

УДК 621.396

**ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ПРИ РАЗРАБОТКЕ  
ПЕРСПЕКТИВНЫХ МЕР ЗАЩИТЫ МАЛОКАНАЛЬНОЙ  
МУЛЬТИСИСТЕМНОЙ НАВИГАЦИОННОЙ АППАРАТУРЫ  
ПОТРЕБИТЕЛЕЙ ГЛОБАЛЬНЫХ НАВИГАЦИОННЫХ СПУТНИКОВЫХ  
СИСТЕМ ОТ ВОЗДЕЙСТВИЯ СПУФИНГ-АТАК**

**П.С. Облов (Воронеж)**

Наряду с преимуществами и доступностью спутниковой навигации, имеется опасность скрытого воздействия на навигационную аппаратуру потребителей сигналами помехами. Существующие станции постановки сигналоподобных помех способны нарушить навигационно-временное обеспечение потребителя сигналами, что может привести к срыву выполнения задачи. Данная работа посвящена анализу существующих мер защиты от воздействия имитирующих помех с целью выявления основных достоинств и недостатков защиты. Приведенная информация может быть использована при разработке перспективных мер защиты навигационной аппаратуры потребителей.

В современных боевых конфликтах все более широкое применение находят беспилотные летательные аппараты (БпЛА), в том числе те из них, функционирование которых основано на беззапросном получении навигационной информации от навигационных спутников (НС) [1]. Спутниковые радионавигационные системы (СРНС) являются инструментом, позволяющим определить местонахождение потребителя, его скорость, а также точное время. Однако, наряду с неоспоримым удобством использования навигационных сигналов от СРНС, следует учитывать возможность некорректного функционирования аппаратуры потребителей (АП) навигационных сигналов ввиду наличия помех, как естественных, так и искусственных. В данной работе более подробно остановимся на рассмотрении преднамеренных помех, имитирующих истинные сигналы. Воздействие таких сигналоподобных помех на навигационную аппаратуру потребителей глобальных навигационных спутниковых систем (НАП ГНСС) называют спуфинг-атакой (от англ. «spoofing» – подмена).

Наиболее широко используемой ГНСС является GPS. Рассмотрим на ее примере штатную систему защиты НАП. Основной мерой защиты, которой оборудуют НАП ГНСС GPS, является способ автономного мониторинга целостности приемника RAIM (Receiver Autonomous Integrity Monitoring). Данный способ обнаруживает помеху, определяя ее как некачественный сигнал, поступивший на НАП ГНСС, для чего из навигационно-временных определений поочередно временно исключается каждый видимый НС. Если различие параметров сигналов, приходящих от временно исключенных НС и от остальной рабочей группировки НС выходит за рамки заданных ограничений, принимается решение о наличии внешнего вмешательства. Однако в случае приема имитирующих помех обеспечивается скрытность воздействия, такая помеха незаметна для НАП ГНСС и стандартные меры защиты оказываются неэффективными [2, 3]. Отдельно стоит отметить, что имитирующая помеха может воздействовать только на сигналы общего доступа.

Наряду с вопросами постановки имитирующих помех, интенсивное развитие получают меры защиты НАП ГНСС. Данному направлению посвящен ряд работ [4-10, 12-15]. Рассмотрим более подробно описанные в указанной литературе меры защиты НАП ГНСС.

В работе [4] предложен способ обнаружения несанкционированного воздействия на точностные характеристики космических навигационных систем, заключающийся в фильтрации и исключения аномальных выбросов, отличающийся от алгоритма RAIM следующим. В течение заданного временного интервала формируется массив достоверных измерений. Далее, на основании его значений производится расчет коэффициентов аппроксимирующего полинома. На следующем этапе производится экстраполяция полученных данных для определенного обозначенного времени, текущие значения сопоставляются с полученными экстраполированными значениями. Опираясь на принятый критерий, делается вывод о наличии внешнего воздействия. Далее фиксируется значение времени, в течение которого обнаружено внешнее воздействие. Производится анализ возможностей аппаратуры для компенсации этого воздействия, если компенсировать его невозможно, результаты измерения, полученные в указанное время, исключаются из обработки. Если в указанном промежутке времени нежелательное воздействие отсутствует, анализируется следующий отсчет времени. К недостаткам данного способа можно отнести невысокое быстродействие аппаратуры, необходимость наличия достоверных априорных данных.

В работе [5] предложен способ обнаружения преднамеренных помех НАП ГНСС. Способ обеспечивает обнаружение преднамеренных помех в несколько этапов. На первом этапе выявляется направление на передатчики полезных сигналов и помех. Далее выделяются сигналы, имеющие различающиеся координаты, но поступившие с одного направления. Такие сигналы определяются как помеховые. На втором этапе производится измерение амплитуды поступивших сигналов. Сигналы, имеющие амплитуду, значительно превышающую расчетное значение, указанное для полезного сигнала, определяются как нежелательные. На третьем этапе сравнивается структура принятых сигналов (в том числе тех, которые определены как нежелательные) с априорными данными о структуре полезного сигнала, принимается решение о соответствии или несоответствии сравниваемых параметров. По итогам трехэтапного функционирования аппаратуры, принимается заключительное решение об истинности каждого прошедшего обработку сигнала, определяются сигналы, поступившие от генераторов ложных навигационных сигналов. В числе недостатков предложенного способа можно указать неприемлемые для тактических БПЛА ближнего действия габариты и энергопотребление, а также необходимость наличия достоверных априорных данных.

В работе [6] предложено устройство обнаружения источников ложных навигационных сигналов НАП ГНСС. Функционирование устройства заключается в следующем. Элементы антенной решетки (АР) осуществляют приём поступающих сигналов, определяется направление, с которого поступают сигналы. Затем анализируются навигационные сообщения путем последовательного выбора одного из направлений формирования главного лепестка диаграммы направленности. Обрабатываются принятые сообщения, выделяются навигационные параметры. Выделенная информация поступает в анализатор сообщений, который принимает решение о принадлежности поступивших сигналов к группировке навигационных космических аппаратов относительно априорных данных. При наличии различий в структуре принятых и априорных данных на этапе анализа сообщений анализатор определяет поступивший сигнал как ложный. Среди недостатков данного устройства можно указать большие размеры фазированной антенной решетки (ФАР) и ее высокое энергопотребление, что является неприемлемыми требованиями тактических БПЛА.

В работе [7] предложен способ обнаружения имитационной помехи воздушным судном. Способ заключается в использовании на борту летательного аппарата (ЛА) технического средства для обнаружения имитирующей помехи и игнорировании ее при решении задач навигационно-временных определений. Для обнаружения имитирующих

помех используют вычислитель инерциальной навигационной системы, который прогнозирует координаты ЛА для определенного временного интервала, преобразует координаты в прогнозируемые псевдодальности для каждого НС из состава рабочей группировки. Вместе с этим на основе принятых от НС сообщений вычисляются реальные псевдодальности. Далее прогнозируемая и «реальная» псевдодальности сравниваются. Если разница является недопустимой, система подозревает НС, от которого поступил сигнал. При повторном недопустимом различии псевдодальностей в другом временном отрезке сигналы, поступающие от подозрительного НС, исключаются из процесса формирования местоположения ЛА. Недостатки данного способа – высокие массогабаритные показатели используемой аппаратуры и ее высокое энергопотребление.

В работе [8] предложен способ обнаружения, оценки параметров и подавления имитирующих, приведен пример его технической реализации. Этот способ основан на использовании метода максимального правдоподобия. В ходе функционирования вычисляются комплексные амплитуды истинных, имитационных и отраженных сигналов. Вычисляются суммы корреляции каждого поступившего комплексного навигационного сообщения с массивом дальномерных кодов, причем данный массив должен заключать в себе всю область сдвигов имитирующей сигналов по отношению к полезному навигационному сообщению. Выделение истинного сигнала на фоне имитационного воздействия осуществляется путем сопоставления параметров принятых сигналов, а, именно, комплексных амплитуд и значений времени задержки с априорными данными. По результатам сравнения принимается решение об истинности или ложности принятого навигационного сообщения. Технически данный способ реализуется с помощью многоканального приемника, в каждый канал которого включены системы слежения за фазой и задержкой. Также в каждом канале должны быть дополнительно введена аппаратура обнаружения и оценки параметров сигналоподобных помех и демультимплексор. К недостаткам предложенного способа относятся высокие материальные и энергетические затраты, а также довольно большие массогабаритные показатели.

Более подробно рассмотрим работы [9, 10], в которых приведен многофункциональный компенсатор (МФК) для НАП ГНСС с возможностью использования локальной навигационной системы (ЛНС), в качестве сигналов ЛНС выступают сигналы, поступающие от отечественных средств радиоподавления. Данное изобретение позволяет НАП корректно функционировать как в зоне дружественных постановщиков помех, так и в зоне помех, генерируемых противником. Причем, в отличие от описанных выше работ, в [9, 10] указывается на гарантированное корректное функционирование при любой интенсивности воздействия помех. Однако есть обязательное условие работы МФК: мощность помехи должна быть значительно выше мощности полезных навигационных сигналов. Рассматривается несколько вариантов функционирования МФК, при условии наличия имитирующих помех. В первом варианте подразумевается, что помехи генерирует только дружественные средства РЭП, в данном случае ухудшения качества навигационно-временного обеспечения не будет.

Во втором случае рассматривается простая помеховая обстановка, когда количество имитирующих помех меньше количества степеней свободы ФАР. В этих условиях работает защита МФК, например, пространственная компенсация помех [9], или пространственная компенсация помех вместе со структурно-временным компенсатором помех [10]. ЛНС не используется ввиду того, что показатели при работе с ГНСС по-прежнему лучше [11].

В третьем случае рассматривается функционирование в условиях сложной помеховой обстановки, причем помехи излучают дружественные генераторы ложных

навигационных сигналов (ГЛНС), когда число помех равно числу пеленгаторов. В таких условиях меры по защите мало отличаются от описанных выше. Наибольший интерес представляют две нижеописанные ситуации.

В четвертом случае, когда наблюдается сложная помеховая обстановка, обусловленная работой как дружеских, так и вражеских ГЛНС, а число помех больше количества степеней свободы ФАР (при условии, что число помех от вражеских ГЛНС меньше числа степеней свободы ФАР), эффективность принимаемых ранее мер, равно как и мер, описанных в работах [4-8], существенно снижается. В такой обстановке принимается решение на обработку сигналов, поступающих от ЛНС, так как при этом точность определения координат значительно выше [11].

В пятом случае рассматривается критическая помеховая обстановка, когда действуют и дружественные, и вражеские ГЛНС, при этом число помех только от вражеских ГЛНС превышает число степеней свободы ФАР. В данном случае корректное функционирование НАП возможно только при приеме сигналов от ЛНС и игнорировании сигналов от ГНСС. Таким образом, основные задачи МФК заключаются в поддержании корректного функционирования НАП ГНСС в условиях воздействия дружественных и вражеских ГЛНС, что обеспечивается компенсацией помех, и в обеспечении навигационно-временного обеспечения с помощью ЛНС, когда корректное функционирование на основе сигналов ГНСС невозможно.

Анализ зарубежной литературы показывает, что наиболее близкой и перспективной работой в области защиты от имитирующих помех является патент [12]. В данном патенте предложено изобретение, реализующее способы защиты НАП ГНСС от имитирующих помех. В частности, предложено назначить более одного канала приема каждому навигационному сигналу и более одного канала приема и отслеживания пиков каждому истинному или относящемуся к имитирующему сигналу пикам. Причем, для приема сигналов и выделения из них информации предусмотрено любое количество сигналов от любого количества спутников. При обнаружении имитирующего воздействия производится оповещение об этом оператора для запроса дальнейших действий. В некоторых случаях устройство самостоятельно принимает решение об изменении режима работы, оповещая при этом оператора. Также устройство может помечать сомнительные сигналы, что удобно при дальнейшей последующем решении навигационной задачи. Описанное в работе устройство принимает решение о наличии имитирующего сигнала на основе набора оцениваемых показателей. Например, оценивается амплитуда сигнала, форма и уровень спектра, уровень шума, направление приема сигналов, параметры сигналов сравниваются с параметрами альманаха, код принятого сигнала (спуфинг-атаке подвержены только сигналы общего доступа, код сигнала ограниченного доступа не имитируется). На основе оценки указанных параметров может быть составлен рейтинг сигналов, который учитывается при решении задачи навигационно-временных определений. При критической помеховой обстановке устройство может перейти на альтернативные способы навигации, основанные на использовании высотомера, компаса, гироскопа и данных от других источников для вывода устройства из зоны критического уровня имитирующих помех (поддельной зоны). Описанное устройство эффективно справляется с воздействием имитирующих помех, однако оно не лишено недостатков. Основными недостатками являются относительно большие габариты устройства, необходимость наличия большого количества (порядка нескольких сотен) свободных каналов приема, дороговизна оборудования.

Принимая во внимание особенности тактических беспилотных аппаратов ближнего действия [16], можно сделать однозначный вывод о невозможности их защиты с помощью приведенных в открытой литературе и описанных выше способов. Несовместимость данных мер защиты и тактических БПЛА ближнего действия прямо

исходит из недостатков представленных мер с одной стороны, и тактико-технических характеристик рассматриваемых БПЛА с другой стороны.

С целью разработки эффективных мер защиты малоканальной мультисистемной НАП ГНСС, обеспечивающей функционирование тактических БПЛА, предлагается провести имитационное моделирование, направленное на определение степени уязвимости рассматриваемых приемников навигационных сигналов к воздействию спуфинг-атаки. Для этого зададим следующие ограничения и допущения:

- воздействие помех на НАП ГНСС постоянно и непрерывно с момента появления АП в зоне действия постановщика помех;
- обнаружение и захват имитирующих помех каналами обработки НАП ГНСС осуществляется при появлении нового НС в зоне радиовидимости АП;
- прием хотя бы одной сигналоподобной помехи влечет за собой искажение навигационной информации [6];
- время функционирования НАП ГНСС составляет 60 минут [16].

НАП ГНСС функционирует в штатном режиме, что достигается не только работоспособностью самой АП, но и выполнением требований по ряду иных условий, таких, как количество и расположение спутников, качество сигналов и др.

Момент, когда НАП ГНСС наиболее подвержена воздействию спуфинг-атаки, можно описать следующим образом. Допустим, изначально приемник функционирует штатно, определяя местоположение по сигналам четырех видимых в настоящий момент навигационных спутников (НС). В определенный момент времени один из НС оказывается за линией радиогоризонта, в то же время приемнику для выдачи навигационно-временных определений необходимо принять навигационный сигнал от нового НС. В данный момент НАП ГНСС осуществляет режим допоиска сигналов, то есть параметры предполагаемого к обнаружению сигнала заложены в приемник. И аппаратура потребителей ищет сигнал некоего конкретного НС. В данный момент (при условии нахождения в зоне действия имитирующих помех) НАП ГНСС вместо искомого навигационного сигнала с гораздо более высокой вероятностью примет в обработку имитирующую помеху, характеристики обнаружения рассчитаны и приведены в работе [17]. В данных условиях необходимо, кроме расчетов характеристик обнаружения истинного сигнала и имитирующей помехи, произвести также расчет потенциальной уязвимости НАП ГНСС. То есть, в соответствии с введенными ограничениями, необходимо рассчитать вероятность появления хотя бы одного нового НС в составе рабочей группы в течение времени функционирования НАП. Для получения интересующих показателей в среде Matlab/Simulink было проведено имитационное моделирование, в ходе которого написаны программы для ЭВМ [18, 19], сущность их заключается в следующем. Мультисистемная малоканальная НАП ГНСС функционирует в условиях получения навигационной информации от СРНС ГЛОНАСС, GPS, Compass, Galileo. Моделируется динамика изменения пространственной конфигурации созвездий различных ГНСС. Основу программы составляет модель невозмущённого движения спутников, которая задаётся математическими соотношениями [20]:

$$X = (R_3 + H_{НС}) \cdot (\cos \omega_{П} \cdot \cos \lambda - \sin \omega_{П} \cdot \sin \lambda \cdot \cos i), \quad (1)$$

$$Y = (R_3 + H_{НС}) \cdot (\cos \omega_{П} \cdot \cos \lambda + \sin \omega_{П} \cdot \sin \lambda \cdot \cos i), \quad (2)$$

$$Z = (R_3 + H_{НС}) \cdot \sin \omega_{П} \cdot \sin i, \quad (3)$$

$$\omega_{П} = \omega_0 + t_{\text{тек}} \cdot 2\pi/T_{\text{ср}}, \quad (4)$$

$$\lambda = \lambda_0 + t_{\text{тек}} \cdot 2\pi/T_{\text{ср}}, \quad (5)$$

где:  $X, Y, Z$  – геоцентрические координаты НС;

$H_{НС}$  – высота орбиты НС;

$\omega_0$  – начальное значение аргумент перигея;

$\lambda_0$  – начальное значение долготы восходящего узла;

$R_3$  – радиус Земли;

$i$  – текущее значение наклона орбиты НС;

$T_{ср}$  – среднее значение драконического периода обращения НС;

$\omega_{II}$  – аргумент перигея, рад;

$t_{тек}$  – текущее время, на которое рассчитываются параметры движения спутника, сек.

Исходными данными для программы являются геодезические координаты НАП ГНСС и вектора начальных геоцентрических координат НС. В каждый момент времени в программе рассчитывается количество видимых НС и время появления нового спутника в зоне видимости НАП ГНСС. Для вновь появившегося  $i$ -го НС определяется значение времени  $T_{псi}$ . После завершения работы программы формируется выборка значения времени  $T_{пс}$  объемом  $N$  для каждой ГНСС. После ранжирования для каждой выборки определяются: выборочные средние, выборочные значения среднеквадратического отклонения и эмпирические функции распределения [20]:

$$\bar{T}_{пс} = \frac{1}{N} \sum_{i=1}^N T_{псi}, \quad (6)$$

$$\sigma_{T_{пс}} = \sqrt{\frac{1}{N} \sum_{i=1}^N (T_{псi} - \bar{T}_{пс})^2}, \quad (7)$$

$$F_n(T_{пс}) = \frac{n_{T_{пс}}}{N}, \quad (8)$$

где:  $\bar{T}_{пс}$  – выборочное среднее;

$\sigma_{T_{пс}}$  – выборочное значения среднеквадратического отклонения;

$F_n(T_{пс})$  – эмпирическая функция распределения;

$n_{T_{пс}}$  – количество значений меньше  $T_{пс}$ .

Полученные результаты приведены на рисунках 1-4.

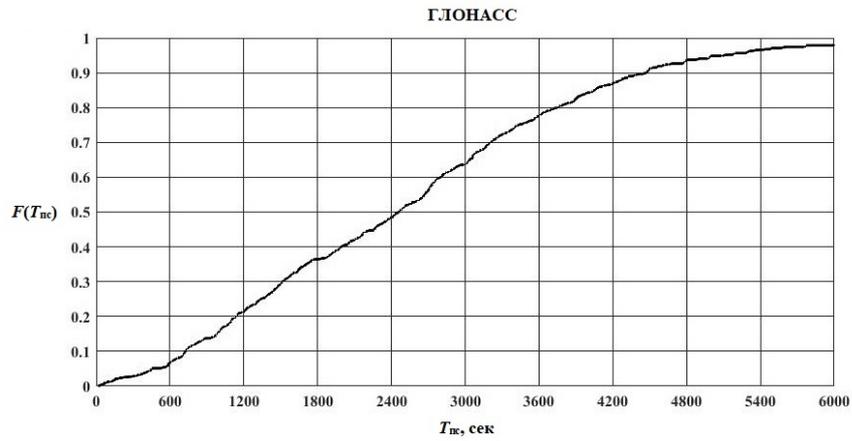


Рис. 1 – Эмпирическая функция распределения случайной величины  $T_{Пс}$  для ГНСС ГЛОНАСС

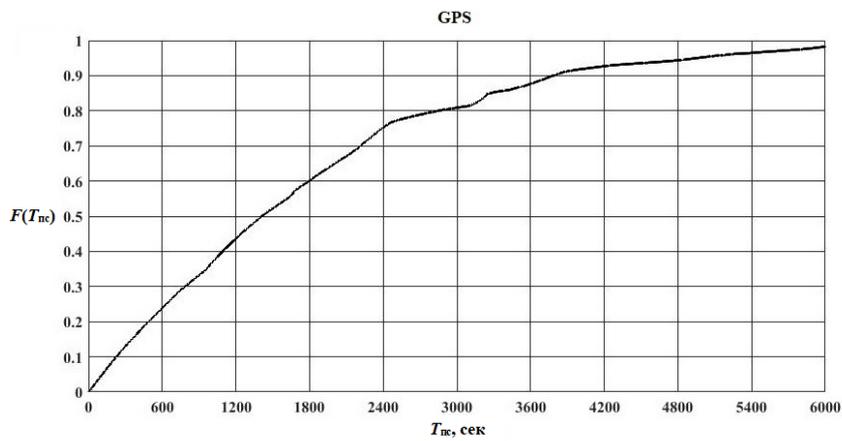


Рис. 2 – Эмпирическая функция распределения случайной величины  $T_{Пс}$  для ГНСС GPS

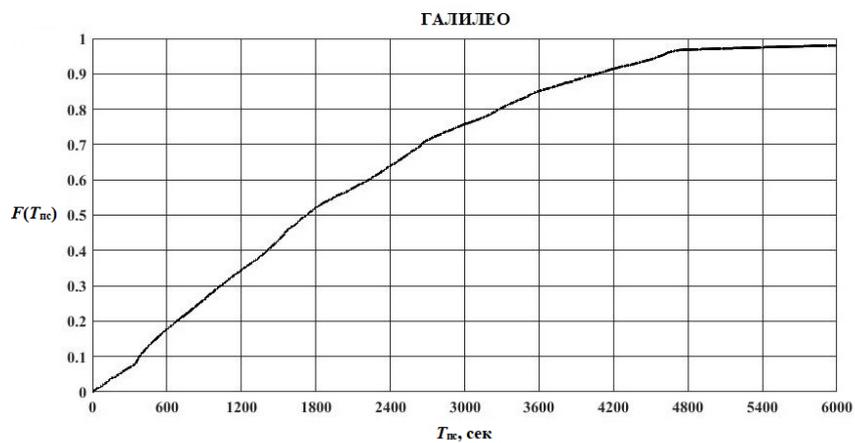


Рис. 3 – Эмпирическая функция распределения случайной величины  $T_{Пс}$  для ГНСС ГАЛИЛЕО

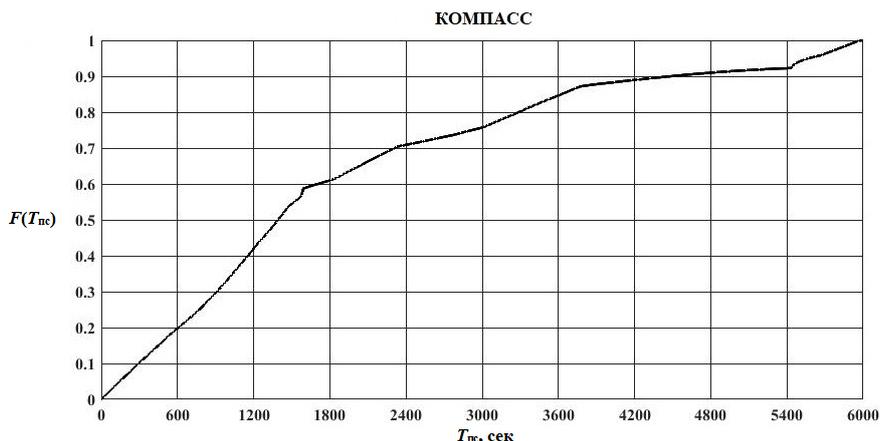


Рис. 4 – Эмпирическая функция распределения случайной величины  $T_{Пс}$  для ГНСС КОМПАСС

Полученные эмпирические функции распределения позволяют определить вероятность спуфинг-атаки за заданное время  $T_{Псз}$  как:

$$P_{са} (T_{Псз} < T_{Пс}) = F(T_{Псз}) . \quad (9)$$

Наблюдаемые при сравнении полученных графиков различия вытекают из особенностей конфигураций НС и количества НС в каждой СРНС.

Таким образом, проведенное в рамках данной работы моделирование позволяет определить степень уязвимости приемников спутниковых навигационных сигналов к спуфинг-атакам. Полученные результаты являются одним из ключевых элементов при разработке перспективных мер защиты НАП ГНСС от воздействия имитирующих помех, необходимость разработки которых, в свою очередь, вытекает из результатов проведенного в статье анализа существующих мер защиты. Представленные в статье данные предлагается использовать при разработке перспективных мер защиты мультисистемной малоканальной НАП ГНСС от воздействия имитирующих помех.

### Литература

1. **Облов П.С., Филфоненко В.В.** Сигналы, используемые в глобальных спутниковых навигационных системах // «Современное состояние и перспективы развития систем связи и радиотехнического обеспечения в управлении авиацией» Сб. науч. ст. по материалам XI Международной науч.-техн. конф. «Современное состояние и перспективы развития систем связи и радиотехнического обеспечения в управлении авиацией» (2-3 марта 2022 г.). – Воронеж: ВУНЦ ВВС «ВВА», 2022. С.325-330.
2. **Кирюшкин В.В., Бабусенко С.И., Коратаев П.Д., Неровный В.В, Облов П.С.** Вероятностные характеристики системы поиска и обнаружения навигационных сигналов в условиях имитирующих помех // Радиотехника, №7, 2023. С.60-66.
3. **Коратаев П.Д., Неровный В.В., Облов П.С., Толстых М.Ю.** Характеристики уязвимости аппаратуры потребителей глобальных навигационных спутниковых систем к спуфинг атакам. Труды учебных заведений связи, Т.9, №6, 2023, С.95-100.
4. Пат. Российская Федерация 2586076, МПК G01S 13/84. Способ обнаружения несанкционированного воздействия на точностные характеристики космических

- навигационных систем/ Гладков И.А., Василенко В.В., Зубчик М.Н; заявители и патентообладатели Федеральное государственное бюджетное учреждение «4 Центральный научно-исследовательский институт Министерства обороны Российской Федерации». 2014154045/07; заявл. , 29.12.2014; опубл 10.06.2016, Бюл. № 16.
5. Пат. Российская Федерация 2671238, МПК G01S 7/36. пособ обнаружения преднамеренных помех НАП ГНСС / Журавлев А.В., Маркин В.Г., Шуваев В.А., Красов Е.М., Иванов А.Ф.; заявитель и патентообладатель АО НВП «ПРОТЕК». 2017143741; заявл. 13.12.2017; опубл.: 30.10.2018, Бюл. № 31.
  6. Пат. Российская Федерация 2677929, МПК G01C 21/24. Устройство обнаружения источников ложных навигационных сигналов НАП ГНСС/ Журавлев А.В., Маркин В.Г., Шуваев В.А., Красов Е.М., Иванов А.Ф.; заявитель и патентообладатель АО НВП «ПРОТЕК». 2018102771; заявл. 24.10.2018; опубл. 22.01.2019, Бюл. № 3.
  7. Пат. Российская Федерация 2708679, МПК G01C 21/24. Способ обнаружения воздушным судном внешней имитационной помехи, вносящей ошибку в определение его местоположения / Затучный Д.А.; заявитель и патентообладатель Затучный Д.А. 2019111337; заявл. 16.04.2019; опубл. 11.12.2019, Бюл. № 35.
  8. Пат. Российская Федерация 2737948, МПК G01S 19/21 H04B 7/185 H04K 3/00. Способ обнаружения, оценки параметров и подавления имитационных помех и навигационный приемник с устройством обнаружения, оценки параметров и подавления имитационных помех / Фридман А.Е.; заявитель и патентообладатель Фридман А.Е. 2020107358; заявл. 18.02.2020; опубл. 07.12.2020, Бюл. № 34.
  9. Пат. Российская Федерация 2774402, МПК G01S 7/36. Многофункциональный компенсатор для навигационной аппаратуры потребителей глобальной навигационной спутниковой системы с возможностью локальной навигации по сигналам отечественных средств радиоподавления / Кирюшкин В.В., Красов Е.М., Бабусенко С.И., Журавлев А.В., Смолин А.В., Шуваев В.А., Маркин В.Г., Исаев В.В., Яковлев С.А.; заявитель и патентообладатель АО НВП «ПРОТЕК». 2021130546; заявл. 20.10.2021; опубл 21.06.2022, Бюл. № 18.
  10. Пат. Российская Федерация 2774403, МПК G01S 7/36. Многофункциональный компенсатор для навигационной аппаратуры потребителей глобальной навигационной спутниковой системы с возможностью локальной навигации по сигналам отечественных средств радиоподавления / Кирюшкин В.В., Красов Е.М., Бабусенко С.И., Журавлев А.В., Смолин А.В., Шуваев В.А., Маркин В.Г., Исаев В.В., Яковлев С.А.; заявитель и патентообладатель АО НВП «ПРОТЕК». 2021130549; заявл. 28.10.2021; опубл.: 21.06.2022, Бюл. № 18.
  11. **Бабусенко С.И., Кирюшкин В.В., Журавлев А.В.** Экспериментальная оценка помехоустойчивости модулей глобальных навигационных спутниковых систем Ublox. // М.: Радиотехника, т. 85, № 6, 2021 г., с. 77-85.
  12. US10983220B2 Classifications G01S19/215. Spoofing detection and rejection / Javad Ashjaee; Current Assignee Javad GNSS Inc. 20190154839A1, application filed 19.11.2018; publication 05.23.2023.
  13. Пат. Российская Федерация 2574860, МПК H04B 1/10. Обнаружитель с компенсатором помех / А.В. Журавлев и др. (РФ); Открытое акционерное общество научно-внедренческое предприятие «ПРОТЕК» (РФ). - №2014152662; Заявлено 24.12.2014; Опубл. 10.02.2016, Бюл. 4. - 6 с.: 1 ил.
  14. Пат. Российская Федерация 2660140, МПК H04B 1/10. Компенсатор помех для навигационной аппаратуры потребителя глобальной навигационной спутниковой системы / Маркин В.Г., Журавлев А.В., Шуваев В.А., Красов Е.М., Безмага В.М. (РФ); акционерное общество научно-внедренческое предприятие «ПРОТЕК». - № 2017122281; Заявлено 23.06.2017; Опубл. 05.07.2018, Бюл. 19. – 12 с.: 3 ил.

15. Пат. Российская Федерация 2722413, МПК G01S 3/74. Устройство и способ пространственного разделения сигналов / Маркин В.Г., Шуваев В.А., Красов Е.М. (РФ); акционерное общество научно-внедренческое предприятие «ПРОТЕК». - № 20189132703; Заявлено 16.10.2019. Опубл. 29.05.2020, Бюл. №16. – 14 с. : 4 ил.
16. **А. Великий, С. Филатов** Солдаты «с ладонь» и «с плеча» // Армейский сборник 2023, №1. С.78-82.
17. **Неровный В.В., Кирюшкин В.В., Бабусенко С.И., Коратаев П.Д., Облов П.С.** Вероятностные характеристики поиска и обнаружения навигационных сигналов в условиях имитирующих помех// Радиотехника 2023. Т.87. №7. С.60-66.
18. Программа формирования вероятности появления нового навигационного спутника в видимой группировке навигационных спутников глобальной навигационной спутниковой системы «ГЛОНАСС». Свидетельство о государственной регистрации программы для ЭВМ № 2023688614 от 22.12.2023 г., Облов П.С. Неровный В.В., Неровная Н.А., Коратаев П.Д.
19. Программа формирования вероятности появления нового навигационного спутника в видимой группировке навигационных спутников глобальной навигационной спутниковой системы «КОМПАСС». Свидетельство о государственной регистрации программы для ЭВМ № 2024610126 от 09.01.2024 г., Облов П.С. Неровный В.В., Неровная Н.А., Коратаев П.Д.
20. Global Positioning Systems, Inertial Navigation, and Integration. Mohinder S. Grewal, Lawrence R. Weill, Angus P. Andrews: 2001. John Wiley & Sons, Inc.