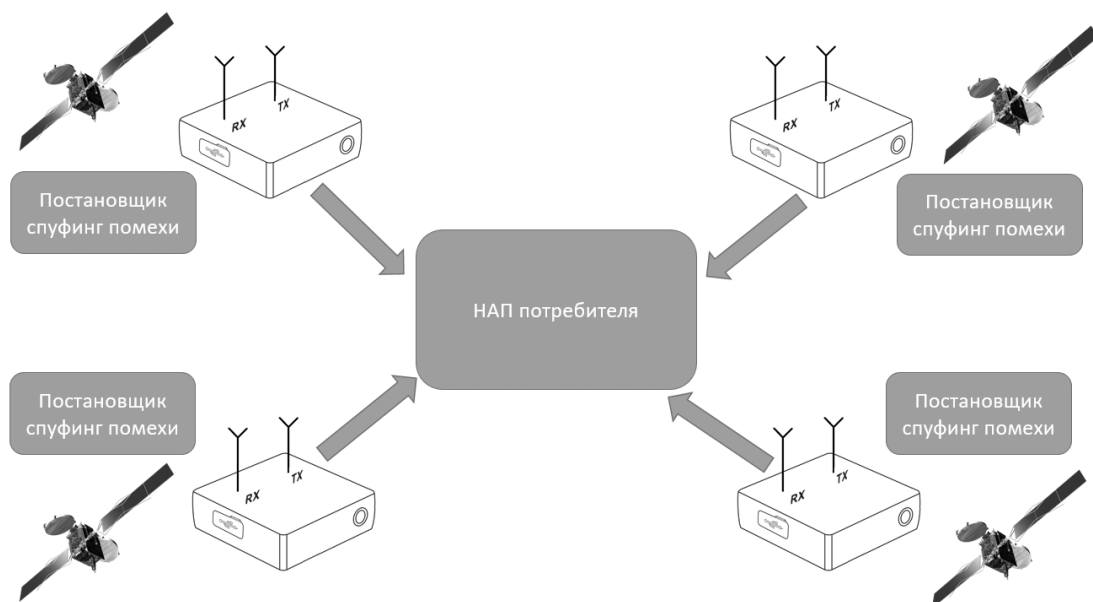


Рис. 3. Схема синхронизированной спуфинг-атаки на основе ретрансляции с несколькими источниками помех

- определение направления поляризации сигнала;
- обнаружение векторных петель слежения.

Анализ амплитуды принимаемого НС

Отношение мощности полезного сигнала к мощности шума является одной из характеристик навигационного сигнала. В нормальных условиях работы НАП это отношение находится в определенных пределах и не подвержено значительным изменениям [33]. Когда с помощью атаки ПП пытается воздействовать на НАП, это отношение может резко измениться. Контролируя данный параметр НС,

можно определить воздействие спуфинга. Аналогичным способом можно оценивать уровень мощности самого принимаемого НС. Еще одним методом, основанном на анализе уровня принимаемых НС, служит оценка разности мощности принимаемых сигналов разных диапазонов частот с одного спутника. Изменение разности или потеря одного из сигналов, может свидетельствовать об атаке [34].

Пространственная оценка НС

Подлинные сигналы передаются с разных спутников и направлений. Если спуфинг-атака совершается с одного передатчика, то такие сигналы приходят с одной антенны. Тем

Тип помехового сигнала		
сгенерированный сигнал	ретранслированный сигнал с задержками	автосинхронизированный помеховый сигнал
Стратегия атаки		
несинхронная атака	синхронная атака	
Цель атаки		
ложная информация о местоположении цели	ложная информация о времени	контроль над целью
Структура атаки		
одионый постановщик помех	несколько помеховых передатчиков	

Рис. 4. Классификация спуфинг-атак

самым, с помощью пространственной обработки сигналов можно выявлять направление источника помехи для управления ДН антенных систем НАП.

Способы пространственной обработки могут быть разными. За счет оценки разности фаз принимаемых сигналов [35], оценки изменения угла пересечения НС между двумя направлениями прибытия на одной антенне [36], разности фаз от двух разнесенных антенн [37], использования многоэлементной антенной решетки (АР), сравнения фазовых измерений коррелятора НАП от разных спутников, определения угла прибытия сигналов и исключения тех, которые были получены из одной пространственной области [38].

Методы, основанные на оценке параметров времени задержки прибытия НС

Для случаев, когда имитирующие помехи используют в своей основе навигационный приемник, необходимо время для получения НС, его обработки и генерации на его основе помехи. Методы по оценке времени задержки могут отличаться. К примеру, алгоритм обнаружения имитирующих помех, основанный на анализе разницы псевдодальности и данных эфемерид [39], метод оценки разницы во времени прибытия (TDOA), измеряемой как дифференциальное отношение псевдодальности к несущей частоте между сигналами имитирующих помех и подлинными НС с помощью корреляции данных с нескольких навигационных приемников [40].

Распознавание спуфинга с использованием инерциальных навигационных систем (ИНС)

Корреляция данных НАП и датчиков ИНС позволяет в различной степени и на разных этапах настраивать и применять методы обнаружения имитирующих помех, даже для медленных атак спуфинга, когда ПП пытается подстраиваться под подлинных НС [41].

Мониторинг качества сигнала

Метод основан на мониторинге качества пика корреляции в условиях многолучевости. НАП на выходе коррелятора подвергается аналогичному воздействию от атак спуфинга, поэтому данный метод может применяться для детектирования имитирующих помех [42]. Эффективность метода снижается в условиях многолучевости.

Методы противодействия имитирующим помехам

Еще в 1994 году проведена оценка использования инерциальной навигационной системы на основе высокоточного кольцевого лазерного гироскопа и акселерометра, позволяющей корректировать курс при отказе или подмене данных со спутников [43]. Интеграция навигационных данных, инерциальной системы и одометрии на основе разработанного алгоритма фильтра Калмана позволяет отфильтровать резкие изменения местоположения и осуществлять кратковременную навигацию без НС ГНСС под воздействием на НАП имитирующих помех. Здесь дрейф инерциальной системы, накапливающийся из-за ошибок в измерениях, ограничивается калибровкой при запуске, и непрерывной оценкой погрешности изменяющихся данных с помощью фильтра Калмана [44]. Использование услуги высокоточного позиционирования для ГНСС GPS с использованием широкополосного сигнала, модулированного дальномерным P(Y) кодом, делает его значительно менее уязвимым к имитирующим помехам по сравнению с открытым кодом C/A (Coarse/Acquisition – грубый прием), но его применение ограничено санкционированными пользователями [45]. Тем не менее, использование даже полубескодowych приемников (semi-codeless receiver), использующих косвенные методы обработки НС с P(Y) в сочетании с ИНС, снижает влияние имитирующих помех по сравнению с C/A [46]. Применение метода двумерного поиска по задержке кода НС и доплеровского сдвига с использованием асимметричного быстрого преобразования Фурье позволяет быстрее определять сдвиг и задержку в условиях слабого сигнала и помех и с меньшими вычислительными затратами, тем самым снижая уязвимость к примитивным имитирующим помехам, направленным на срыв синхронизации [47]. В борьбе с несложными некогерентными спуфинг-атаками при подмене НС хорошо зарекомендовали себя методы использования референсных станций ДНС, вычисляющие поправки и передающие их другим НАП по каналам связи, защищенным от спуфинг-сигналов [48]. Более высокоточной, чем дифференциальная, является технология RTK (Real Time Kinematic). Метод использует гибридную систему, состоящую из НС улучшенной целостности с технологией RTK. Данные устройств ИНС и относитель-

ной навигации на основе ультразвуковых и оптических датчиков позволяют проводить перекрестную проверку навигационных данных для выявления и возможной фильтрации спуфинг-сигналов [49]. Для гражданской НАП, не имеющей доступа к широкополосным защищённым военным сигналам, надёжными методами борьбы с имитирующими помехами являются методы пространственной обработки сигнала, использующие пространственную фильтрацию для адаптивного формирования нулей диаграммы направленности АР в направлении источников помех [50]. Уровень помехоустойчивости при применении многодиапазонных гибридных антенн сопоставим с применением более громоздких многоэлементных АР [33]. Применение АР эффективно при обработке сложной навигационной помеховой обстановки.

В контексте обзора методов противодействия имитирующим помехам нужно рассмотреть перспективные системы навигации для воздушных судов по физическим полям: магнитного и гравитационного поля Земли [51]. Существуют методы использования оптической навигации, позволяющие корректировать навигационное решение или осуществлять независимую навигацию по видео изображению [52]. Для навигации морских судов предлагается метод корреляции измерений глубины рельефа бортовыми эхолотами с цифровыми батиметрическими картами в сочетании с ИНС [53].

Инженерный университет в городе Харбин в 2022 году провел большое исследование на тему обзора технологий имитирующих помех и методов борьбы с ними [4]. В работе были объединены труды 121 научного исследования и на их основе сформированы оценочные выводы об эффективности рассмо-

тренных методов. Наивысшие оценки получили следующие методы:

- методы оценки мощности и векторных контуров слежения принимаемых НС;
- оценка отклонений от нормы параметров в принимаемых НС в сочетании с использованием инструментов криптозащиты и шифрования;
- анализ дрейфа параметров НС, где наивысшую оценку получили методы, сочетающие в себе корреляцию оцениваемых параметров с инерциальными датчиками ориентации или оптическими датчиками;
- определение местоположения источников излучения принимаемых сигналов;
- использование нейронных сетей и других методов машинного обучения, позволяющих комбинировать различные методы защиты в зависимости от стратегии атаки.

Заключение

Несмотря на развитие технологий и методов борьбы с имитирующими помехами, технологии спуфинга НС ГНСС на основе генерации НС или использующие подлинные НС все меньше отличаются от реальных НС. Исходя из этого, приоритеты развития методов обнаружения и борьбы с имитирующими помехами будут смещаться к комбинации интегрированных НАП, ИНС и методов машинного обучения в различных сочетаниях.

Для гражданской НАП эффективным и недорогим методом борьбы с помехами является применение адаптивных антенных систем или АР. При разработке адаптивных навигационных антенных систем для борьбы с помехами, в дополнение к методам пространственной оценки источников сигналов, повысить эффективность поможет оценка дрейфа параметров НС в сочетании с инерциальными датчиками или полноценной ИНС.

Работа выполнена при финансовой поддержке Министерства науки и высшего образования РФ (тема № FEUZ-2023-0015)

Литература

1. Карутин С.Н., Власов И.Б., Дворкин В.В. Дифференциальная коррекция и мониторинг глобальных навигационных спутниковых систем. 2014. 463 с.
2. Warner J.S., Johnston R.G., and Alamos C.L. A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing. The Journal of Security Administration, 2002, vol. 25, no. 10, pp. 19–28.
3. Перов А.И. ГЛОНАСС. Модернизация и перспективы развития. Монография. М: Радиотехника, 2020. 1072 с.
4. Meng L. et al. A Survey of GNSS Spoofing and Anti-Spoofing Technology. Remote Sensing, 2022, vol. 14, no. 19, p. 4826.
5. Слюсар В. Цифровые антенные решетки – будущее радиолокации. Электроника: Наука, технология, бизнес, 2001, № 3(33), с. 42–47.
6. Lubbers B. GNSS Accuracy Under White Gaussian Noise Jamming. Engineering Proceedings, 2025, vol. 88, no. 1, p. 26.
7. Elghamrawy H. et al. Experimental Evaluation of the Impact of Different Types of Jamming Signals on Commercial GNSS Receivers. Applied Sciences, 2020, vol. 10, no. 12, p. 4240.
8. Ruegamer A. et al. Jamming and Spoofing of GNSS Signals – An Underestimated Risk?! Proc. Wisdom Ages Challenges Modern World, 2015, vol. 3, pp. 17–21.
9. Кашин В.А. Методы фазового синтеза антенных решеток. Зарубежная радиоэлектроника. Успехи современной радиоэлектроники, 1997, № 1, с. 47–60.
10. Монзинго Р.А., Миллер Т.У. Адаптивные антенные решетки: введение в теорию; пер. с англ. В.Г. Челпанова, В.А. Лексаченко; под общ. ред. В.А. Лексаченко. М.: Радио и связь, 1986, 448 с.
11. Sharifi-Tehrani O., Ghasemi M.H. A Review on GNSS-Threat Detection and Mitigation Techniques. Cloud Computing and Data Science, 2023, pp. 161–185.
12. Broumandan A., Jafarnia-Jahromi A., Lachapelle G. Spoofing Detection, Classification and Cancellation (SDCC) Receiver Architecture for a Moving GNSS Receiver. GPS Solutions, 2015, vol. 19, pp. 475–487.
13. Tippenhauer N. O. et al. On the Requirements for Successful GPS Spoofing Attacks. Proceedings of the 18th ACM Conference on Computer and Communications Security, 2011, pp. 75–86.
14. Psiaki M. L. et al. GNSS lies, GNSS truth: Spoofing Detection with Two-Antenna Differential Carrier Phase. GPS World, 2014, vol. 25, no. 11, pp. 36–44.
15. Glomsvoll O. Jamming of GPS & GLONASS signals. Department of Civil Engineering, Nottingham Geospatial Institute, 2014, pp. 25–32.
16. Borio D. et al. Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers. Proceedings of the IEEE, 2016, vol. 104, no. 6, pp. 1233–1245.
17. Jafarnia-Jahromi A. et al. Detection and Mitigation of Spoofing Attacks on a Vector Based Tracking GPS Receiver. Proceedings of the 2012 International Technical Meeting of the Institute of Navigation, 2012, pp. 790–800.
18. Kyle W., Daniel S., Todd H. Straight Talk on Anti-Spoofing Securing the Future of PNT. GPS World, 2012, vol. 23, pp. 32–43.
19. Ouyang X. et al. Analysis and Evaluation of Spoofing Effect on GNSS Receiver. 2015 IEEE 12th Intl Conf. on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf. on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf. on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom). IEEE, 2015, pp. 1388–1392.
20. Aissou G. et al. Instance-Based Supervised Machine Learning Models for Detecting GPS Spoofing Attacks on UAS. 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2022, pp. 0208–0214.
21. Caparra G., Wullems C., Ioannides R.T. An Autonomous Gns Anti-Spoofing Technique. 2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC). IEEE, 2016, pp. 1–8.
22. Ledvina B.M. et al. An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers. Proceedings of the 2010 International Technical Meeting of the Institute of Navigation, 2010, pp. 698–712.
23. Wesson K., Shepard D., Humphreys T. Straight Talk on Anti-Spoofing. GPS World, 2012, vol. 23, no. 1, pp. 32–39.
24. Humphreys T.E. Detection Strategy for Cryptographic GNSS Anti-Spoofing. IEEE Transactions on Aerospace and Electronic Systems, 2013, vol. 49, no. 2, pp. 1073–1090.

25. Peng C. et al. Research of Intermediate Spoofing without Precise Target Information. China Satellite Navigation Conference (CSNC) 2019 Proceedings: Volume II. Springer Singapore, 2019. pp. 615–624.
26. Manfredini E.G. Signal Processing Techniques for GNSS Anti-Spoofing Algorithms. Polytechnic University of Turin, Italy, 2017.
27. Psiaki M.L., Humphreys T.E. GNSS Spoofing and Detection. Proceedings of the IEEE, 2016, vol. 104, no. 6, pp. 1258–1270.
28. Неровный В.В. и др. Характеристики уязвимости аппаратуры потребителей глобальных навигационных спутниковых систем к спуфинг-атакам. Труды учебных заведений связи, 2023, т. 9, № 6, с. 95–100.
29. Zen K. C. et al. A Practical GPS Location Spoofing Attack in Road Navigation Scenario. Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications, 2017, pp. 85–90.
30. Khan I., Centeno V. Undetectable GPS-Spoofing Attack on Time Series Phasor Measurement Unit Data, arXiv preprint arXiv:2206.12440, 2022.
31. Zaragoza S., Zumalt E. Spoofing a Superyacht at Sea. Cockrell School of Engineering. Univ. of Texas/Austin, 2013, available at <http://www.utexas.edu/know/2013/07/30/spoofing-asuperyacht-at-sea>.
32. Key E.L. Techniques to Counter GPS Spoofing. Internal Memorandum. MITRE Corporation, Bedford, 1995.
33. Криницкий Г.В. Повышение помехоустойчивости навигационной аппаратуры потребителей с использованием различных конфигураций антенных систем. Радиотехника, 2022, т. 86, № 9, с. 31–39.
34. Jafarnia-Jahromi A. et al. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. International Journal of Navigation and Observation, 2012, vol. 2012, no. 1, pp. 127072.
35. Montgomery P.Y., Humphreys T.E., Ledvina B.M. Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-Antenna Receiver Defense against a Portable Civil GPS Spoofer. Proceedings of the 2009 International Technical Meeting of the Institute of Navigation, 2009, pp. 124–130.
36. Chen S. et al. GNSS Spoofing Detection via the Intersection Angle between Two Directions of Arrival in a Single Rotating Antenna. Sensors, 2024, vol. 24, no. 4, p. 1116.
37. Dinh T.N. et al. A Method to Build Feature Descriptor for GNSS Spoofing Detection by Carrier Phase Double Difference Measurement. Measurement Science and Technology, 2024, vol. 35, no. 6, p. 066307.
38. McDowell C. E. GPS Spoofer and Repeater Mitigation System Using Digital Spatial Nulling: pat. № 7250903, USA, 2007.
39. Liu K. et al. Spoofing Detection Algorithm Based on Pseudorange Differences. Sensors, 2018, vol. 18, no. 10, p. 3197.
40. Zhang Z., Zhan X. GNSS Spoofing Network Monitoring Based on Differential Pseudorange. Sensors, 2016, vol. 16, no. 10, p. 1771.
41. Gao Y., Li G. A Slowly Varying Spoofing Algorithm on Loosely Coupled GNSS/IMU Avoiding Multiple Anti-Spoofing Techniques. Sensors, 2022, vol. 22, no. 12, pp. 4503.
42. Pini M. et al. Signal Quality Monitoring Applied to Spoofing Detection. Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011), 2011, pp. 1888–1896.
43. Gilster G. High Accuracy Performance Capabilities of the Military Standard Ring Laser Gyro Inertial Navigation Unit. Proceedings of 1994 IEEE Position, Location and Navigation Symposium-PLANS'94. IEEE, 1994, pp. 464–473.
44. Beckmann H., Niedermeier H., Eissfeller B. Improving GNSS Road Navigation Integrity Using MEMS INS and Odometry. 2012 6th ESA Workshop on Satellite Navigation Technologies (Navitec 2012) & European Workshop on GNSS Signals and Signal Processing. IEEE, 2012, pp. 1–7.
45. Wolfert R. et al. Direct P (Y)-Code Acquisition Under a Jamming Environment. IEEE 1998 Position Location and Navigation Symposium (Cat. No. 98CH36153). IEEE, 1996, pp. 228–235.
46. Tang X., Yuan M., Wang F. Analysis of GPS P(Y) Signal Power Enhancement Based on the Observations with a Semi-Codeless Receiver. Satellite Navigation, 2022, vol. 3, no. 1, p. 26.
47. Lu H. et al. Two Dimension Direct GPS Signal Acquisition Based on Unsymmetrical FFT. 2009 4th IEEE Conference on Industrial Electronics and Applications. IEEE, 2009, pp. 1769–1772.
48. Jin M. H. et al. GPS Spoofing Signal Detection and Compensation Method in DGPS Reference Station. 2011 11th International Conference on Control, Automation and Systems. IEEE, 2011, pp. 1616–1619.
49. Brewer E. et al. A Low SWaP Implementation of High Integrity Relative Navigation for Small UAS. 2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014. IEEE, 2014, pp. 1183–1187.

50. Magiera J., Katulski R. Applicability of Null-Steering for Spoofing Mitigation in Civilian GPS. 2014 IEEE 79th Vehicular Technology Conference (VTC Spring). IEEE, 2014, pp. 1–5.
51. Каршаков Е.В. и др. Перспективные системы навигации летательных аппаратов с использованием измерений потенциальных физических полей. Гирскопия и навигация, 2021, Т. 29, №. 1, с. 112.
52. Веселов Г.Е. и др. Разработка и испытания навигационной системы на основе оптического потока для беспилотных транспортных средств. 2024 IEEE 3-я Международная конференция по проблемам информатики, электроники и радиотехники (PIERE). IEEE, 2024, с. 90–95.
53. Hagen O.K., Ånonsen K.B., Skaugen A. Robust Surface Vessel Navigation Using Terrain Navigation. 2013 MTS/IEEE OCEANS-Bergen. IEEE, 2013, pp. 1–7.

References

1. Karutin S.N., Vlasov I.B., Dvorkin V.V. Differential Correction and Monitoring of Global Navigation Satellite Systems [Differencial'naja korekciya i monitoring global'nyh navigacionnyh sputnikovyh system], 2014, 463 p.
2. Warner J.S., Johnston R.G., and Alamos C.L. A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing. The Journal of Security Administration, 2002, vol. 25, no. 10, pp. 19–28.
3. Perov A.I. GLONASS. Modernization and Development Prospects Monograph. [Modernizacija i perspektivy razvitiya. Monografija]. Moscow, Radio Engineering, 2020, 1072 p.
4. Meng L. et al. A Survey of GNSS Spoofing and Anti-Spoofing Technology. Remote Sensing, 2022, vol. 14, no. 19, p. 4826.
5. Slyusar V. Digital Antenna Arrays – the Future of Radar [Cifrovye antennye reshetki – budushhee radiolokacii]. Electronics: Science, Technology, Business, 2001, no. 3, pp. 42–47.
6. Lubbers B. GNSS Accuracy Under White Gaussian Noise Jamming. Engineering Proceedings, 2025, vol. 88, no. 1, p. 26.
7. Elghamrawy H. et al. Experimental Evaluation of the Impact of Different Types of Jamming Signals on Commercial GNSS Receivers. Applied Sciences, 2020, vol. 10, no. 12, p. 4240.
8. Ruegamer A. et al. Jamming and Spoofing of GNSS Signals – An Underestimated Risk?! Proc. Wisdom Ages Challenges Modern World. 2015, vol. 3, pp. 17-21.
9. Kashin V.A. Methods of phase synthesis of antenna arrays [Metody fazovogo sinteza antennykh reshetok]. Foreign radioelectronics. Successes Modern Radioelectronics [Zarubezhnaya radioelektronika. Uspеhi sovremennoy radioelektroniki], 1997, vol. 1, pp. 47–60.
10. Monzingo R.A., Miller T.W. Adaptive Antenna Arrays: Introduction to the Theory [Adaptivnye antennye reshetki: vvedenie v teoriyu]; translated from English by V. G. Chelpanova, V. A. Leksachenko; edited by V. A. Leksachenko. Moscow: Radio i svyaz, 1986, 448 p.
11. Sharifi-Tehrani O., Ghasemi M.H. A Review on GNSS-Threat Detection and Mitigation Techniques. Cloud Computing and Data Science, 2023, pp. 161–185.
12. Broumandan A., Jafarnia-Jahromi A., Lachapelle G. Spoofing Detection, Classification and Cancellation (SDCC) Receiver Architecture for a Moving GNSS Receiver. GPS Solutions, 2015, vol. 19, pp. 475–487.
13. Tippenhauer N. O. et al. On the Requirements for Successful GPS Spoofing Attacks. Proceedings of the 18th ACM Conference on Computer and Communications Security, 2011, pp. 75–86.
14. Psiaki M. L. et al. GNSS Lies, GNSS Truth: Spoofing Detection with Two-Antenna Differential Carrier Phase. GPS World, 2014, vol. 25, no. 11, pp. 36–44.
15. Glomsvoll O. Jamming of GPS & GLONASS signals. Department of Civil Engineering, Nottingham Geospatial Institute, 2014, pp. 25–32.
16. Borio D. et al. Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers. Proceedings of the IEEE, 2016, vol. 104, no. 6, pp. 1233–1245.
17. Jafarnia-Jahromi A. et al. Detection and Mitigation of Spoofing Attacks on a Vector Based Tracking GPS Receiver. Proceedings of the 2012 International Technical Meeting of the Institute of Navigation, 2012, pp. 790–800.
18. Kyle W., Daniel S., Todd H. Straight Talk on Anti-Spoofing Securing the Future of PNT. GPS World, 2012, vol. 23, pp. 32–43.
19. Ouyang X. et al. Analysis and Evaluation of Spoofing Effect on GNSS Receiver. 2015 IEEE 12th Intl Conf. on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf. on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf. on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom). IEEE, 2015, pp. 1388–1392.

20. Aissou G. et al. Instance-Based Supervised Machine Learning Models for Detecting GPS Spoofing Attacks on UAS. 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2022, pp. 0208–0214.
21. Caparra G., Wullems C., Ioannides R.T. An Autonomous Gnss Anti-Spoofing Technique, 2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC). IEEE, 2016, pp. 1–8.
22. Ledvina B.M. et al. An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers. Proceedings of the 2010 International Technical Meeting of the Institute of Navigation, 2010, pp. 698–712.
23. Wesson K., Shepard D., Humphreys T. Straight Talk on Anti-Spoofing. GPS World, 2012, vol. 23, no. 1, pp. 32–39.
24. Humphreys T.E. Detection Strategy for Cryptographic GNSS Anti-Spoofing. IEEE Transactions on Aerospace and Electronic Systems, 2013, vol. 49, no. 2, pp. 1073–1090.
25. Peng C. et al. Research of Intermediate Spoofing without Precise Target Information. China Satellite Navigation Conference (CSNC) 2019 Proceedings: Volume II. Springer Singapore, 2019. pp. 615–624.
26. Manfredini E.G. Signal Processing Techniques for GNSS Anti-Spoofing Algorithms. Polytechnic University of Turin, Italy, 2017.
27. Psiaki M.L., Humphreys T.E. GNSS Spoofing and Detection. Proceedings of the IEEE, 2016, vol. 104, no. 6, pp. 1258–1270.
28. Nerovny V. V. et al. Characteristics of vulnerability of consumer equipment of global navigation satellite systems to spoofing attacks [Harakteristiki ujazvimosti apparatury potrebitelej global'nyh navigacionnyh sputnikovyh sistem k spufing-atakam]. Proceedings of educational institutions of communication [Trudy uchebnyh zavedenij svjazi], 2023, vol. 9, no. 6. pp. 95–100.
29. Zen K.C. et al. A Practical GPS Location Spoofing Attack in Road Navigation Scenario. Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications, 2017, pp. 85–90.
30. Khan I., Centeno V. Undetectable GPS-Spoofing Attack on Time Series Phasor Measurement Unit Data, arXiv preprint arXiv:2206.12440, 2022.
31. Zaragoza S., Zumalt E. Spoofing a Superyacht at Sea. Cockrell School of Engineering. Univ. of Texas/ Austin, 2013, available at <http://www.utexas.edu/known/2013/07/30/spoofing-asuperyacht-at-sea>.
32. Key E.L. Techniques to Counter GPS Spoofing. Internal Memorandum. MITRE Corporation, Bedford, 1995.
33. Krinitsky, G.V. Increasing the Noise Immunity of Consumer Navigation Equipment Using Various Configurations of Antenna Systems [Povyshenie pomehoustojchivosti navigacionnoj apparatury potrebitelej s ispol'zovaniem razlichnyh konfiguracij antennyh system]. Radio Engineering, 2022, vol. 86, no. 9, pp.31–39.
34. Jafarnia-Jahromi A. et al. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. International Journal of Navigation and Observation, 2012, vol. 2012, no. 1, pp. 127072.
35. Montgomery P.Y., Humphreys T.E., Ledvina B.M. Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-Antenna Receiver Defense against a Portable Civil GPS Spoofer. Proceedings of the 2009 International Technical Meeting of the Institute of Navigation, 2009, pp. 124–130.
36. Chen S. et al. GNSS Spoofing Detection via the Intersection Angle between Two Directions of Arrival in a Single Rotating Antenna. Sensors, 2024, vol. 24, no. 4, p. 1116.
37. Dinh T.N. et al. A Method to Build Feature Descriptor for GNSS Spoofing Detection by Carrier Phase Double Difference Measurement. Measurement Science and Technology, 2024, vol. 35, no. 6, p. 066307.
38. McDowell C. E. GPS Spoofer and Repeater Mitigation System Using Digital Spatial Nulling: pat. № 7250903, USA, 2007.
39. Liu K. et al. Spoofing Detection Algorithm Based on Pseudorange Differences. Sensors, 2018, vol. 18, no. 10, p. 3197.
40. Zhang Z., Zhan X. GNSS Spoofing Network Monitoring Based on Differential Pseudorange. Sensors, 2016, vol. 16, no. 10, p. 1771.
41. Gao Y., Li G. A Slowly Varying Spoofing Algorithm on Loosely Coupled GNSS/IMU Avoiding Multiple Anti-Spoofing Techniques. Sensors, 2022, vol. 22, no. 12, pp. 4503.
42. Pini M. et al. Signal Quality Monitoring Applied to Spoofing Detection. Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011), 2011, pp. 1888–1896.
43. Gilster G. High Accuracy Performance Capabilities of the Military Standard Ring Laser Gyro Inertial Navigation Unit. Proceedings of 1994 IEEE Position, Location and Navigation Symposium-PLANS'94. IEEE, 1994, pp. 464–473.

44. Beckmann H., Niedermeier H., Eissfeller B. Improving GNSS Road Navigation Integrity Using MEMS INS and Odometry. 2012 6th ESA Workshop on Satellite Navigation Technologies (Navitec 2012) & European Workshop on GNSS Signals and Signal Processing. IEEE, 2012, pp. 1–7.
45. Wolfert R. et al. Direct P (Y)-Code Acquisition Under a Jamming Environment. IEEE 1998 Position Location and Navigation Symposium (Cat. No. 98CH36153). IEEE, 1996, pp. 228–235.
46. Tang X., Yuan M., Wang F. Analysis of GPS P(Y) Signal Power Enhancement Based on the Observations with a Semi-Codeless Receiver. Satellite Navigation, 2022, vol. 3, no. 1, p. 26.
47. Lu H. et al. Two Dimension Direct GPS Signal Acquisition Based on Unsymmetrical FFT. 2009 4th IEEE Conference on Industrial Electronics and Applications. IEEE, 2009, pp. 1769–1772.
48. Jin M. H. et al. GPS Spoofing Signal Detection and Compensation Method in DGPS Reference Station. 2011 11th International Conference on Control, Automation and Systems. IEEE, 2011, pp. 1616–1619.
49. Brewer E. et al. A Low SWaP Implementation of High Integrity Relative Navigation for Small UAS. 2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014. IEEE, 2014, pp. 1183–1187.
50. Magiera J., Katulski R. Applicability of Null-Steering for Spoofing Mitigation in Civilian GPS. 2014 IEEE 79th Vehicular Technology Conference (VTC Spring). IEEE, 2014, pp. 1–5.
51. Karshakov E.V. et al. Promising aircraft navigation systems using measurements of potential physical fields [Perspektivnye sistemy navigatsii letatel'nyh apparatov s ispol'zovaniem izmerenij potencial'nyh fizicheskikh polej]. Gyroscopy and navigation, 2021, vol. 29, no. 1, pp. 112.
52. Veselov G.E. et al. Development and testing of an optical flow-based navigation system for unmanned vehicles [Razrabotka i ispytaniya navigacionnoj sistemy na osnove opticheskogo potoka dlja bespilotnyh transportnyh sredstv]. 2024 IEEE 3rd International Conference on Problems of Informatics, Electronics, and Radio Engineering (PIERE) [3-ja Mezhdunarodnaja konferencija po problemam informatiki, elektroniki i radiotekhniki]. IEEE, 2024, pp. 90–95.
53. Hagen O.K., Ånonsen K.B., Skaugen A. Robust Surface Vessel Navigation Using Terrain Navigation. 2013 MTS/IEEE OCEANS-Bergen. IEEE, 2013, pp. 1–7.

БЕРДЮГИН-МАЛИНОВСКИЙ Денис Александрович, студент магистратуры ФГАОУ ВО «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 32. E-mail: Berdiugin-Malinovs@urfu.me

ШАБУНИН Сергей Николаевич, доктор технических наук, профессор, заведующий кафедрой радиоэлектроники и телекоммуникаций ФГАОУ ВО «Уральский федеральный университет им. первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 32. E-mail: s.n.shabunin@urfu.ru

BERDYUGIN-MALINOVSKIY Denis Alexandrovich, master's student of the Federal State Autonomous Educational Institution of Higher Education «Ural Federal University named after the first President of Russia B.N. Yeltsin». 620002, Ekaterinburg, Mira st., 32. E-mail: Berdiugin-Malinovs@urfu.me

SHABUNIN Sergey Nikolaevich, Doctor of Technical Sciences, Professor, Head of the Department of Radioelectronics and Telecommunications, Ural Federal University named after the first President of Russia B.N. Yeltsin. 620002, Ekaterinburg, Mira st., 32. E-mail: s.n.shabunin@urfu.ru