УДК 623.746.-519
DOI: 10.26102/2310-6018/2026.55.4.013

Экспериментальный анализ устойчивости многосистемных ГНСС-приемников беспилотных летательных аппаратов к преднамеренным радиочастотным воздействиям

А.А. Ступина[1,2,3], В.В Кукарцев[2], К.И. Кравцов[1]✉, М.А. Масюк[1]

[1]Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, Красноярск, Российская Федерация
[2]Российский государственный аграрный университет – МСХА имени К.А. Тимирязева, Москва, Российская Федерация
[3]Сибирская пожарно-спасательная академия ГПС МЧС России, Железногорск, Российская Федерация

Резюме. В большинстве современных беспилотных летательных аппаратов (БПЛА) в качестве основного средства определения пространственного положения используются глобальные навигационные спутниковые системы (ГНСС). Однако навигационные сигналы гражданского назначения обладают низкой энергетической защищенностью и уязвимы к преднамеренным радиочастотным воздействиям на физическом уровне, таким как подавление и подмена сигналов, что может приводить к потере навигационного решения или формированию ложных координат. Целью данной работы является экспериментальный анализ устойчивости навигационных приемников БПЛА к преднамеренным радиочастотным воздействиям и оценка влияния параметров мешающего сигнала на надежность приема навигационной информации ГНСС. В рамках исследования проанализированы частотные и сигнальные характеристики систем GPS, ГЛОНАСС, Galileo и BeiDou, а также проведены экспериментальные измерения отношения сигнал/шум C/N_0 при воздействии заградительных помех различной мощности и геометрии расположения источника помех. Дополнительно исследовано влияние экранирования навигационного приемника и реализована асинхронная атака с использованием программно-определяемых радиосредств. В результате установлено, что снижение C/N_0 ниже 25–28 дБ·Гц приводит к потере устойчивого навигационного приема независимо от используемой навигационной системы. Показано, что маломощные источники помех способны нарушать навигационное обеспечение БПЛА на расстояниях до нескольких сотен метров, а экранирование приемника снижает эффективность воздействия помех, но не обеспечивает полной защиты.

Ключевые слова: беспилотные летательные аппараты, глобальные навигационные спутниковые системы, навигационные приемники, радиочастотные помехи, устойчивость навигации.

Для цитирования: Ступина А.А., Кукарцев В.В., Кравцов К.И., Масюк М.А. Экспериментальный анализ устойчивости многосистемных ГНСС-приемников беспилотных летательных аппаратов к преднамеренным радиочастотным воздействиям. *Моделирование, оптимизация и информационные технологии.* 2026;14(4). URL: https://moitvivt.ru/ru/journal/article?id=2205 DOI: 10.26102/2310-6018/2026.55.4.013

Experimental analysis of the stability of unmanned aerial vehicles multi-system GNSS receivers to deliberate radio frequency impacts

A.A. Stupina[1,2,3], V.V. Kukartsev[2], K.I. Kravtsov[1]✉, M.A. Masyuk[1]

[1]Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, the Russian Federation

[2]Russian State Agrarian University – Moscow Timiryazev Agricultural Academy, Moscow, the Russian Federation
[3]Siberian Fire and Rescue Academy of State Fire Service of the Ministry of Emergency Situations of Russia, Zheleznogorsk, the Russian Federation

Abstract. In most modern unmanned aerial vehicles (UAVs), global navigation satellite systems (GNSS) are used as the main means of determining spatial position. However, civilian navigation signals have low energy security and are vulnerable to deliberate radio frequency influences at the physical level, such as signal suppression and substitution, which can lead to loss of navigation solutions or the formation of false coordinates. The purpose of this work is an experimental analysis of the stability of UAV navigation receivers to deliberate radio frequency influences and an assessment of the influence of interfering signal parameters on the reliability of receiving GNSS navigation information. As part of the study, the frequency and signal characteristics of GPS, GLONASS, Galileo and BeiDou systems were analyzed, as well as experimental measurements of the signal-to-noise ratio C/N_0 when exposed to barrage interference of various power and geometry of the interference source location. Additionally, the effect of shielding the navigation receiver was investigated and an asynchronous attack using software-defined radio devices was implemented. As a result, it was found that a decrease in C/N_0 below 25–28 dB·Hz leads to a loss of stable navigation reception, regardless of the navigation system used. It is shown that low-power sources of interference can disrupt the navigation support of UAVs at distances up to several hundred meters, and the shielding of the receiver reduces the effectiveness of interference, but does not provide complete protection.

Keywords: unmanned aerial vehicles, global navigation satellite systems, navigation receivers, radio frequency interference, navigation stability.

For citation: Stupina A.A., Kukartsev V.V., Kravtsov K.I., Masyuk M.A. Experimental analysis of the stability of unmanned aerial vehicles multi-system GNSS receivers to deliberate radio frequency impacts. 2026;14(4). (In. Russ.). URL: https://moitvivt.ru/ru/journal/article?id=2205 DOI: 10.26102/2310-6018/2026.55.4.013

Введение

В последние годы беспилотные летательные аппараты (БПЛА) получили широкое распространение в задачах мониторинга, аэрофотосъемки, логистики, обеспечения безопасности и автоматизации различных процессов [1]. Существенное распространение областей применения БПЛА сопровождается ростом требований к надежности, устойчивости в навигационном обеспечении, так как ошибки в позиционировании напрямую влияют на безопасность полета и корректность выполнения задач [2].

БПЛА в качестве основного средства определения пространственного положения используют глобальные навигационные спутниковые системы (ГНСС), такие как GPS, ГЛОНАСС, Galileo и BeiDou. Несмотря на развитие навигационных приемников, навигационные сигналы ГНСС остаются уязвимыми к воздействиям на разных уровнях [3]. В результате этого, навигационные приемники БПЛА подвержены помехам и целенаправленным деструктивным воздействиям.

Особую опасность для функционирования БПЛА представляют преднамеренные радиочастотные воздействия, включая подавление навигационных сигналов и их подмену. Подобные атаки способны приводить к полной потере навигационного решения либо к формированию заведомо ложных координат, что в условиях автономного полета может вызвать отклонения от маршрута, потерю управления или аварию [4]. Несмотря на наличие значительного числа теоретических работ, посвященных анализу уязвимостей ГНСС, недостаточно изучены зависимости между мощностью мешающего воздействия, геометрией расположения источника помех и устойчивостью приема навигационных сигналов [5]. Это затрудняет выработку рекомендаций по повышению надежности навигационного обеспечения БПЛА.

В связи с этим актуальной является задача экспериментального анализа устойчивости навигационных приемников БПЛА к преднамеренным радиочастотным воздействием с учетом современных архитектур ГНСС и условий их практического применения.

Главной целью исследования является экспериментальный анализ устойчивости навигационных приемников БПЛА к намеренным воздействиям на физическом уровне и оценка влияния параметров мешающего сигнала на надежность приема навигационной информации ГНСС.

Для достижения цели в работе решались следующие основные задачи:

– анализ структуры и частотные диапазоны навигационных сигналов ГНСС, используемые в современных БПЛА;

– экспериментальное воздействие заградительных помех на устойчивость приема навигационных сигналов в зависимости от мощности источника помех и пространственного расположения БПЛА;

– оценка изменения отношения сигнал / шум навигационных сигналов при воздействии мешающих сигналов и определение порогового значения, приводящих к потере устойчивого навигационного сигнала;

– исследование влияния экранирования навигационного приемника на снижение эффективности мешающих воздействий в реальных условиях эксплуатации БПЛА;

– формирование ложного навигационного решения при реализации асинхронной атаки с использованием программно-определяемых радиосредств.

Материалы и методы

Для обоснования параметров мешающих воздействий были проанализированы рабочие частотные диапазоны навигационных сигналов указанных ГНСС. Диапазоны несущих частот и ширины каналов навигационных сигналов представлены в Таблице 1 [6].

Таблица 1 – Диапазоны частот навигационных сигналов ГНСС
Table 1 – Frequency ranges of GNSS navigation signals

ГНСС	Поддиапазон	Несущая частота, МГц	Ширина канала, МГц
GPS	L1	1575,42	30,69
	L2	1227,6	30,69
	L5	1176,45	–
ГЛОНАСС	L1	1602	10 (14×0,5625)
	L2	1246	5,6875 (14×0,4375)
	L3	1202,025	8,037 (20×0,4230)
Galileo	E1	1575,42	24,552
	E6	1278,75	40,92
	E5	1207,14	51,15
BeiDou	B1	1575,42	32,736 (B1C), 4,092 (B1I)
	B3	1268,52	20,46
	B2	1207,14	20,46

Таблица 1 демонстрирует, что основные гражданские навигационные сигналы ГНСС сосредоточены в L-диапазоне частот (1–2 ГГц) и характеризуются частичным перекрытием спектров различных систем. Это обусловливает необходимость комплексного воздействия при анализе устойчивости многосистемных навигационных

приемников, поскольку подавление сигналов одной навигационной системы не гарантирует потери навигационного решения в целом.

Для оценки эффективности мешающих воздействий также были рассмотрены методы модуляции, структура сигналов и используемые псевдослучайные последовательности (ПСП) навигационных сигналов (НС). Характеристики навигационных сигналов различных ГНСС приведены в Таблице 2 [7]. В таблице представлены только открытые гражданские сигналы, используемые в навигационных приемниках БПЛА.

Таблица 2 – Характеристики навигационных сигналов различных ГНСС (открытые сигналы)
Table 2 – Characteristics of navigation signals of various GNSS (open signals)

ГНСС	Поддиапазон	НС	Модуляция	Компоненты	Частота кода, Мбит/с	Длина кода	ПСП
GPS	L1	C/A	BPSK	Инф.	1.023	1023	код Голда
	L1	L1C	TMBOC	Инф.+пилот	1.023	10230	код Вейла
	L2	CM	BPSK	Инф.	0.5115	10230	М-посл.
	L2	CL	BPSK	Пилот	0.5115	767250	М-посл.
	L5	I	BPSK	Инф.	10.23	10230	М-посл.
	L5	Q	BPSK	Пилот	10.23	10230	М-посл.
ГЛОНАСС	L1	C/A	BPSK	Инф.	0.511	511	М-посл.
	L2	C/A	BPSK	Инф.	0.511	511	М-посл.
Galileo	E1	E1 OS	CBOS	Инф.+пилот	1.023	250	М-посл.
	E5	E5a/E5b	BOC	Инф.+пилот	10.23	10230	М-посл.
BeiDou	B1	I	BPSK	Инф.+пилот	0.2046	2046	код Голда
	B2	I	BPSK	Инф.+пилот	0.1023	2046	код Голда

Таблица 2 показывает, что навигационные сигналы различных ГНСС используют схожие методы модуляции и близкие частоты кодирования, что определяет сопоставимую чувствительность приемников к широкополосным и заградительным помехам. Наличие пилотных компонентов и различий в структуре сигналов может влиять на устойчивость приема, однако при воздействии помех достаточной мощности потеря устойчивого приема наблюдается для всех рассматриваемых систем [8].

Совмещенный спектр навигационных сигналов различных ГНСС приведен на Рисунке 1 [9].

Рисунок наглядно иллюстрирует перекрытие рабочих диапазонов GPS, ГЛОНАСС, Galileo и BeiDou и подтверждает целесообразность анализа воздействия мешающих сигналов в широком диапазоне частот. Представленные спектральные соотношения использовались при выборе параметров генерации помех в экспериментальной части исследования.

Приведение характеристик навигационных сигналов ГНСС необходимо для понимания механизмов воздействия радиочастотных помех на навигационный приемник. Навигационные сигналы гражданских ГНСС имеют крайне малую мощность на входе приемника – порядка –155–160 дБВт, что делает их уязвимыми даже к маломощным источникам помех. Ширина каналов навигационных сигналов составляет от 5 до 50 МГц, вследствие чего широкополосная заградительная помеха,

перекрывающая соответствующий диапазон, приводит к резкому снижению отношения сигнал/шум [10].

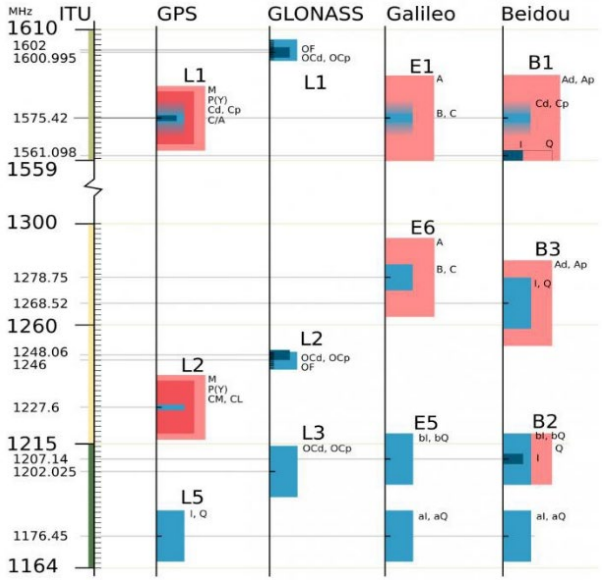


Рисунок 1 – Используемые диапазоны НС различных ГНСС
Figure 1 – Used NS ranges of various GNSS

Используемые методы модуляции и частоты кодирования 0,1–10,23 Мбит/с определяют устойчивость приемника к различным типам помех, однако при снижении сигнал/шум ниже 25–28 дБ·Гц становится невозможной устойчивая корреляционная обработка навигационных сигналов [11]. Перекрытие рабочих диапазонов GPS, ГЛОНАСС, Galileo и BeiDou в L-диапазоне частот приводит к тому, что воздействие помехи в одной частотной области может одновременно ухудшать прием сигналов нескольких навигационных систем, что критично для многосистемных приемников БПЛА [12].

Подавление навигационных сигналов осуществлялось заградительной помехой в диапазоне 1–2 ГГц, соответствующем рабочим частотам ГНСС. Мощность источника помех изменялась в пределах 0–17,5 Вт. Расстояние между источником помех и БПЛА составляло 200–800 м, высота полета БПЛА – 0–200 м. Измерения проводились при наличии и отсутствии экранирования навигационного приемника.

Критерием устойчивости приема использовалось отношение сигнал/шум. Потеря устойчивого приема фиксировалась при снижении <25–28 дБ·Гц, что соответствует срыву корреляционной обработки навигационных сигналов. Для каждого уровня мощности помехи регистрировались значения и состояние навигационного решения.

Воздействие реализовывалось в виде асинхронной имитации навигационного сигнала GPS с использованием программно-определяемого радиосредства. Эффективность атаки оценивалась по факту смещения вычисленных координат навигационного приемника относительно истинного положения.

Результаты

Результаты измерения отношения сигнал/шум C/N_0 при воздействии заградительной помехи с указанием номера космического аппарата (КА) приведены в Таблице 3. Эксперименты проводились при фиксированном пространственном

расположении БПЛА (L = 500 м, H = 100 м) с плавным увеличением мощности источника помех в диапазоне 0–17,5 Вт.

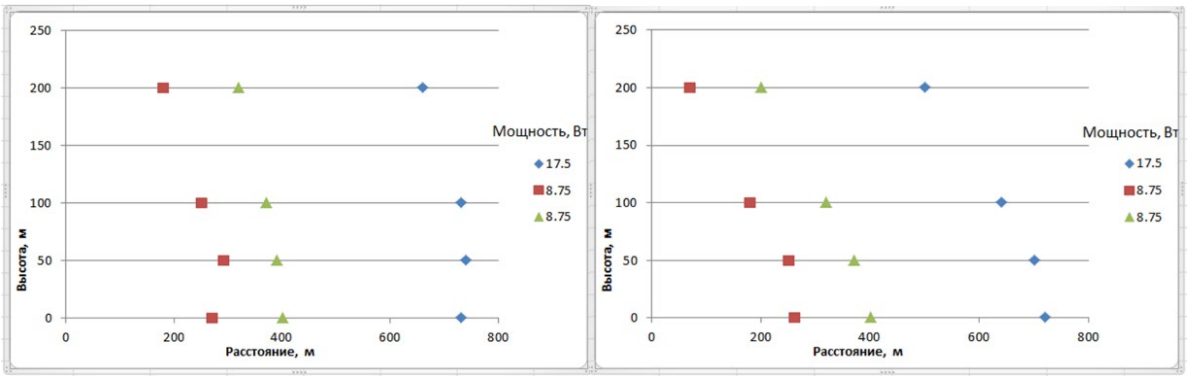
Таблица 3 – Отношение сигнал/шум (C/N0 [дБ·Гц]) при воздействии jamming-атаки
Table 3 – Signal-to-noise ratio (C/N0 [dB·Hz]) under jamming attack

ГНСС	№ КА	0 Вт	6 Вт	9 Вт	12 Вт	17,5 Вт
GPS	16	47,3	31,8	25,2	21,2	15,9
	23	43,2	29,7	23,1	18,7	н/о
	24	41,9	32,3	24,2	18,5	н/о
BeiDou	36	42,7	32,0	24,1	18,6	н/о
	19	38,3	29,7	23,2	15,1	н/о
Galileo	5	46,1	28,1	23,9	20,4	н/о
	24	43,6	24,0	20,0	18,1	н/о
Приём		Уст.	Уст.	Уст.	Неуст.	Неуст.

Примечание: н/о – устойчивый прием навигационного сигнала отсутствует.

Из собранных данных следует, что при отсутствии помех значения C/N_0 для навигационных сигналов GPS, Galileo и BeiDou находились в диапазоне 42–47 дБ·Гц, что соответствует устойчивому приему. При увеличении мощности помехи до 6–9 Вт наблюдалось резкое снижение C/N_0 до 23–28 дБ·Гц, а при дальнейшем увеличении мощности до 12 Вт и более устойчивый прием навигационных сигналов становился невозможным для большинства аппаратов, что фиксировалось как потеря навигационного решения.

Можно сказать, что для гражданских многосистемных навигационных приемников порог устойчивого приема при воздействии заградительной помехи соответствует значениям C/N_0 = 25–28 дБ·Гц, независимо от используемой навигационной системы. Пространственные характеристики зоны подавления навигационного сигнала представлены на Рисунке 2. На Рисунке 2*а* показаны результаты измерений при отсутствии экранирующего слоя, на Рисунке 2*б* – при наличии экранирования навигационного приемника.



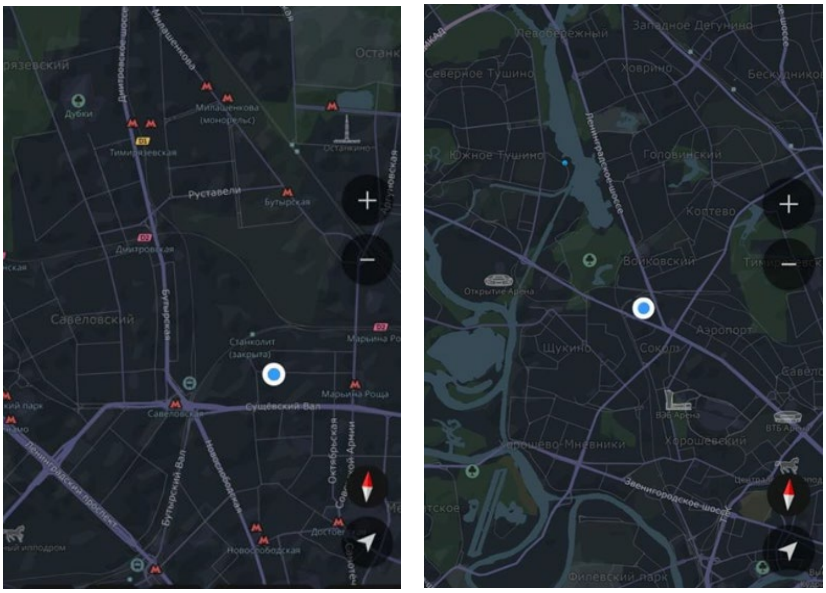
а) *б*)

Рисунок 2 – Пространственные характеристики зоны подавления навигационного сигнала: *а* – без экранирующего слоя; *б* – при наличии экранирующего слоя
Figure 2 – Spatial characteristics of the navigation signal suppression zone: *a* – without a shielding layer; *b* – with a shielding layer

Из рисунка видно, что при максимальной мощности источника помех (17,5 Вт) зона неустойчивого приема без экранирования достигает расстояний до 700–750 м, тогда

как применение экранирования приводит к сокращению эффективной зоны подавления до ≈500–600 м, особенно на высотах более 100 м.

Результаты реализации асинхронной атаки приведены на Рисунке 3. В исходном состоянии навигационный приемник корректно определял свое пространственное положение (Рисунок 3*а*). При включении генерации ложного навигационного сигнала наблюдалось смещение вычисленных координат приемника в заранее заданную точку, не соответствующую истинному местоположению (Рисунок 3*б*).



а) *б*)

Рисунок 3 – Результаты реализации асинхронной атаки: *а* – истинное положение навигационного приемника; *б* – ложное положение навигационного приемника
Figure 3 – The results of the asynchronous attack: *a* – the true position of the navigation receiver; *b* – the false position of the navigation receiver

Факт успешного формирования ложного навигационного решения подтверждает уязвимость гражданских навигационных приемников БПЛА к атакам при отсутствии механизмов аутентификации навигационных сигналов. Реализованная атака не требовала высокой выходной мощности передатчика и осуществлялась в пределах стандартных рабочих диапазонов GPS.

Обсуждение

Полученные экспериментальные результаты подтверждают высокую уязвимость гражданских навигационных приемников БПЛА к преднамеренным радиочастотным воздействиям на физическом уровне. Согласно данным, снижение отношения сигнал/шум C/N_0 ниже пороговых значений 25–28 дБ·Гц приводит к потере устойчивого навигационного решения независимо от используемой навигационной системы. Это указывает на сопоставимую чувствительность GPS, Galileo и BeiDou к заградительным помехам при работе в перекрывающихся диапазонах L-диапазона.

Анализ пространственных характеристик зоны подавления показал, что применение экранирования навигационного приемника позволяет уменьшить эффективную дальность воздействия помех на 20–30 %, однако не обеспечивает полной защиты при увеличении мощности источника помех. Экранирование может

рассматриваться лишь как вспомогательная мера повышения устойчивости навигационного приема.

Результаты эксперимента демонстрируют возможность формирования ложного навигационного решения без применения высокомощных передатчиков, что представляет потенциальную угрозу для автономных БПЛА, использующих ГНСС в качестве основного источника навигационной информации.

Заключение

На основе анализа параметров навигационных сигналов GPS, ГЛОНАСС, Galileo и BeiDou и экспериментальных измерений установлены пороговые условия, при которых происходит потеря устойчивого навигационного решения.

Показано, что при воздействии заградительных помех, снижение отношения сигнал/шум C/№ ниже 25–28 дБ·Гц приводит к срыву корреляционной обработки навигационных сигналов и потере устойчивого приема для всех рассматриваемых ГНСС. Экспериментально подтверждено, что маломощные источники помех с выходной мощностью 9–12 Вт способны нарушать навигационное обеспечение БПЛА на расстояниях до 500–700 м в условиях прямой радиовидимости.

Установлено, что применение экранирования навигационного приемника позволяет снизить дальность эффективного воздействия помех, однако не обеспечивает полной защиты от преднамеренных радиочастотных воздействий. Реализация асинхронной атаки продемонстрировала возможность формирования ложного навигационного решения без использования высокомощных передатчиков, что подтверждает уязвимость гражданских навигационных приемников при отсутствии механизмов аутентификации навигационных сигналов.

Полученные результаты могут быть использованы при проектировании навигационных систем БПЛА для оценки потенциальных угроз на физическом уровне и обоснования необходимости применения комплексных навигационных решений, повышающих устойчивость к подавлению и подмене навигационных сигналов.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Hashim H.A. Advances in UAV avionics systems architecture, classification and integration: A comprehensive review and future perspectives. *Results in Engineering.* 2025;25. https://doi.org/10.1016/j.rineng.2024.103786
2. Zhao T., Zhang Y., Wang M., et al. A critical review on the battery system reliability of drone systems. *Drones.* 2025;9(8). https://doi.org/10.3390/drones9080539
3. Добрякова Л.А., Лемишевский Л.С., Очин Е.Ф. Атаки на глобальные навигационные спутниковые системы и обнаружение спуфинга беспилотных кораблей, базирующееся на облачных технологиях. *Ural Radio Engineering Journal.* 2018;2(2):40–56. (На англ.). https://doi.org/10.15826/urej.2018.2.2.003
   Dobryakova L.A., Lemieszewski Ł.S., Ochin E.F. Global navigation satellite systems attacks and a cloud-based spoofing detection for unmanned ships. *Ural Radio Engineering Journal.* 2018;2(2):40–56. https://doi.org/10.15826/urej.2018.2.2.003
4. Богуспаев Н., Ахмедов Д., Кобдикова Ш., Савельев Е. Разработка модуля приема и обработки радиосигналов ГНСС на основе технологии SDR. *Вестник Казахской академии транспорта и коммуникаций им. М. Тынышпаева.* 2025;(1):88–95.
   Boguspayev N., Akhmedov D., Kobdikova Sh., Savelyev Ye. Development of a GNSS radio signal reception and processing module based on SDR technology. *Bulletin of the Kazakh Academy of Transport and Communications named after M. Tynyshpayev.* 2025;(1):88–95. (In Russ.).

5. Валайтите А.А., Никитин Д.П., Садовская Е.В. Исследование влияния ошибки многолучевости на точность определения параметров сигналов ГНСС (глобальных навигационных спутниковых систем) при помощи имитатора навигационного поля. *Труды МАИ.* 2014;(77). URL: https://trudymai.ru/published.php?ID=53172
Valaitite A.A., Nikitin D.P., Sadovskaya E.V. Investigation of the multipath effect on the estimation of the GNSS signal parameters using simulator of navigation field. *Trudy MAI.* 2014;(77). (In Russ.). URL: https://trudymai.ru/eng/published.php?ID=53172
6. Федотовских А.В. *Особенности разработки и эксплуатации гражданских беспилотных авиационных систем с технологиями искусственного интеллекта в Арктической зоне Российской Федерации.* Москва: Ай Пи Ар Медиа; 2022. 277 с.
7. Ni Sh., Ren B., Chen F., et al. GNSS spoofing suppression based on multi-satellite and multi-channel array processing. *Frontiers in Physics.* 2022;10. https://doi.org/10.3389/fphy.2022.905918
8. Mendu B., Mbuli Nh. State-of-the-art review on the application of unmanned aerial vehicles (UAVs) in power line inspections: Current innovations, trends, and future prospects. *Drones.* 2025;9(4). https://doi.org/10.3390/drones9040265
9. Meitivyeki M.M., Liu H. Global positioning system signal verification through correlation function distortion and received power tracking. *Journal of Technology and Systems.* 2024;6(3):34–51. https://doi.org/10.47941/jts.1835
10. Hamza V., Stopar B., Sterle O., Pavlovčič-Prešeren P. Recent advances and applications of low-cost GNSS receivers: a review. *GPS Solutions.* 2025;29(1). https://doi.org/10.1007/s10291-025-01815-x
11. Hu J., Wu Yu., Su Sh. Flexible prescribed performance tracking control for receiver UAV with actuator faults and constraints. *Journal of the Franklin Institute.* 2025;362(16). https://doi.org/10.1016/j.jfranklin.2025.108033
12. Saber M.J., Hasna M., Badarneh O.S. THz-enabled UAV communications under pointing errors: tractable statistical channel modeling and security analysis. *IEEE Open Journal of Vehicular Technology.* 2025;6:801–811. https://doi.org/10.1109/OJVT.2025.3547244

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTORS

Ступина Алена Александровна, доктор технических наук, профессор, профессор кафедры прикладной информатики, Российский государственный аграрный университет – МСХА имени К.А. Тимирязева, Москва, Сибирская пожарно-спасательная академия ГПС МЧС России, Железногорск, Российская Федерация.
e-mail: h677hm@gmail.com

Alena A. Stupina, Doctor of Engineering Sciences, Professor, Professor at the Department of Applied Informatics, Russian State Agrarian University – Moscow Timiryazev Agricultural Academy, Moscow, Siberian Fire and Rescue Academy of State Fire Service of the Ministry of Emergency Situations of Russia, Zheleznogorsk, the Russian Federation.

Кукарцев Владислав Викторович, кандидат технических наук, доцент, доцент кафедры прикладной информатики, Российский государственный аграрный университет – МСХА имени К.А. Тимирязева, Москва, Российская Федерация.
e-mail: vlad_saa_2000@mail.ru

Vladislav V. Kukartsev, Candidate of Engineering Sciences, Docent, Associate Professor at the Department of Applied Informatics, Russian State Agrarian University – Moscow Timiryazev Agricultural Academy, Moscow, the Russian Federation.

Кравцов Кирилл Игоревич, магистрант, Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, Красноярск, Российская Федерация.
e-mail: rhfdwjdr1@gmail.com

Kirill I. Kravtsov, Master's Degree student, Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, the Russian Federation.

Масюк Максим Анатольевич, кандидат технических наук, доцент, заведующий кафедрой информационных экономических систем, Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, Красноярск, Российская Федерация.
e-mail: masyuk@sibsau.ru

Maxim A. Masyuk, Candidate of Engineering Sciences, Docent, Head of the Department of Information Economic Systems, Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, the Russian Federation.

Статья поступила в редакцию 07.02.2026; одобрена после рецензирования 17.04.2026; принята к публикации 22.04.2026.

The article was submitted 07.02.2026; approved after reviewing 17.04.2026; accepted for publication 22.04.2026.