УДК 338.48-6:629.056.8
DOI:https://doi.org/10.25128/2519-4577.25.3.17

Іван РУДАКЕВИЧ, кандидат географічних наук,
доцент кафедри географії України і туризму, ORCID: https://orcid.org/0000-0002-3901-5897
Тернопільський національний педагогічний університет імені Володимира Гнатюка,
46015, вул. М.Кривоноса, 2, м. Тернопіль, Україна

СУЧАСНІ ГЕОПРОСТОРОВІ ПРОБЛЕМИ РОЗВИТКУ СИСТЕМ СУПУТНИКОВОЇ НАВІГАЦІЇ, ЇХ ВИКОРИСТАННЯ У ГОСПОДАРСЬКІЙ ТА ТУРИСТИЧНІЙ ДІЯЛЬНОСТІ

У публікації охарактеризовані сучасні геопросторові проблеми розвитку систем супутникової навігації, їх використання у господарській та туристичній діяльності. Проаналізовано актуальність проблематики використання супутникових навігаційних систем у різних сферах діяльності. Розкрито аспекти вразливості геопозиційних систем через підміну їх сигналу (спуфінг) чи глушіння. Охарактеризовано напрями використання супутникових навігаційних систем у туристичній діяльності. Проаналізовані заходи щодо запобігання спотворенню та перетворенню сигналів навігаційних супутникових систем.

Ключові слова: *геопозиціонування, глушіння, GPS, супутникові навігаційні системи, спуфінг, туризм.*

Ivan RUDAKEVYCH. Candidate of Geographical Sciences,Associate Professor,
Department of Geography of Ukraine and Tourism, ORCID: https://orcid.org/0000-0002-3901-5897
Ternopil Volodymyr Hnatiuk National Pedagogical University,
46015, M.Kryvonosa St., 2, Ternopil, Ukraine

MODERN GEOSPATIAL PROBLEMS OF SATELLITE NAVIGATION SYSTEMS DEVELOPMENT, THEIR USE IN ECONOMIC AND TOURIST ACTIVITIES

The publication modern geospatial problems of satellite navigation systems development, their use in economic and tourist activities are described. The relevance of the issues of using satellite navigation systems in various fields of activity is analyzed. Aspects of vulnerability of geopositioning systems due to substitution of their signal (spoofing) or its jamming are revealed. The possible negative consequences of distortion of satellite navigation system signals are described. The contribution to the study of modern aspects of navigation systems development in the context of modern challenges in the research of ukrainian and foreign scientists is analyzed. The most common satellite navigation systems in the world are briefly described. The American GPS network is the most widespread in the world and provides the best signal accuracy. The Russian GLONASS is less popular due to frequent failures and problems with satellites. The European Galileo navigation system is a completely civilian development, although it can be used by the military to ensure the security of EU countries. The Chinese BeiDou system was developed with a strategic goal to reduce China's dependence on American or European satellite navigation. In tourism, satellite navigation systems are used mainly for the use of tourist maps and the use of geolocation for orientation in the terrain. In tourism, navigation systems are also used for orientation and tracking of groups moving by road, water or air transport. Global navigation satellite systems (GNSS) are used to determine precise positioning (location), navigation and time (PNT). Due to navigation failures, the precise time function of PNT is often lost, which leads to a deterioration in the accuracy of geopositioning. Depending on the change in PNT, interference in the operation of navigation systems is distinguished as signal substitution (spoofing) or jamming. The features of the manifestation of spoofing or signal jamming in the operation of satellite systems are characterized. GPS failures were recorded primarily near military facilities. For the first time, spoofing and jamming technologies for satellite navigation systems were recorded back in 2008. Until then, experts considered the GPS system resistant to distortion and interference. Problems with navigation system signals were especially acute by 2019, when experts recorded numerous radio-electronic interference from Russia. The most massive damage to GPS signals was recorded in January 2024 in Poland and the Baltic Sea. Then the signals of this navigation system were jammed. Negative trends in the distortion of navigation signals continued in 2025, when they were also recorded in Bulgaria. Most often, failures concerned air transport navigation. Such events can negatively affect tourist flows and centers. To prevent distortion and transformation of signals of navigation satellite systems, a number of measures are being implemented to increase their stability: analysis of power and signal correction, use of multi-frequency and multi-system receivers, signal filtering, etc. Improved receivers contain updated firmware algorithms or digital filters that can detect and remove interfering signals. Satellite navigation systems themselves are also being improved by launching more modern satellites and increasing the number of correction stations.

Keywords: *geolocation, jamming, GPS, satellite navigation systems, spoofing, tourism.*

Постановка науково-практичної проблеми: актуальність і новизна дослідження. Сучасні системи супутникової навігації (Global Navigation Satellite System, GNSS) мають велике значення у модерному інформаційному суспільстві, забезпечуючи точне позиціонування, визначення часу та параметрів руху різних об'єктів у будь-якій точці Землі. Головним значен-

ням цих систем є їх здатності надавати універсальні та високоточні геопросторові дані, що є критично важливим для визначення місця розташування об'єктів, навігації, визначення точного часу, моніторингу, тощо. Універсальність систем супутникової навігації дозволяє їх використовувати у різних сферах людської діяльності: транспорті та логістиці, геодезії та картографії, землеустрої, сільському господарстві, туризмі, рятувальній та військовій справах. Супутникова навігація є фундаментальною технологією XXI століття, що стала невід'ємною частиною інфраструктури, економіки та повсякденного життя.

Зв'язок теми з важливими науково-практичними завданнями. Попри свої переваги, у сучасних умовах глобальні навігаційні супутникові системи (GNSS) є вразливими до зовнішніх втручань, таких як spoofing («спуфінг» – підміна сигналів) і jamming («джеммінг» – глушіння сигналів). Такі дії можуть привести до небажаних наслідків, зокрема порушення навігації, втрати зв'язку або навіть аварій. Особливо критичною ця проблема є для автономних систем, де людський контроль обмежений, а точність позиціонування напряму впливає на безпеку функціонування [9, с. 584].

До 2000-х років системи супутникової навігації (особливо GPS) вважалися невразливими до значних електронних перешкод чи глушіння. Однак зростаюча кількість збоїв і втручання в діяльність цих систем підтверджують їх вразливість щодо зміни їх сигналів. Особливо загострилися ці тенденції під час російсько-української війни та інших конфліктів, коли військові з обох сторін використовували і досі використовують глушіння та спотворення супутникових систем з метою переваги на полі бою. Однак в останні роки втручання у роботу супутникової навігації створює суттєві проблеми для цивільного сектору. Його негативними наслідками стають збої у роботі транспорту (особливо авіаційного), інформаційних систем (прив'язаних до геопозиціонування – служби таксі, доставки, трансферу, туризм), систем мобільного зв'язку та інших галузей економіки.

Аналіз попередніх публікацій за темою дослідження. Тематиці проблем використання супутникових навігаційних систем у контексті сучасних викликів їх функціонування присвячено багато публікацій українських та іноземних науковців. У дослідженнях Петровського А.В., Волошин Д.Г., Бульби С.С. [2, 7], Нетаврованої А.Г. [5] описані методи та алгоритми виявлення перешкод у роботі навігаційних систем (передовсім, GPS). У публікації Мустафаєва О. В. [4] проаналізовано технології захисту від спотворення сигналів GPS.

Дослідники Radoš K., Brkić M., Begušić D. [16] розглядають методи виявлення перешкод і глушіння сигналів системи GPS, а Janiar S. та Wang P. [14] пропонують методи протидії GPS jamming. Alkhatib M. та інші [10] досліджують класифікацію атак на GPS, не використовуючи адаптивні методи. Mohanty A. та Gao G. [13] оглядають машинне навчання для покращення GNSS, не зосереджуючись на кіберзахисті.

Метою даної публікації є вивчення геопросторових проблем розвитку систем супутникової навігації у контексті їх використання у господарській та туристичній діяльності.

Виклад основного матеріалу. На сьогодні у світі використовується більше десятка різних супутникових навігаційних систем. Розглянемо найбільш поширені з них, які часто використовуються у різних сферах людської діяльності.

Найпоширенішою і найчастіше використовуваною глобальною навігаційною (геопозиційною) системою є американська система NAVSTAR/GPS (Global Positioning System). Вона складається з 32 супутників і космічних апаратів, які обертаються на навколоземних орбітах в 6 площинах на висоті близько 20 тисяч км.

Середня точність сучасних GPS-приймачів приблизно 5-8 метрів. На території США, Канади, Японії, КНР, Європейського Союзу та Індії є станції WAAS, EGNOS, MSAS й інші, які передають поправки для зниження похибки до 1-2 метрів на територіях цих країн. При використанні більш складних режимів точність визначення координат можна довести до 10 см [3].

Система NAVSTAR/GPS характеризується як максимально надійна, яка постійно оновлюється. Наприклад, відповідно до плану оновлення системи у 2010-2016 роках на орбіту виведені дванадцять супутників нової версії GPS IIF. З 2018 по 2023 роки було поповнено угруповання 8 супутниками у версії GPS III. Планується також з 2025 по 2034 роки на орбіту вивести ще 24 супутника в версії GPS IIIF. І запусками сучасних супутників система вдосконалюється в контексті захисту від перешкод і збоїв у роботі.

Інфраструктура російської системи ГЛОНАСС представлена 28 космічними апаратами, з яких 24 використовуються за цільовим призначенням. На даний момент один апарат тимчасово виведений на техобслуговування. Ще по одному знаходяться в орбітальному резерві, на етапі введення в систему і на етапі льотних випробувань.

Навіть з повідомлень офіційних російських джерел у ГЛОНАСС дуже багато проблем. Наприклад, ще досі в другій і третій орбітальних площинах немає резервних супутників. Близько половини супутників відпрацювали гарантійний термін. Виникають питання також щодо надійності цієї системи. 2 квітня 2014 року відбувся великий збій в роботі навігаційної системи ГЛОНАСС. Протягом майже 11 годин усі 24 супутники системи видавали некоректні дані, тобто система виявилася непрацездатною. У середині лютого 2016 року подібна ситуація повторилась – система ГЛОНАСС перестала функціонувати на деякий час. Залишається актуальним питання надійності роботи цієї системи [3].

Європейська глобальна навігаційна система Galileo є сумісною з супутниковими навігаторами GPS і ГЛОНАСС, однак не контролюється військовими. Щоправда, з 2008 року її дозволено використовувати для військових потреб щодо забезпечення європейської безпеки. На земній орбіті навігаційна система налічує 26 супутників, з яких поки функціонують 22 одиниці. Розробку навігаційної системи Galileo також фінансували Китай, Південна Корея, Ізраїль та Україна. Система має можливості для вирішення навігаційних завдань щодо будь-яких рухомих об'єктів з точністю менше одного метра. Загальна вартість цього міжнародного проекту становить близько 5 млрд. євро.

Китай реалізовує власну супутникову навігаційну систему – BeiDou (назва перекладається з китайської як "Північний ківш" або сузір'я Великої Ведмедиці). Китайська влада пояснює її розвиток необхідністю наявності власної системи, щоб не залежати від «ворожої» американської GPS. Китайська система BeiDou вважається єдиним потужним конкурентом для США. З 1989 р. вона пройшла три генерації і саме остання (BeiDou-3) безпосередньо конкурує з американською GPS, європейською Galileo і російською системою ГЛОНАСС. В системі Beidou-3 27 супутників Beidou-M, розташованих на середній круговій орбіті, п'ять супутників Beidou-G на геостаціонарній орбіті і ще три супутники Beidou-IGSO, розташованих на геосинхронних похилих високих орбітах.

За офіційними даними, точність визначення координат об'єкту для військової сфери системою Beidou становить до 2 м, для цивільної – до 10 м. Деякий час назад на навколоземну орбіту Китай вивів черговий супутник навігаційної системи Beidou - Qianqin II, в якому, як заявлено, використовується електронний чіп, що дозволяє визначати координати об'єкта з мінімальною похибкою [3].

У туристичній діяльності супутникові навігаційні системи використовують переважно у двох напрямах: використання туристичних карт і застосування геопозиціонування для орієнтування на місцевості.

Під час туристичних подорожей є актуальним встановлення свого місцезнаходження, зокрема географічних координат. Цього досягають з використанням GPS-навігації (хоча для таких потреб можна використовувати системи Galileo, Beidou). Власник приймача GPS або оснащеного ним смартфону може визначити своє місцезнаходження з точністю до кількох метрів – достатньо лише активізувати опцію GPS. Розташування користувача відображається на дисплеї смартфону (залежно від вибору), завантаженій карті чи космічному знімку. До того ж є змога визначення географічних координат, які ще можуть бути інформаційною складовою фотознімків [1, с. 80-81].

У самих подорожах поза відвідуваними територіями значне поширення набули GPS-навігатори, спеціально створені для туризму. Їх найголовнішими функціями є не лише велика точність позиціювання, а й фіксація пройденого маршруту, показ напрямку руху до заданої точки, розрахунок швидкості пересування, необхідного часу руху тощо. Окремо має бути згадана кнопка SOS, яка в туризмі не буває зайвою. Такі навігатори зазвичай виготовляють ударота водостійкими. Близькі функції мають GPS-трекери – пристрої, що показують пересування відповідного приладу. Це важливо в екстремальному туризмі, оскільки дає змогу моніторити рух людини чи групи туристів навіть тоді, коли вони свідомо не повідомляють про своє місцезнаходження [1, с. 81].

Багато видів людської діяльності (геодезичні вимірювання, землевпорядкування, військова справа, туризм, транспортна навігація) вимагають точної інформації про місцезнаходження певних об’єктів на земній поверхні, для чого використовуються глобальні навігаційні супутникові системи (GNSS) для визначення точного позиціонування (місця розташування), навігації та часу (PNT). Під загальним поняттям GNSS розуміють сукупність спеціалізованих супутників, які передають необхідні дані для навігації, позиціонування та визначення часу. Радіочастотні сигнали GNSS використовуються для навігаційних потреб у різних галузях господарства та військовій сфері (наземні та морські системи), які вимагають високої точності, доступності та надійності.

Збої, перешкоди та глушіння передачі сигналу GNSS можуть призводити до часткової

або повної втрати PNT, тобто навігація здійснюється наосліп. Зміни сигналів супутникових систем можуть бути як ненавмисними, так і навмисними. Було зафіксовано значну кількість випадків ненавмисного втручання у діяльність таких систем, наприклад від несправних телевізійних передавачів чи іншими джерелами передачі сигналів, які потрапляли у діапазони частот GNSS. Якщо змінений або спотворений сигнал зумисно передається в діапазоні частот GNSS, то таке явище називається глушінням (jamming). Більш поширеною та небезпечнішою загрозою для супутникової навігації є підробка сигналу (спуфінг, spoofing) (рис. 1). Тоді відбувається навмисне надсилання підроблених або спотворених сигналів GNSS на приймач, який вказує хибне положення користувача. Такий різновид загрози небезпечний у критично важливих безпекових програмах у різних сферах людської діяльності (особливо військова, транспорт, геодезія), які покладаються на точне позиціонування у режимі реального часу.

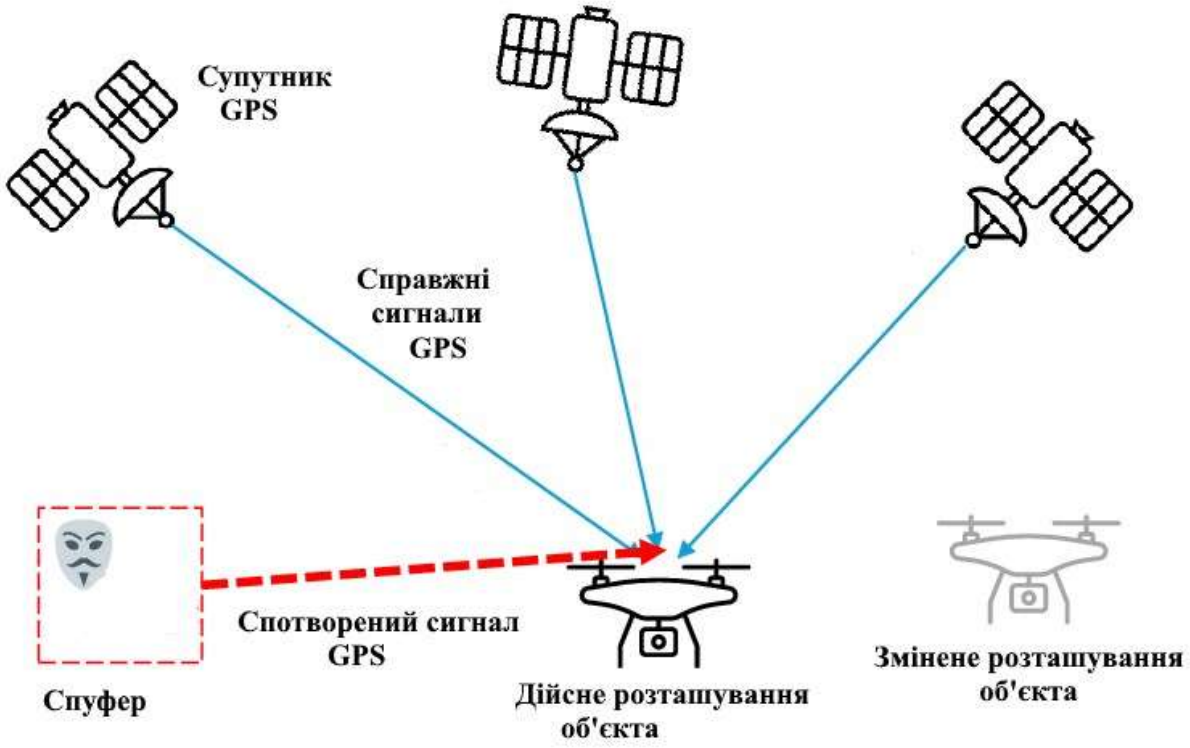

Рис. 1. Схема спотворення сигналу навігаційної системи GPS (спуфінг GPS)

Головною відмінністю між спуфінгом і глушінням з точки зору користувача є вплив, який він має на здатність приймача надавати PNT. Перешкоди у роботі навігаційних систем проявляються як втрата інформації PNT, оскільки їх сигнал перекривається перешкодами. Відповідно з точки зору користувача спуфінг GNSS викликає більше проблем, бо на відміну від глушіння, він не знає, що його обманюють. Переважно глушіння супутникових систем здійснюється через перевантаження приймача GNSS сигналами більшої потужності радіочастот. Хоча така діяльність у більшості країн світу є незаконною, однак передавачі перешкод малої потужності можна вільно придбати в Інтернеті та використовувати у своїх цілях. Можливості простого малопотужного передавач перешкод можуть спотворити сигнали GNSS на значній території.

Спуфінг часто є двоетапним процесом. На першому етапі використовуються перешкоди які заважають приймачу здійснювання відстеження автентичних сигналів GNSS, а потім використовується радіопередавач для надсилання хибних сигналів цільовому приймачу. Помилкові сигнали можуть бути створені генератором сигналів або ретрансляцією записаних сигналів GNSS, що називається meaconing [8].

Глушіння здійснюються шляхом перевантаження приймача GNSS радіочастотними сигналами більшої потужності. Незважаючи на те, що в більшості країн це незаконно, малопотужні передавачі перешкоди, відомі як «пристрої конфіденційності», можна придбати в Інтернеті та використовувати для цієї мети. Навіть простий передавач перешкод може подавити сигнали GNSS на великій території, зриваючи PNT. Ефективність засобів перешкод в першу чергу залежить від їх вихідної потужності та відстані до приймача супутникових сигналів. Іншими характеристиками передавачів перешкод є їх сигнали. Передають вони вузькосмугові

або широкосмугові завади, чи вони передаються у вигляді безперервної хвилі (на вибраній частоті, або у виді розгортки на заданому спектрі), або пульсують з певною швидкістю на нижчому рівні потужності [8].

Значною проблемою, яка загострюється в останні роки, є загрози та спотворення сигналів GNSS та пов'язаною з нею технології PNT. Вразливими до цього є зони бойових дій та морські прибережні регіони. Акваторії та узбережжя Чорного, Середземного та Балтійського морів, які насичені комерційною та промисловою активністю, а також військовими об'єктами, через прибережну та наземну діяльність часто піддаються загрозам в роботі GNSS через конкуренцію різних країн і військових блоків.

Вперше використання спуфінгу та глушіння сигналів супутникових систем було зафіксовано американськими військовослужбовцями у 2008 році. У 2012 році дослідники університету з Техасу експериментальним шляхом довели можливість перехоплення керування безпілотним апаратом через спуфінг. Ці дослідження були проведені у контексті розслідування подій 2011 року, коли в результаті хакерської атаки було втрачено безпілотник Lockheed, який помилково приземлився на іранський аеродром.

Навесні 2019 р американська неурядова організація C4ADS заявила, що росія використовує технології по дезорієнтації системи супутникової навігації GPS у тимчасово окупованому Криму. За даними наукового сенсора Міжнародної космічної станції, організації вдалося ідентифікувати діяльність, яка представляє значну загрозу для GPS-систем цивільних авіаліній в регіоні. Крім цього, аналітики виявили безліч прикладів діяльності щодо перешкоджання роботі Глобальної навігаційної супутникової системи GNSS на території росії, на окупованих територіях України і на військових об'єктах за кордоном. Всього було виявлено 9883 випадки російського втручання в роботу GNSS в 10 місцях, які вплинули на роботу навігаційних систем 1311 цивільних кораблів. Дослідники також зафіксували спотворення сигналів GPS на територіях, де росія проводить активні бойові дії або навчання [3].

У січні 2024 р. над північною частиною Польщі та прилеглою до неї акваторією Балтійського моря зник сигнал навігаційної системи GPS (рис. 2). Це призвело до збоїв у роботі авіаційного, морського, автомобільного транспорту, служб доставки й таксі, роботи мереж мобільного зв'язку та інших. Європейські та польські експерти з кібербезпеки пов'язували збої у роботі навігаційних систем із військовими навчаннями збройних сил росії у Калінінградській області, яка межує з Польщею. Подібні проблеми з сигналами GPS неоднора-зово повторювалися в акваторії Балтійського моря та в північних регіонах Польщі літом і восени 2025 р.

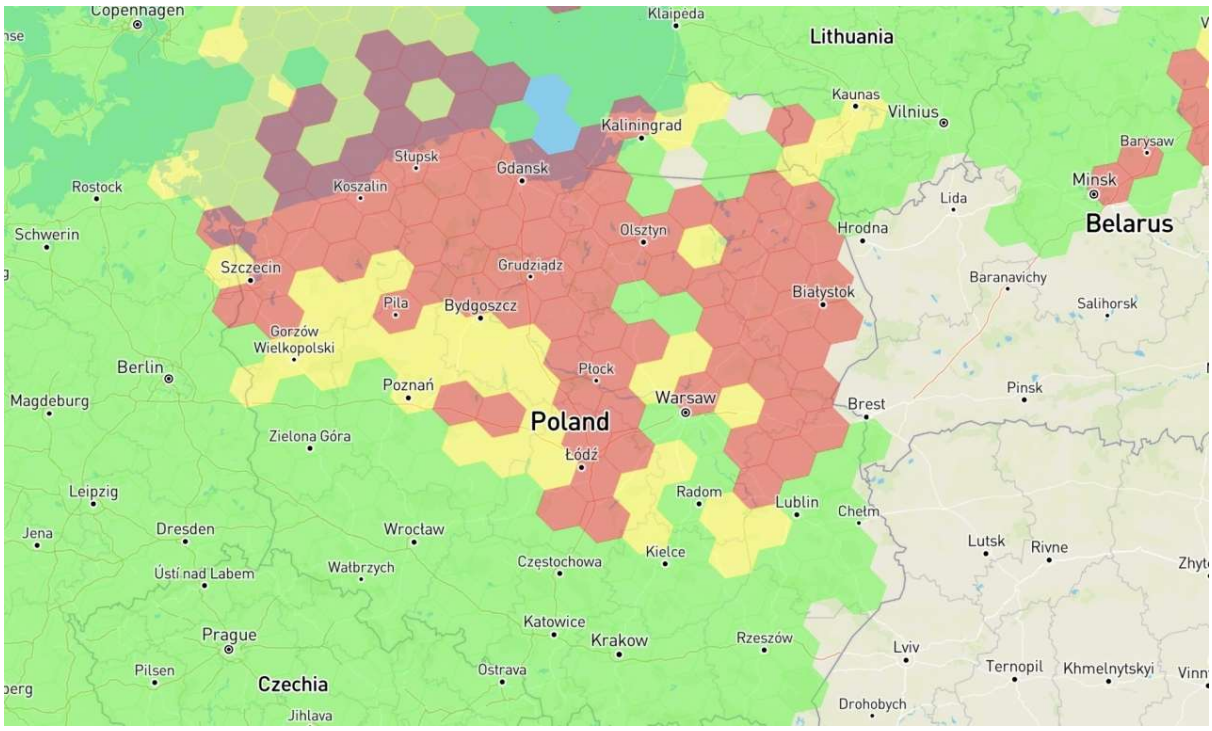

Рис. 2. Картосхема зон на території Польщі, де був відсутній сигнал навігаційної системи GPS 17 січня 2024 р. (джерело: https://epoznan.pl/) [18]

У вересні 2025 року на території Болгарії пропав сигнал системи GPS, внаслідок чого

виникли проблеми з посадкою літака президентки Єврокомісії Урсули фон дер Ляєн. Лише за чотири місяці 2025 року 122,6 тисячі авіарейсів на півночі Європи зіткнулися з перешкодами в роботі GPS та інших супутникових систем з вини Росії. Представники цих країн зазначили, що така ситуація становить серйозну загрозу для міжнародної авіаційної безпеки [6].

Перспективи використання результатів дослідження. У контексті розвитку туристичної діяльності вплив на системи супутникової навігації теж має певні ризики та загрози. Наприклад, через спуфінг і глушіння системи GPS можуть виникати збої у роботі авіаційного транспорту, який здійснює вагому частину туристичних перевезень. Втручання у роботу навігаційних систем також негативно впливає діяльність у сфері спортивного та екстремального туризму. Через змінений або заглушений сигнал GPS чи іншої системи групи туристів можуть втратити траси маршрутів, що створює загрози для їх безпеки.

Для запобігання спотворенню та перетворенню сигналів навігаційних супутникових систем проводять ряд заходів із посилення їх стійкості. Наприклад, аналіз потужності та коригування сигналу, використання мультичастотних і багатосистемних приймачів, фільтрація сигналів з допомогою штучного інтелекту, інтеграція з інерційними навігаційними системами [4, с. 60].

Удосконалені GNSS-приймачі містять фірмові алгоритми мікропрограм або цифрові фільтри, які можуть виявляти та видаляти заважаючі сигнали, зменшуючи їх потужність. Вони включають позасмугові сигнали, а також сигнали внутрішньосмугових перешкод більшої потужності [8].

Навігаційна система GPS для запобігання перешкодам у сигналах комплектується супутниками новіших поколінь, випромінювання від яких є набагато стійкішим проти глушіння чи підміни даних. Планується також запуск нових коригувальних станцій для поліпшення якості сигналів і боротьби з їх спотворенням.

Висновки. Системи супутникової навігації здобули значне поширення у сучасному цифровому світі. Вони використовуються у різних галузях господарства, однак наймасовіше на транспорті, туризмі та у військовій сфері. Найбільш поширеними у світі є навігаційні системи GPS (США), Galileo (країни ЄС), Beidou (Китай), ГЛОНАСС (росія). В останні роки використання супутникових навігаційних систем зіткнулося із перешкодами у їх роботі. Найпоширенішими є них є спуфінг (підміна координат) і глушіння (пропадання супутникового сигналу). Особливо кількість цих перешкод зросла в останні роки на території країн Центральної Європи, що пов'язано з деструктивною діяльністю російських збройних сил. Розробляються та впроваджуються сучасні методи боротьби з спотворенням та перетворенням сигналів навігаційних супутникових систем.

Література:

1. Вишневський В.І. Використання космічних та інформаційних технологій в екскурсійно-туристичній діяльності. Вісник Київського університету імені Тараса Шевченка. Географія. 2018. Вип. 1 (70). С. 79–83.
2. Волошин Д. Г., Бульба С. С. Інтелектуальний метод виявлення спуфінгу БПЛА. Сучасні інформаційні системи, 2022. Вип. 6(1), С. 88–96. https://doi.org/10.20998/2522-9052.2022.1.155.
3. Глобальні навігаційні системи – роль в сучасних військових конфліктах. URL: https://defence-ua.com/army_and_war/globalni_navigatsijni__sistemi_rol__v_suchasnih_vijskovih_konfliktah-2538.html (дата звернення: 22.10.2025).
4. Мустафаєв О. В. Сучасні технології захисту від GPS спуфінгу у системах навігації. Вчені записки ТНУ імені В. І. Вернадського. 2024. Серія: Технічні науки, 35(74), № 5, С. 58–61. https://doi.org/10.32782/2663-5941/2024.5.1/106.
5. Нетаврована, А. Геометричний метод визначення GPS spoof атак на безпілотні літальні апарати. Матеріали конференцій МЦНД (22.12.2023, Одеса, Україна). URL: https://archive.mcnd.org.ua/index.php/conference-proceeding/article/view/954 (дата звернення: 24.10.2025).
6. *Нова загроза: у Європі тисячі рейсів зіткнулися з проблемами навігації через глушіння GPS Росією. URL: https://epravda.com.ua/svit/u-yevropi-tisyachi-reysiv-zitknulisya-z-problemami-navigaciji-cherez-glushinnya-gps-rosiyeyu-811305/ (дата звернення: 25.10.2025).*
7. Петровський А. В. Алгоритм виявлення впливу спуфінгу під час виконавчої прокладки програмними засобами електронної картографічної навігаційно-інформаційної системи. Проблеми інформаційних технологій, 2019. Вип. 25, С. С. 30–38. https://doi.org/10.35546/2313-0687.2019.25.30-384.
8. Підроблено (spoofed) чи заглушено (jammed)? URL: https://cms.eps.com.ua/uploads/Hexagon_Nov_Atel_Spoofed_or_Jammed_ukr_compressed_30667109a0.pdf (дата звернення: 25.10.2025).
9. Снєосіков, О. Методи виявлення та протидії кібератакам типу gps spoofing і gps jamming з використання AI для систем диференційної корекції та глобальної навігаційної супутникової системи. Herald of Khmelnytskyi National University. Technical Sciences. 2025. 355(4), С. 584-592. https://doi.org/10.31891/2307-5732-2025-355-82
10. Alkhatib, M., McCormick, M., Williams, L., Leon, A., Camerano, L., Al, K., Devabhaktuni, V. K., Kaabouch, N., Svm, D., & Regularization, L. (2024). Classification and source location indication of jamming attacks targeting UAVs via multi-output multiclass machine learning modeling. 2024. IEEE International Conference on Consumer Electronics (ICCE). P. 1–5).

11. Bhatti J. A., Humphreys T. E. Hostile control of ships via false GPS signals: Demonstration and detection. Journal of the Institute of Navigation. № 64(1). 2017. P. 51 – 66. URL : https://doi.org/10.1002/navi.183.
12. Broumandan A., Kennedy S. and Schleppe J. Demonstration of a Multi-Layer Spoofing Detection Implemented in a High Precision GNSS Receiver. IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 2020, pp. 538-547, doi: 10.1109/ PLANS46316.2020.9109842.
13. Mohanty, A., & Gao, G. A survey of machine learning techniques for improving global navigation satellite systems. EURASIP Journal on Advances in Signal Processing, 2024, P. 1–40. URL: https://asp-eurasipjournals.springeropen.com/counter/pdf/10.1186/s13634-024-01167-7.pdf (дата звернення: 20.10.2025).
14. Lianxiao Meng, Lin Yang, Wu Yang,Long Zhang. A survey of GNSS spoofing and anti-spoofing technology. MDPI. Vol. 14. № 19. 2022. P. 00 – 00. URL : https://doi.org/10.3390/rs14194826. (дата звернення: 18.10.2025).
15. Psiaki M., Humphreys T. GNSS spoofing and detection // Proceedings of the IEEE. 2016. T. 104. P. 1—13.
16. Radoš, K., Brkić, M., Begušić, D. Recent advances on jamming and spoofing detection in GNSS. Sensors, 2024, 24(13), P. 42. https://doi.org/10.3390/s241342108.
17. Siavash, J., & Ping, W. (2024). Intelligent anti-jamming based on deep reinforcement learning and transfer learning. IEEE Transactions on Vehicular Technology, 2024. 1–10. URL: https://doi.org/10.1109/TVT.2024.33594269.
18. Zakłócenia sygnału GPS nad Polską. Kłopoty również w naszym regionie. URL: https://epoznan.pl/news-news-147001-zaklocenia_sygnalu_gps_nad_polska_klopoty_rowniez_w_naszym_regionie (дата звернення: 25.10.2025).

References:

1. Vyshnevskyi V.I. Vykorystannia kosmichnykh ta informatsiinykh tekhnolohii v ekskursiino-turystychnii diialnosti. Visnyk Kyivskoho universytetu imeni Tarasa Shevchenka. Heohrafiia. 2018. Vyp. 1 (70). S. 79–83.
2. Voloshyn D. H., Bulba S. S. Intelektualnyi metod vyiavlennia spufinhu BPLA. Suchasni informatsiini systemy, 2022. Vyp. 6(1), S. 88–96. https://doi.org/10.20998/2522-9052.2022.1.155.
3. Hlobalni navihatsiini systemy – rol v suchasnykh viiskovykh konfliktakh. URL: https://defence-ua.com/army_and_war/globalni_navigatsijni__sistemi_rol__v_suchasnih_vijskovih_konfliktah-2538.html (data zvernennia: 22.10.2025).
4. Mustafaiev O. V. Suchasni tekhnolohii zakhystu vid GPS spufinhu u systemakh navihatsii. Vcheni zapysky TNU imeni V. I. Vernadskoho. 2024. Seriia: Tekhnichni nauky, 35(74), № 5, S. 58–61. https://doi.org/10.32782/2663-5941/2024.5.1/106.
5. Netavrovana, A. Heometrychnyi metod vyznachennia GPS spoof atak na bezpilotni litalni aparaty. Materialy konferentsii MTsND (22.12.2023, Odesa, Ukraina). URL: https://archive.mcnd.org.ua/index.php/conference-proceeding/article/view/954 (data zvernennia: 24.10.2025).
6. *Nova zahroza: u Yevropi tysiachi reisiv zitknulysia z problemamy navihatsii cherez hlushinnia GPS Rosiieiu. URL: https://epravda.com.ua/svit/u-yevropi-tisyachi-reysiv-zitknulisya-z-problemami-navigaciji-cherez-glushinnya-gps-rosiyeyu-811305/ (data zvernennia: 25.10.2025).*
7. Petrovskyi A. V. Alhorytm vyiavlennia vplyvu spufinhu pid chas vykonavchoi prokladky prohramnymy zasobamy elektronnoi kartohrafichnoi navihatsiino-informatsiinoi systemy. Problemy informatsiinykh tekhnolohii, 2019. Vyp. 25, S. S. 30–38. https://doi.org/10.35546/2313-0687.2019.25.30-384.
8. Pidrobleno (spoofed) chy zahlusheno (jammed)? URL: https://cms.eps.com.ua/uploads/Hexagon_Nov_Atel_Spoofed_or_Jammed_ukr_compressed_30667109a0.pdf (data zvernennia: 25.10.2025).
9. Cnieosikov, O. Metody vyiavlennia ta protydii kiberatakam typu gps spoofing i gps jamming z vykorystannia AI dlia system dyferentsiinoi korektsii ta hlobalnoi navihatsiinoi suputnykovoi systemy. Herald of Khmelnytskyi National University. Technical Sciences. 2025. 355(4), C. 584-592. https://doi.org/10.31891/2307-5732-2025-355-82
10. Alkhatib, M., McCormick, M., Williams, L., Leon, A., Camerano, L., Al, K., Devabhaktuni, V. K., Kaabouch, N., Svm, D., & Regularization, L. (2024). Classification and source location indication of jamming attacks targeting UAVs via multi-output multiclass machine learning modeling. 2024. IEEE International Conference on Consumer Electronics (ICCE). P. 1–5).
11. Bhatti J. A., Humphreys T. E. Hostile control of ships via false GPS signals: Demonstration and detection. Journal of the Institute of Navigation. № 64(1). 2017. P. 51 – 66. URL : https://doi.org/10.1002/navi.183.
12. Broumandan A., Kennedy S. and Schleppe J. Demonstration of a Multi-Layer Spoofing Detection Implemented in a High Precision GNSS Receiver. IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 2020, pp. 538-547, doi: 10.1109/ PLANS46316.2020.9109842.
13. Mohanty, A., & Gao, G. A survey of machine learning techniques for improving global navigation satellite systems. EURASIP Journal on Advances in Signal Processing, 2024, P. 1–40. URL: https://asp-eurasipjournals.springeropen.com/counter/pdf/10.1186/s13634-024-01167-7.pdf (дата звернення: 20.10.2025).
14. Lianxiao Meng, Lin Yang, Wu Yang,Long Zhang. A survey of GNSS spoofing and anti-spoofing technology. MDPI. Vol. 14. № 19. 2022. P. 00 – 00. URL : https://doi.org/10.3390/rs14194826. (data zvernennia: 18.10.2025).
15. Psiaki M., Humphreys T. GNSS spoofing and detection // Proceedings of the IEEE. 2016. T. 104. P. 1—13.
16. Radoš, K., Brkić, M., Begušić, D. Recent advances on jamming and spoofing detection in GNSS. Sensors, 2024, 24(13), P. 42. https://doi.org/10.3390/s241342108.
17. Siavash, J., & Ping, W. (2024). Intelligent anti-jamming based on deep reinforcement learning and transfer learning. IEEE Transactions on Vehicular Technology, 2024. 1–10. URL: https://doi.org/10.1109/TVT.2024.33594269.
18. Zakłócenia sygnału GPS nad Polską. Kłopoty również w naszym regionie. URL: https://epoznan.pl/news-news-147001-zaklocenia_sygnalu_gps_nad_polska_klopoty_rowniez_w_naszym_regionie (data zvernennia: 25.10.2025).

Надійшла до редакції 05.11.2025 р.
Прийнята до друку 19.11.2025 р.
Опублікована 29.12.2025 р.