Актуальность работы

А к т у а л ь н о с т ь р а б о т ы. В современном мире системы ГНСС активно внедряются в глобальную инфраструктуру и используются в различных отраслях экономики. Первоначальный энтузиазм в отношении спутниковой навигации, технологии ГНСС и в качестве координатно-временной информации (КВИ) постепенно уступает место более рациональному отношению к возможностям, предоставляемым ГНСС. В основном это связано с не безупречностью ГНСС к случайным и преднамеренным помехам: уязвимость приемников ГНСС для конечных пользователей давно признана, но редко учитывалась производителями приемников и пользователями.

Объект и предмет исследования

Объект	• спутниковые системы геопозиционирования и навигации.
Предмет	• анализ уязвимостей спутниковых систем геопозиционирования и навигации.

Цель и задачи работы

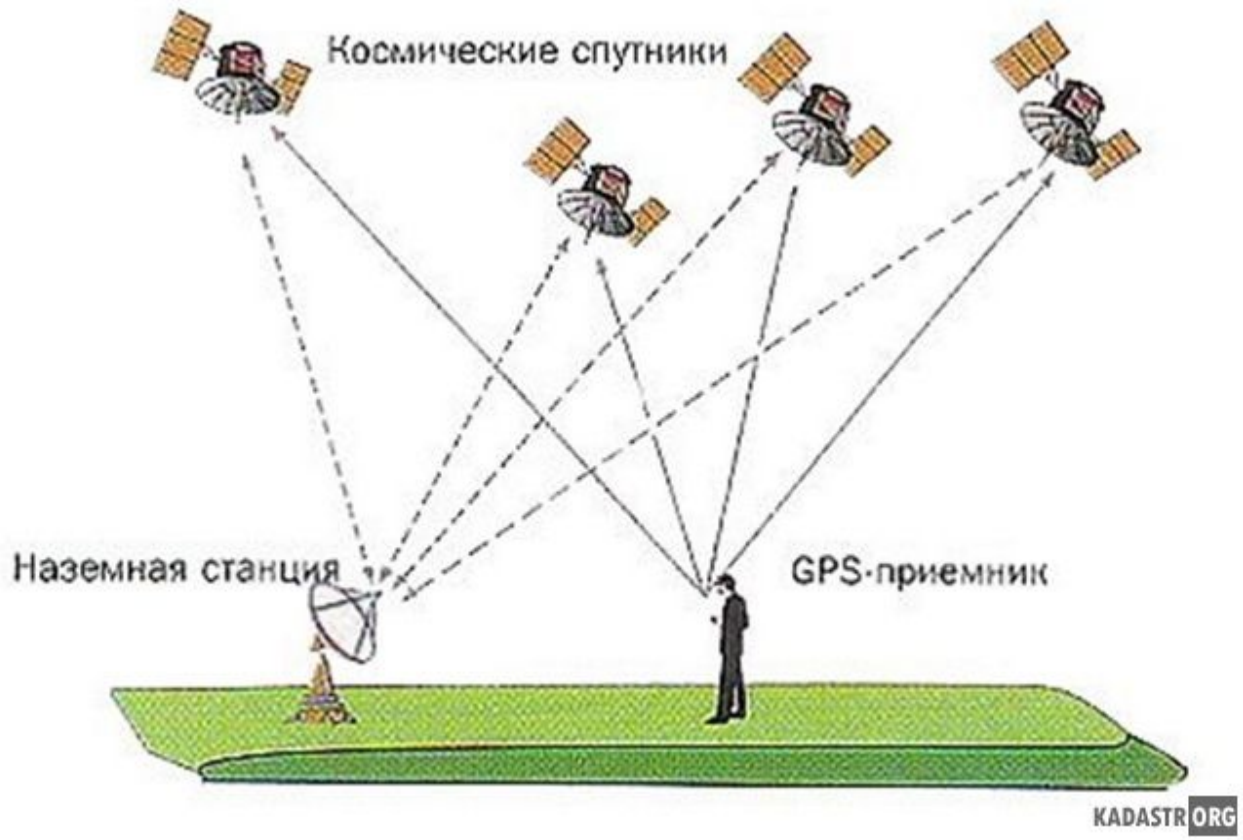
Цель: Разработка и поиск решений по преодолению уязвимостей навигации.

Для достижения этой цели в работе решаются следующие задачи:

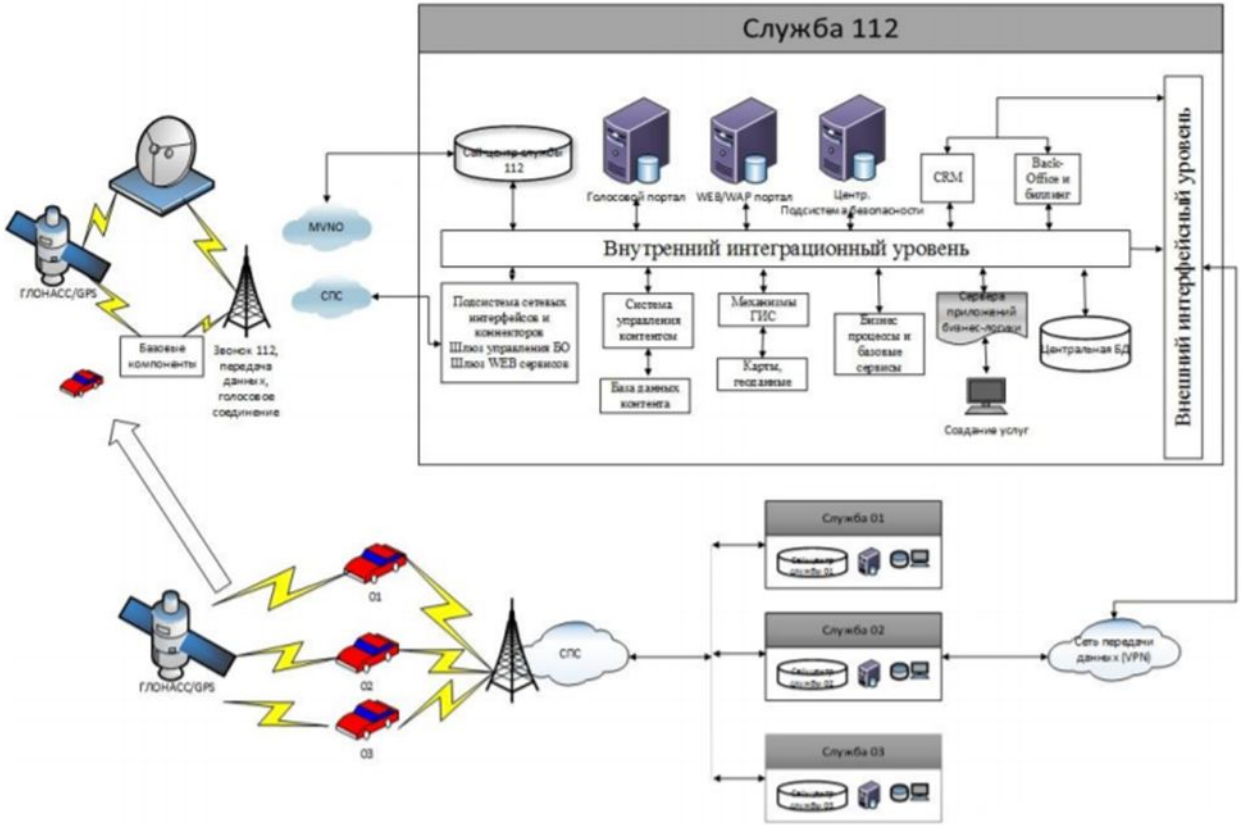
- Изучить понятие и сущность спутниковых систем геопозиционирования и навигации;
- Рассмотреть области применения спутниковых систем геопозиционирования и навигации;
- Описать современное состояние спутниковых систем геопозиционирования и навигации;
- Охарактеризовать уязвимости систем спутниковой навигации;
- Разработать рекомендации по преодолению уязвимостей спутниковых систем геопозиционирования и навигации.

Теоретическая составляющая работы

Глобальная система спутниковой навигации (GNSS) предоставляет возможность пользователям определить свое местоположение с помощью сети различных космических и наземных систем. Самыми распространенными из них являются американский GPS и российский ГЛОНАСС. А также Galileo, разработанный странами Европейского союза, и BeiDou из Китая, однако они не столь популярны.



Характеристика уязвимости систем спутниковой навигации



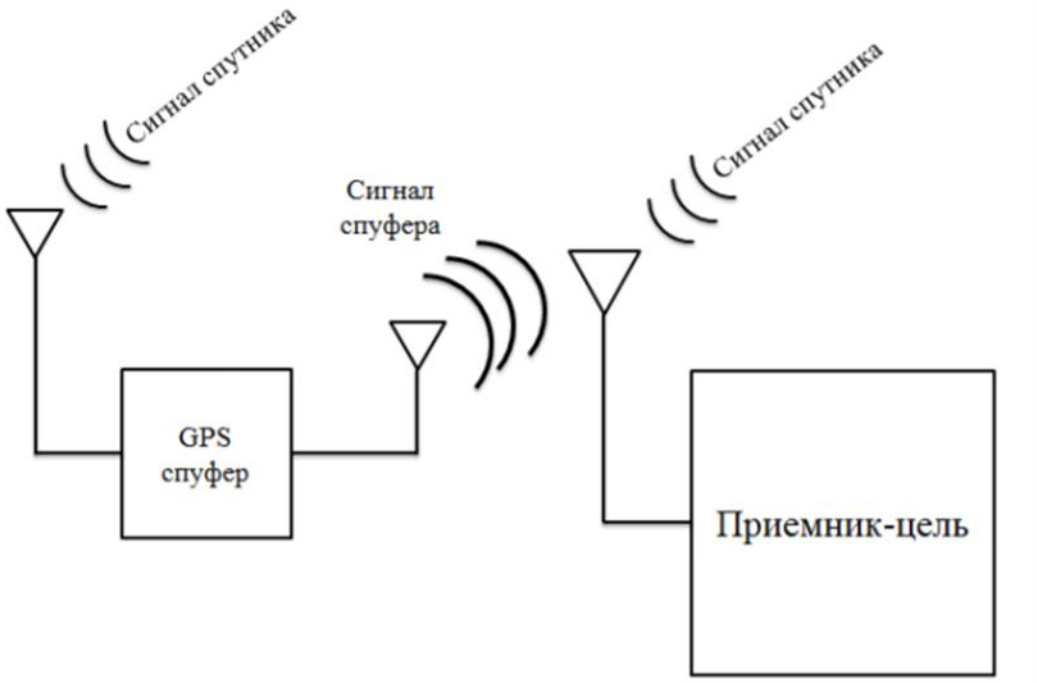
Наземная система «ЭРА-ГЛОНАСС» состоит из автомобильных терминалов, которые определяют местоположение и серьезность происшествий и автоматически отправляют сообщения экстренным службам, а также географически распределенных центров данных и региональных центров обмена информацией.

Характеристика уязвимости систем спутниковой навигации

Изучая бесконечный список атак на навигационное оборудование, можно выделить два основных вида:

- глушение сигнала
- подмена (спуфинг) сигнала.

Структура и функционирование спуфинга



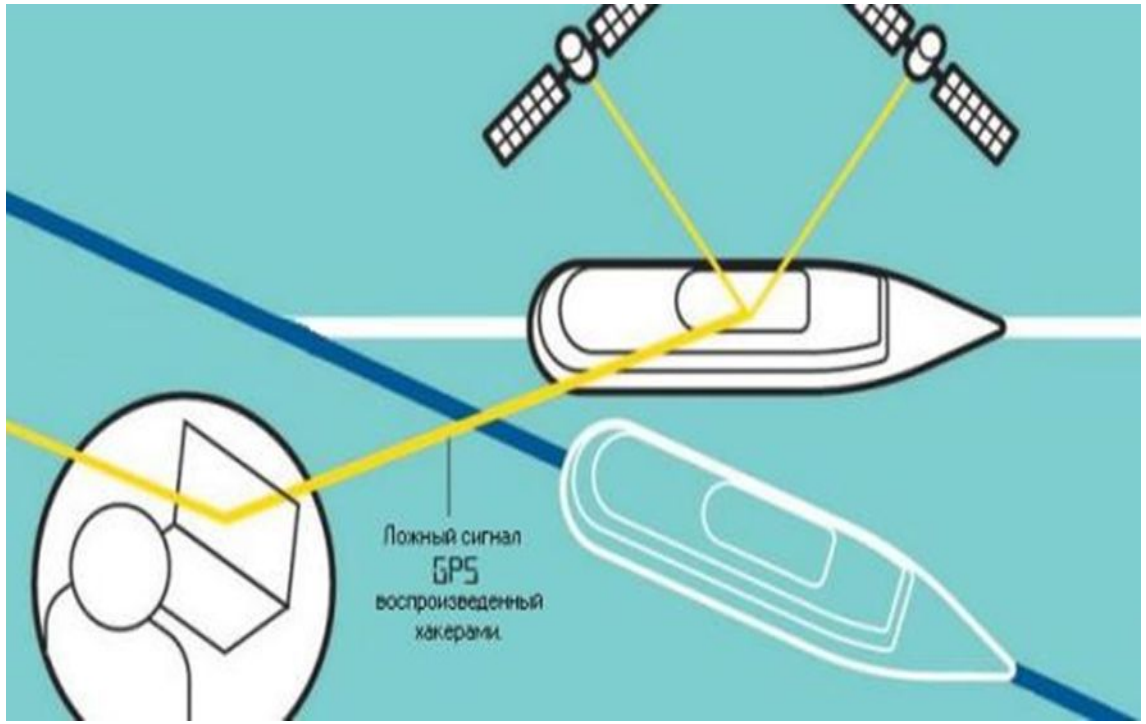


Таблица найденных инцидентов

Инцидент	Что и как было нарушено.	Результат
04.04.23 Место: Россия Модель: Navitel Navigation Взломщик: ЗАО «ЦНТ» (https://obzorstore.ru/navitel-navigator-i-karty-na-android/)	Взлом навигационного ПО, подмена координат, Подавление сигнала.	Эксперемент ученых, тест
30.01.2023 Место: Россия Модель: Pilotage Shadow FPV Взломщики: не известен (https://kopterinfo.ru/podmena-koordinat-gps-kvadrokopter/)	Взлом навигационного ПО, угон дрона и его модернизация,подмена координат, взятие под контроль еще одного дрона.	Уничтожение дрона.
07.09.2022 Место: США Цель: беспилотный автомобиль TESLA Взломщик: Рахуль Саси (Rahul Sasi) (https://www.autonews.ru/news/59afac259a79471c3db23861)	Взлом ПО	Утеря конфиденциальных данных
2022 Место: Россия Цель: Бортовой компьютер Лада Веста Взломщик: Верещака Артем (https://kazanfirst.ru/news/602116)	Нарушение доступности информации.	Утеря бортового компьютера, утеря GPS приемника.
23.12.2022 Место: Россия Цель: Бортовой компьютер, иммобилайзер IGLA 231, GPS приемник. Взломщик: неизвестен	Нарушение доступности информации, взлом ПО автомобиля.	Утеря конфиденциальных данных, искажение координат, утеря машины, похищение денежных средств (эксперимент)
22.04.23 Место: штат Миссисипи Цель :электронный браслет Взломщик: Джерри Рэйнс (https://savepearlharbor.com/?p=263290)	GPS спуфинг, электронный браслет не покидает заданную территорию.	Побег заключенного (эксперимент)

Проблемы уязвимости навигации

Возникает ожесточенное обсуждение отслеживания объектов при помощи спутников в масштабах планетарного уровня из-за возможных нарушений конфиденциальности.

Вследствие этого остро встает вопрос практической значимости поиска решений по преодолению уязвимостей систем навигации. 3 направления работы с уязвимостями:

1) Помехи и подавление спутниковых сигналов нежелательного слежения;

2) Меры по сохранению конфиденциальности данных;

3) Актуальность активного подавления систем навигации противника.

Проблемы спуфинга

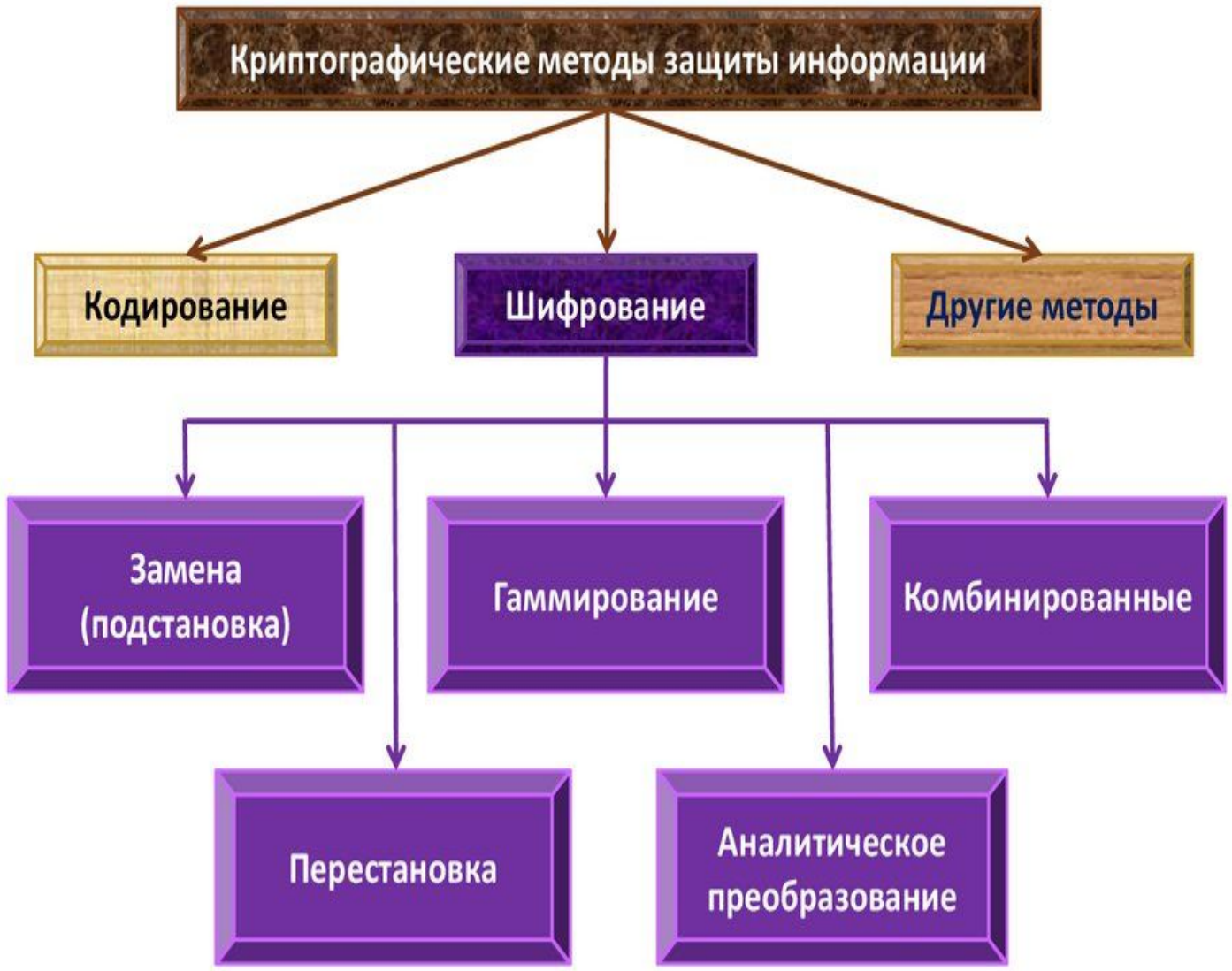
Были определены различные виды намеренных помех:

- шумовая помеха
- информационный сигнал;
- помеха со сложным законом модуляции,
- воздействие которой аналогично шумовой помехе;
- сигналы с несущей частотой,
- не модулируемой по сравнению с информационным сигналом;
- имитационная помеха,
- имеющая структуру, аналогичную структуре навигационных сигналов.

Для предотвращения спуфинг-атак на незашифрованные методы геопозиционирования рекомендуется использовать следующие меры:

- проверка мощности сигнала GPS,
- проверка изменения уровня сигнала GPS и сравнение с предыдущими значениями,
- отслеживание возможных изменений псевдодальности,
- запись временных сдвигов.
- использовать два сигнала ГНСС - российского ГЛОНАСС и американского GPS.

Разработка рекомендаций по преодолению уязвимостей систем навигации



- блокировать GPS-сигнал с помощью устройства помех.
- использовать устройство, которое обнаруживает сигнал GPS и предупреждает владельца.
- активное подавление канала навигации БПЛА противника.

Заключение

Анализ уязвимостей в навигационном канале спутниковых систем геопозиционирования выявил проблему: спуфинг-атаки против технологии ГНСС. Список атак на навигационные системы длинный, но атаки на приемники можно разделить на два наиболее распространенных типа: глушение сигнала и спуфинг. И другие решения это адаптивные антенные системы и методы создания многолучевых диаграмм, например, использование диаграммообразующих схем.

СПАСИБО ЗА ВНИМАНИЕ!