The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

Received: *March 2, 2026* | **Revisions Requested:** - | **Revision Received:** -
Accepted: *May 8, 2026* | **Published Online:** *August 5, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.2.17

Інтелектуальний спосіб протидії безпілотним літальним апаратам противника з LTE-модемами на основі виявлення поточних аномалій траєкторних параметрів

Ігор Шовкошитний
доктор технічних наук, старший науковий співробітник
головний науковий співробітник Центру воєнно-стратегічних досліджень
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: igor65@meta.ua
ORCID: 0000-0001-9245-4111

Олексій Муромець
ад'юнкт
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: alexlesli77733@gmail.com
ORCID: 0000-0001-9940-511X

Ольга Василенко
доктор філософії
ад'юнкт
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: nicety@ukr.net
ORCID: 0000-0003-2633-0131

Дмитро Бровченко
молодший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: brovchenkodmitry@gmail.com
ORCID: 0009-0001-2665-5836

Анотація. У статті розглядається проблема протидії ударним безпілотним літальним апаратам противника, оснащеним LTE-модемами. Такі апарати здатні передавати відео в реальному часі або в записі через мобільні базові станції національних операторів зв'язку, а також отримувати команди для коригування курсу. Показано, що широке застосування мереж 4G/LTE для дистанційного керування, коригування траєкторії та передавання розвідувальної інформації суттєво знижує ефективність традиційних засобів радіоелектронної боротьби. Розглянуто обмеження класичних підходів щодо протидії безпілотним літальним апаратам

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

типу «Shahed» та обґрунтовано необхідність переходу до гнучких організаційно-технічних заходів. Мета статті – розробити інтелектуальний спосіб виявлення, локалізації та селективної нейтралізації безпілотних літальних апаратів з LTE-модемами на основі оперативного аналізу поточних аномалій траєкторних параметрів. Запропоновано комплексний підхід, що поєднує аналітичні методи, формальну та нечітку логіку, нейромережеві моделі штучного інтелекту для виявлення аномалій траєкторних параметрів за даними позиціювання SIM-карток у стільниковій мережі. Розроблено набір критеріїв аномальності: просторові координати, абсолютна та відносна швидкість, курс, швидкість зміни курсу, а також комбіновані індикатори поведінкових відхилень. Описано алгоритм інтелектуального способу протидії, що базується на оперативному аналізі поточних аномалій траєкторних параметрів рухомих об’єктів. Запропоновано алгоритм селективного блокування доступу аномальних об’єктів до мережевих сервісів без загального відключення базових станцій. Метод дозволяє реалізувати вибіркові заходи протидії – адресне блокування передачі даних, деактивацію сервісів – із мінімальними наслідками для цивільної інфраструктури. Дослідження демонструють, що запропонований інтелектуальний підхід забезпечує високу ефективність нейтралізації загроз від безпілотних літальнів апаратів зі збереженням функціональності мережі та зниженням ризиків для цивільних сервісів. Надано рекомендації щодо інтеграції запропонованих алгоритмів у системи мережевого менеджменту (NMS) операторів, створення правових механізмів для оперативного блокування International Mobile Subscriber Identity (Міжнародний ідентифікатор мобільного абонента) та регулярного перенавчання ML-модулів. Розроблений спосіб є придатним для практичного впровадження в системах захисту об’єктів критичної інфраструктури.

Ключові слова: безпілотний літальний апарат, LTE-модем, оператор мобільного зв’язку, стільникова мережа, аномалія траєкторних параметрів, протидія безпілотним літальним апаратам.

Вступ (Introduction)

Із початку широкомасштабної агресії росії проти України у 2022 році значно зросли масштаби застосування противником ударних безпілотних літальних апаратів (БпЛА), які становлять загрозу не лише для військ, а й більшою мірою для об’єктів критичної інфраструктури в глибині контрольованої Україною території. При цьому динаміка застосування таких БпЛА та рівень руйнівних наслідків постійно зростають. Найбільш поширеними засобами ураження, які застосовує противник для здійснення терористичних атак, є ударні БпЛА типу “Shahed-131” (“Герань-1”), “Shahed-136” (“Герань-2”), “Shahed-238” (“Герань-3”), характеристики і способи використання яких безперервно еволюціонують. Крім покращення ударних властивостей ударних безпілотних систем, значну увагу противник приділяє підвищенню стійкості бортового обладнання до радіоперешкод, адаптивності до поточної обстановки та керованості за межами прямої радіовидимості, яка для наземної станції управління не перевищує 150–170 км. Особливо показовою є еволюція технічних параметрів бортового обладнання БпЛА сімейства “Shahed”, а також способів його використання. Зокрема, спостерігається поступовий перехід від простого традиційного навігаційного обладнання до комплексних бортових систем автономної навігації, зв’язку та управління. Перші зразки БпЛА “Shahed-131/136” іранського виробництва передбачали наведення за допомогою комбінації інерційної системи та GPS-навігації, що обмежувало завдавання противником ударів виключно по цілях із фіксованими заздалегідь відомими координатами [1]. Проте із розвитком засобів радіоелектронної боротьби (РЕБ) та розгортанням просторово-розподілених систем радіоелектронної протидії (типу російської системи “Поле-21” та вітчизняної системи “Покрова”), ефективність застосування таких БпЛА певною мірою

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

знизилась. Це спонукало противника до пошуку дієвих способів підвищення керованості (на значному віддаленні від точки запуску / управління) та завадозахищеності ударних БпЛА. З цією метою ворог намагався підвищувати перешкодозахищеність бортових систем управління та наведення БпЛА завдяки: експериментам із цільовим навантаженням (з комбінуванням оптико-електронних датчиків денного / нічного бачення); упровадженню CRPA-антен з адаптивною діаграмою спрямованості, які суттєво зменшили вплив сигналів завад бортовим засобам супутникової радіонавігації. Від початку 2023 року для забезпечення керованості ударних БпЛА на значних відстанях противник експериментує із альтернативними системами наведення [2, 3], комбінуючи базові способи гіроскопічного і GPS-позиціювання з різними способами дистанційного управління ударними БпЛА сімейства “Shahed”. Оскільки традиційний підхід до забезпечення дальнього управління БпЛА за допомогою мережі наземних (повітряних) радіоретрансляторів (зокрема MESH-мереж) є доволі складним та не завжди надійним у бойових умовах (ефективна відстань між ретрансляторами не перевищує 150 км), противник обрав інший підхід, який виявився доволі ефективним і полягав у використанні наявної мережі базових станцій стільникового радіозв’язку для передавання команд управління та інформації з бортових датчиків БпЛА на пункти управління, що розташовані в будь-якій точці непідконтрольної окупованої території або у росії. З цього самого періоду на БпЛА “Shahed” ворог починає епізодично експериментувати з модемами 4G-зв’язку з антенами MIMO та SIM-картками оператора “Київстар” (від передавання SMS із поточними координатами до потокового відео з бортових камер через telegram-канали). БпЛА з LTE-зв’язком можуть виконувати функції розвідника, ударного засобу або хибної цілі для перевантаження української ППО. LTE-модем є компактним електронним пристроєм, що працює зі стільниковими мережами 4-го покоління (4G LTE) та забезпечує високошвидкісний доступ до мережі Інтернет [4].

Останні модифікації БпЛА “Shahed” (які починаючи з серпня 2025 року застосовуються противником для руйнування об’єктів критичної інфраструктури) вже обладнують камерою та двома LTE-модемами, які дозволяють передавати відео в реальному часі або в записі через мобільні базові станції, а також отримувати команди для коригування курсу. В ударній версії камера (за умови зміни кута огляду) та віддалене керування можуть використовуватись для наведення на ціль оператором за принципом FPV-БпЛА [2]. При цьому передавання даних може бути здійснене через:

ланцюг базових станцій українських операторів стільникового зв’язку, з урахуванням роумінгу з під’єднанням до мереж стільникового зв’язку сусідніх держав;

ланцюг базових станцій операторів стільникового зв’язку сусідніх країн (в прикордонних районах можливе використання LTE-модемів із SIM-картками російського оператора “Теле2” (t2), які успішно працюють у роумінгу через мережі сусідніх країн) [5];

найближчі базові станції з виходом із них на інтегровані з ними термінали супутникового зв’язку.

Масштабність проблеми підтверджується даними служби державного фінансового моніторингу, якою спільно зі Службою безпеки України в період із середини 2025 року по травень 2026 року було розкрито групу осіб-підприємців та приватних осіб, причетних до закупівлі (за дроп-схемами), активації та передачі українських SIM-карт противнику для подальшого їх використання в БпЛА з метою забезпечення зв’язку, навігації й точного наведення на об’єкти критичної інфраструктури. Загалом було виявлено понад 29 тисяч мобільних номерів і транзакцій на суму понад 60 млн гривень.

Застосування противником LTE-мереж національних операторів стільникового зв’язку, експерименти з активацією SIM-карток (зокрема в умовах роумінгу) та маршрутизація через мережі стільникового зв’язку сусідніх держав дозволяють суттєво подовжити оперативний радіус управління ударними БпЛА, обходячи проблему управління ними, зумовлену

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

дальністю радіогоризонту. Це відкриває можливість для стійкої двосторонньої передачі потокового відео й команд управління в реальному часі, що фактично дає змогу перетворити найбільш масові ударні БпЛА на FPV-платформи великого радіуса дії. Отже, такий спосіб управління застосуванням противником ударних БпЛА створює значну загрозу як для військових, так і для цивільних об’єктів. Також слід зазначити, що умовах масового використання в ударних БпЛА LTE-модемів наявні засоби РЕБ стають менш ефективними, а спосіб відключення інтернету на вежах стільникових операторів під час повітряної тривоги, який періодично пропонується унормувати у законодавчому полі [6], є радикальним та не вибірковим і може призвести до небажаних побічних ефектів. Наразі превентивне відключення базових станцій у зонах можливого прольоту БпЛА здійснюється в межах спеціальних заходів з безпеки за вказівкою відповідних органів військового управління. Проте такі рішення мають серйозні соціально-економічні та безпекові наслідки, адже можуть ускладнювати роботу спеціальних служб та ускладнити функціонування багатьох важливих сервісів, наприклад, екстрених служб і онлайн-сервісу “е-ППО” під час оголошення повітряної тривоги.

Отже, виникає наукова та прикладна задача – розроблення спеціальних методів (способів), що забезпечать виявлення та адресну нейтралізацію загроз використання противником мереж стільникового зв’язку національних операторів для навігації розвідувальних і ударних дистанційно-керованих безпілотних комплексів та віддаленого управління ними зі збереженням стійкої роботи інфраструктури мереж стільникового зв’язку. Особливий інтерес представляють підходи, що базуються на аналізі та виявленні аномалій траєкторних параметрів рухомих об’єктів, які переміщуються в межах зон радіопокриття стільникових мереж: вони дозволяють інтерпретувати поведінкові ознаки підозрілих платформ та реалізувати вибіркові заходи з обмеження доступу до мережевих сервісів без загального відключення (блокування) інфраструктури для звичайних абонентів. У статті обґрунтовано необхідність переходу від використання суто традиційних методів і засобів радіоелектронного подавлення бортового обладнання динамічних об’єктів (зокрема БпАК противника) до організаційно-технічних механізмів виявлення та блокування мережевих сервісів для аномальних об’єктів, а також запропоновано інтелектуальний підхід для практичної реалізації цих ідей.

Методологічна основа (Methodological Framework)

В основу дослідження покладено термінологічний апарат, у центрі якого розглядається таке поняття, як “аномалія траєкторних параметрів” (anomalies of trajectory parameters), під якою, відповідно до [4, 5], мають на увазі сукупність значень динамічних характеристик об’єкта, що виходять за межі статистично обґрунтованої норми для заданого класу об’єктів.

Методологічна основа дослідження ґрунтується на концепті виявлення та ідентифікації поточних аномалій траєкторних параметрів динамічних об’єктів (зокрема БпЛА) за допомогою аналізу даних їхнього позиціювання. Оскільки управління БпЛА здійснюється через LTE-модеми, методологія спирається на здатність національних операторів мобільного зв’язку відстежувати переміщення активних SIM-карток у зонах покриття базових станцій операторів стільникового зв’язку. Для виявлення та швидкого оцінювання відхилень (аномалій) запропоновано використовувати комплексний методичний і алгоритмічний підхід, який поєднує аналітичні методи, методи формальної та нечіткої логіки, а також навчені нейромережеві моделі (штучний інтелект). Такий підхід адаптує методи, які перевірені та використовуються у суміжних предметних галузях, зокрема для аналізу відхилень траєкторій космічних апаратів, виявлення геодинамічних аномалій у часових рядах GNSS за допомогою машинного навчання, а також у системах адресно-часової селекції для захисту мережевого трафіка від кіберзагроз [4]. Завдяки такій інтеграції методів може бути реалізовано

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

інтелектуальний спосіб автоматизованого виявлення та ідентифікації поточних аномалій траєкторних параметрів динамічних об'єктів (поведінки БпЛА противника з LTE-модемами) та оперативного ухвалення рішень щодо протидії таким об'єктам.

Результати та обговорення (Results and Discussions)

Слід зазначити, що подальше використання противником LTE-модемів у системах управління ударних БпЛА зумовлено низкою переваг LTE-мереж, якими прогнозовано слід вважати:

можливість керування БпЛА на значних відстанях, що не можна здійснити у разі використання традиційних радіоканалів, які обмежуються дальністю прямої радіовидимості;

високу надійність і стабільність LTE-зв'язку порівняно з радіоуправлінням, що особливо важливо у разі застосування ударних БпЛА в умовах міської забудови (де можлива наявність значної кількості зон радіотіні компенсується зонами впевненого покриття завдяки розгалуженій інфраструктурі ретрансляторів стільникового зв'язку національних операторів) або складного рельєфу, де можливі додаткові радіоперешкоди у зв'язку з багатопроменевим поширенням радіохвиль;

об'єктивну неможливість застосування засобів РЕБ підрозділами сил оборони України для радіоподавлення мереж власних LTE-ретрансляторів або базових станцій;

високу стійкість та обчислювальну потужність локальної LTE-мережі у разі об'єднання ударних БпЛА з відповідними модемами у групи (рої), адже нині такі БпЛА все частіше оснащують швидкодіючими процесорами та для реалізації спеціальних алгоритмів на основі штучного інтелекту, що дозволяє їм через LTE-мережі обробляти дані в реальному часі, аналізувати відео та самостійно виконувати завдання.

З огляду на зазначене, в основу запропонованого авторами інтелектуального способу протидії БпЛА противника з LTE-модемами на основі виявлення поточних аномалій траєкторних параметрів покладено низку логічних висновків та припущень:

противник і надалі зберігатиме інтерес до цієї технології в контексті диверсифікації способів позиціювання та управління ударними БпЛА;

оператори стільникового зв'язку завдяки застосуванню програмно-апаратних засобів можуть здійснювати моніторинг переміщення SIM-карток між сегментами покриття ("стільниками") із просторовою точністю від 20 до 2000 метрів залежно від щільності базових станцій та швидкості об'єкта (ударного БпЛА з LTE-модемом);

носії LTE-модемів (ударні БпЛА) можуть бути виявлені та ідентифіковані операторами стільникового зв'язку за низкою параметрів руху, які відрізняються від подібних параметрів типових динамічних об'єктів;

виявлені та ідентифіковані поточні аномалії параметрів динамічних об'єктів (відхилення їхньої траєкторії по GPS-координатах) можуть бути використані для припинення доступу "аномальних" об'єктів до мережевих сервісів.

Прототипами інтелектуального способу є відомі підходи до вирішення проблеми в певній галузі на основі виявлення аномалій. Наприклад, у [7] розглядається "аномалія траєкторії" космічних апаратів як відхилення від очікуваної траєкторії та аналізується вплив неочікуваних прискорень. У [8] автор розглядає геодинамічні "аномальні відхилення" (просторові та висотні зміни, які не відповідають очікуваним) у часових рядах GNSS, використовуючи методи машинного навчання. У [6] подібна ідея застосована у сфері захисту інформаційно-телекомунікаційних систем від потенційних кіберзагроз. Зокрема, авторами запропоновано автокомпенсаційний принцип "адресно-часової селекції" для виділення та нейтралізації аномалій мережевого трафіка. У контексті обраної тематики важливим є уточнення таких понять, як:

"аномалія" – точка або набір точок, які відносно віддалені від інших точок у

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

багатовимірному просторі ознак);

“аномалії” – закономірності в даних, які не відповідають чітко визначеному поняттю нормальної поведінки [9];

“аномалії траєкторних параметрів” (anomalies of trajectory parameters) – відхилення руху об’єкта (зокрема БпЛА, ракети, літака чи супутника) від його нормальної, розрахованої або прогнозованої траєкторії.

Поведінка динамічного об’єкта може вважатись нормальною, якщо його ключові траєкторні параметри знаходяться в межах визначених допустимих діапазонів. Аномалії траєкторних параметрів об’єктів проявляються у будь-яких змінах, що виходять за межі допустимих відхилень. Для динамічних об’єктів типовими траєкторними параметрами зазвичай є положення (координати) та швидкість (вектор і модуль швидкості; прискорення).

Відстеження параметрів переміщення будь-якого динамічного об’єкта-носія LTE-модема із SIM-карткою може здійснюватись за набором траєкторних параметрів її носія: положення (площинні координати x, y і висота h); швидкість (v); курсовий параметр (k); швидкість зміни курсу (ω). Оператор стільникового зв’язку може визначати та вимірювати траєкторні параметри носія LTE-модема з активною SIM-карткою незалежно від того, чи здійснюється передавання чи приймання інформації LTE-модемом (для відстеження активної SIM-карти в мережі 4G (LTE) активна передача користувацького трафіка не є необхідною). Для визначення траєкторних параметрів модема може використовуватись:

його ідентифікація за IMEI (International Mobile Equipment Identity) – унікальним міжнародним ідентифікатором мобільного пристрою;

постійна реєстрація модема в мережі (Idle Mode) – повідомлення про присутність у мережі; тріангуляція модема (Cell-ID);

сигнальний трафік (обмін службовими повідомленнями між модемом і базовими станціями навіть в режимі очікування);

визначення координат модема за оцінками часу проходження сигналів до веж стільникового зв’язку.

Для виявлення “аномальних” динамічних об’єктів розроблено систему критеріїв, представлену в табл. 1. Відхилення від норми хоча б одного чи декількох найбільш важливих траєкторних параметрів (за критерієм “n із m”) свідчитиме про “аномалію траєкторних параметрів” БпЛА (носія LTE-модема з активною SIM-карткою), що буде підставою для вибіркового блокування доступу “аномального” об’єкта до мережевих сервісів, зокрема передачі даних через мережу ретрансляторів стільникового зв’язку.

Приклад аномальної поведінки динамічного об’єкта (БпЛА) наведено на рис. 1. Ідентифікація аномального динамічного об’єкта здійснюється за набором логічних правил (критеріїв “аномальності траєкторних параметрів”), зміст яких розглянуто вище. При цьому порядок застосування наведених у табл. 1 критеріїв траєкторних параметрів може бути довільний, проте логічно починати з першого критерію, який задає початкові умови (поточні координати перебування об’єкта) для всіх інших.

На підставі наведених вище міркувань розроблено загальну схему алгоритму інтелектуального способу протидії БпЛА противника з LTE-модемами на основі виявлення поточних аномалій траєкторних параметрів (рис. 2). Алгоритм реалізується як послідовність взаємопов’язаних кроків оброблення інформації, що формується в мережі стільникового зв’язку під час взаємодії між базовими станціями стільникового зв’язку та встановленим на БпЛА LTE-модемом із активною SIM-карткою.

На **першому кроці** алгоритму здійснюється збір первинної інформації про функціонування LTE-модема у мережі стільникового зв’язку. Ця інформація формується базовими станціями оператора стільникового зв’язку в процесі реєстрації, обслуговування та переміщення абонентського пристрою між зонами покриття (стільниками). До такої інформації належать:

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

ідентифікатор абонента (SIM-картки);
час підключення до базової станції;
ідентифікатор базової станції;
параметри радіосигналу;
службова інформація про хендовери (handover – процеси перемикання користувацького пристрою (модема) з однієї базової станції на іншу в мережах стільникового зв'язку, що дозволяє уникнути розриву з'єднання під час руху абонентського пристрою (термінала) між базовими станціями).

Таблиця 1. Критерії поточних аномалій траєкторних параметрів, які доцільно використовувати під час організації протидії БпЛА противника (авторська розробка)

Траєкторні параметри	**Критерій "аномальності траєкторних параметрів" (умова блокування передавання даних / доступу об'єкта до мережевих сервісів)**
Положення об'єкта (його площинні координати x, y і висота h), м	Об'єкт у забороненій зоні – область простору Ω_{xyh}, в якому знаходиться об'єкт (БпЛА противника) з координатами (x, y, h), входить в область простору Ω, в якій перебування заборонене. $\Omega_{xyh} \subseteq \Omega$
Швидкість (v), км/год	Швидкість об'єкта перевищує максимально можливу для цього класу об'єктів ($v>V_{max}$). БпЛА часто рухаються вздовж автошляхів, імітуючи наземні засоби. Проте для БпЛА "Shahed" V_{max} v~180–185 км/ч, тоді як для більшості наземних засобів швидкість практично не перевищує V_{max}~150 км/ч (залежить від категорії і якості автомобільних шляхів).
Курсовий параметр (k)	Цей параметр широко використовується у розрахунках наведення зброї й дає змогу визначити точку, у якій ціль буде знаходитись в момент влучання. Тобто аномальним може бути визнано об'єкт, який прогнозовано рухається в бік важливого (критичного) об'єкта або рухається за межами доріг (автошляхів) чи в місцевості, де знаходження (пересування наземних (надводних) засобів неможливо в силу геофізичних особливостей.
Швидкість зміни курсу (ω), (°/с) або радіан/с	$\omega>\omega_{max}$, де ω_{max} – максимальна кутова швидкість, з якою об'єкт може змінювати свій курс. Тобто об'єкт, який різко та часто змінює курс (маневрує), особливо за межами автошляхів або дозволених коридорів польоту, є аномальним.

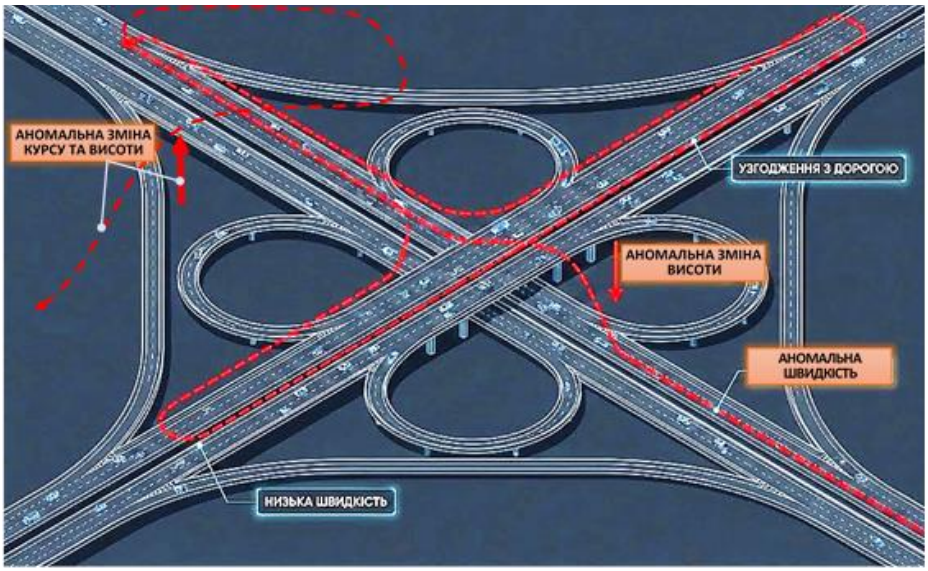


Рисунок 1. Приклад аномальної поведінки динамічного об'єкта (БпЛА)
На основі цих даних формується часова послідовність переміщення SIM-картки в мережі стільникового зв'язку

The Central Research institute
of the Armed Forces of Ukraine
ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

На **другому кроці** здійснюється визначення поточних траєкторних параметрів носія LTE-модема. Для цього використовується інформація про географічне розташування базових станцій та часові інтервали між підключеннями. У результаті обчислюються такі параметри руху об'єкта:

поточні координати об'єкта – x, y, h;

швидкість переміщення (v);

курсовий параметр (k);

швидкість зміни курсу (ω).

Отже, SIM-картка інтерпретується як датчик руху об'єкта, що дозволяє відстежувати його поведінку у просторі через інформацію щодо зміни поточних координат.

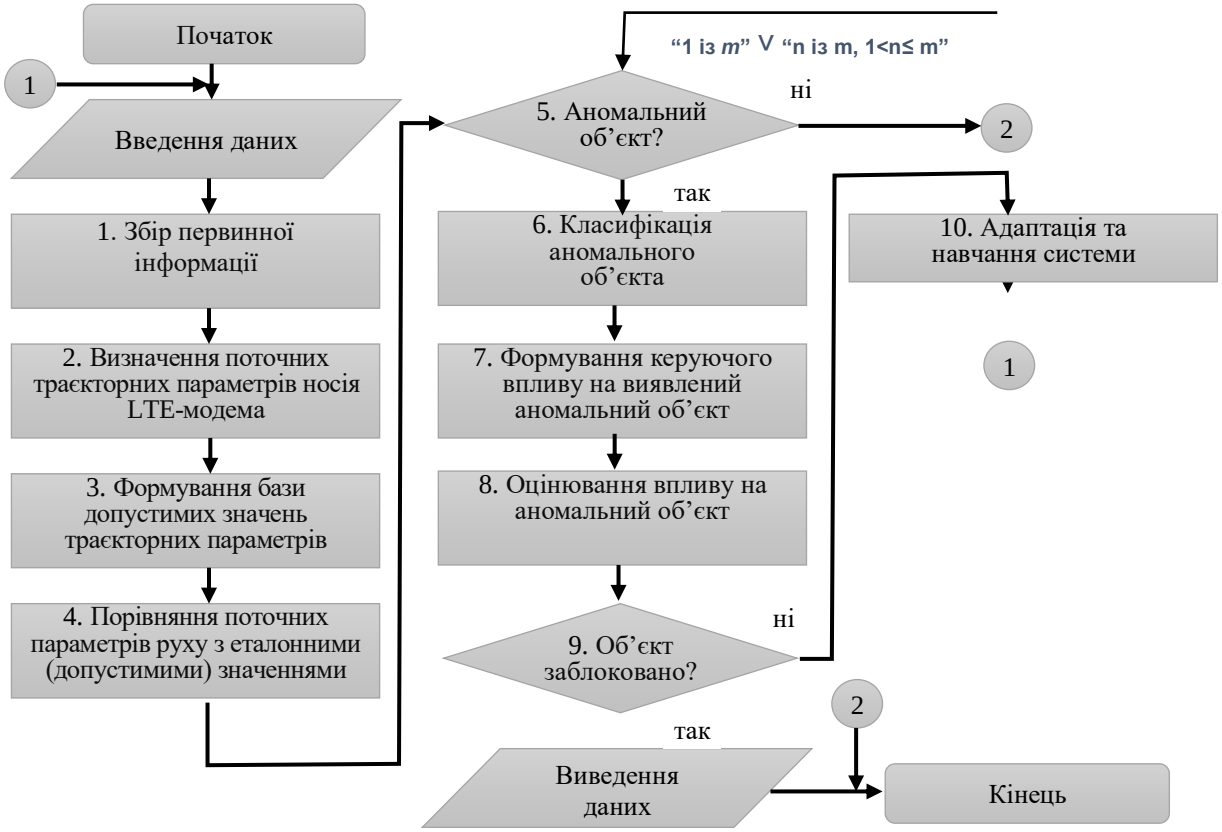


Рисунок 2. Алгоритм інтелектуального способу протидії безпілотним літальним апаратам противника з LTE-модемами на основі виявлення поточних аномалій траєкторних параметрів

На **третьому кроці** формується база еталонних (допустимих) значень траєкторних параметрів. Ця база містить характеристики, які відповідають нормальній поведінці типових об'єктів, зокрема: наземного транспорту (автомобілі, залізничні засоби); цивільних користувачів мережі; повітряних об'єктів (за наявності відповідних коридорів та дозволів на використання повітряного простору).

Слід зазначити, що під час воєнного стану в Україні польоти будь-яких цивільних БпЛА потребують обов'язкового дозволу від Служби безпеки України, Державіаслужби або місцевої адміністрації, а всі безпілотні апарати вагою понад 250 г або з камерою має бути зареєстровано. Допустимі значення траєкторних параметрів можуть задаватися у вигляді:

фіксованих порогів (наприклад, максимальна швидкість, висота);

у вигляді просторових обмежень (заборонені зони, коридори польотів повітряних об'єктів);

у вигляді функціональних залежностей або моделей нормальної поведінки.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

На **четвертому кроці** у режимі реального часу здійснюється порівняння поточних параметрів руху з еталонними (допустимими) значеннями. Результати порівняльного оцінювання поточних параметрів з еталонними є вхідною інформацією для ухвалення рішення про аномальність об'єкта. Зазначене рішення базується на згаданому вище критерії "*n* із *m*". При цьому рішення може бути ухвалене на **п'ятому кроці** за "жорстким" або "м'яким" правилом. За "жорстким" правилом "1 із *m*" об'єкт вважається аномальним, якщо виконується хоча б одна з умов:

об'єкт перебуває в забороненій або нетиповій для його типу зоні;

швидкість об'єкта перевищує допустимі значення для наземних об'єктів;

траєкторія руху не відповідає дорожній інфраструктурі (див. рис. 1);

напрямок руху орієнтований на критично важливі об'єкти;

спостерігається висока маневреність (часті або різкі зміни курсу).

За "м'яким" правилом використовується критерій "*n* із *m*, $1<n\leq m$", за яким висновок про наявність аномалії приймається на основі сукупності декількох *n* ознак із загальної кількості *m* можливих.

На **шостому кроці** на основі всіх траєкторних параметрів $\{x, y, h, v, k, \omega\}$ здійснюється класифікація об'єкта. У разі перевищення встановлених порогів або невідповідності поведінковій моделі об'єкт ідентифікується як: потенційно небезпечний; такий, що має ознаки БпЛА або іншого керованого засобу, який використовується з порушенням встановлених обмежень. Результати такої класифікації є підставою для інформування уповноважених органів безпеки та військового управління, які здійснюють моніторинг застосування повітряного простору та координують заходи з протидії загрозам.

На **сьомому кроці** формується керуючий вплив на виявлений аномальний об'єкт. Залежно від рівня загрози можуть застосовуватись такі заходи протидії:

вибіркове обмеження доступу до мережі (блокування передачі даних);

деактивація окремих сервісів (наприклад, мобільного інтернету);

примусове відключення від мережі.

На **восьмому кроці** здійснюється перевірка (оцінювання) результатів впливу зазначених заходів на аномальний об'єкт. Якщо аномальний об'єкт не буде заблоковано (що перевіряється на **дев'ятому кроці**), надалі здійснюється адаптація та навчання системи виявлення аномалій траєкторних параметрів динамічного об'єкта (**десятий крок**). На основі накопичених даних уточнюються порогові значення, коригуються моделі нормальної поведінки динамічних об'єктів з метою підвищення точності виявлення аномалій траєкторних параметрів динамічних об'єктів. Для цього може бути застосовано методи: статистичного аналізу; нечіткої логіки; машинного навчання.

Отже, запропонований інтелектуальний спосіб працює за принципом: "розвідка – оцінювання параметрів руху динамічного об'єкта – виявлення аномалій траєкторних параметрів – вибірковий просторово-частотний вплив на аномальний об'єкт". Ключовою особливістю способу є те, що:

аналіз параметрів руху динамічних об'єктів (БпЛА) здійснюється не за змістом трафіка, а за поведінкою об'єкта у просторі;

рішення щодо впливу на аномальний об'єкт (блокування доступу його до мережевих сервісів) ухвалюється в режимі реального часу;

вплив є вибірковим і зосереджується на динамічних об'єктах з аномаліями траєкторних параметрів.

Це дозволяє: своєчасно виявляти аномальні динамічні об'єкти; мінімізувати хибні спрацювання; уникати порушення роботи цивільної телекомунікаційної інфраструктури.

Практичний ефект запропонованого способу полягає в тому, що він дозволяє знижувати ефективність розвідувальних та ударних БпЛА, які використовують LTE-модеми з SIM-

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

картами національних операторів мобільного зв'язку, без шкоди для загальної працездатності мобільної інфраструктури та абонентів критичної інфраструктури. Для практичної реалізації способу необхідно:

інтегрувати алгоритми виявлення аномалій у програмне забезпечення систем управління та моніторингу (NMS) операторів стільникового зв'язку (що забезпечить оперативний режим моніторингу аномалій);

розробити юридичні механізми для оперативного адресного блокування ідентифікаторів абонентів стільникового зв'язку IMSI (International Mobile Subscriber Identity) за наявності критеріїв аномальності траєкторних параметрів;

забезпечити регулярну адаптацію системи виявлення аномалій шляхом перенавчання ML-модулів на нових даних, враховуючи еволюцію технологій, використовуваних противником для наведення високоточних засобів.

Висновок (Conclusion)

Результати дослідження демонструють, що інтелектуальний спосіб виявлення поточних аномалій траєкторних параметрів є ефективним інструментом селективної протидії БпЛА, в бортове обладнання яких противник інтегрує LTE-модеми із SIM-картами національних операторів мобільного зв'язку. Запропонований спосіб дозволяє реалізовувати вибіркові заходи впливу (адресне блокування LTE-модемів динамічних об'єктів з аномальними траєкторними параметрами) з мінімальними наслідками для абонентів цивільного сектору та збереженням стійкого функціонування об'єктів критичної інфраструктури. Подальше розроблення обраної тематики слід фокусувати на інтеграції запропонованого інтелектуального способу протидії БпЛА на основі виявлення аномалій їхніх траєкторних параметрів у мультисенсорну мережу різнорідних засобів виявлення та протидії, покращенні моделей виявлення аномалій траєкторних параметрів та прогнозування поведінки аномальних об'єктів у повітряному просторі; створенні (удосконаленні) нормативно-правової бази для впровадження та оперативного застосування запропонованого способу, інтегрованого у військово-цивільну систему виявлення потенційних загроз (типу ситеми "Покрова").

Рекомендації (Recommendations)

Результати дослідження можуть бути використані для удосконалення систем територіальної ППО та захисту стратегічних об'єктів. Подальші дослідження доцільно спрямувати на удосконалення алгоритмів виявлення аномалій траєкторних параметрів динамічних об'єктів і розроблення алгоритмів автоматичного розпізнавання роїв БпЛА противника, що використовують LTE- та MESH-мережі для навігації, управління та координації дій. Результати дослідження доцільно врахувати:

операторам мобільного зв'язку, які мають інтегрувати в архітектуру систем управління мережею NMS алгоритми автоматичного виявлення аномалій на основі критерію "*n* із *m*" та нейромережевих моделей розпізнавання патернів маневрування динамічних об'єктів з LTE-модемами;

державним регуляторним органам, які мають забезпечити правову основу для оперативного адресного блокування SIM-карток, що демонструють аномальну траєкторну поведінку, без потреби у тривалих процедурах узгодження;

науковим установам та фахівцям, які вивчають проблематику виявлення та протидії засобам повітряного нападу із зосередженням подальших досліджень на методах прогнозування траєкторій БпЛА (або інших динамічних об'єктів) в умовах розрідженого покриття базових станцій та використанні методів глибокого машинного навчання (Deep Learning) моделей виявлення аномалій траєкторних параметрів динамічних об'єктів і компенсації похибок визначення їхніх поточних координат.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

Конфлікт інтересів (Conflict of Interest)
Автори заявляють, що у них немає конфлікту інтересів.

Використані джерела

1. *Легко зробити – важко захиститися: чим небезпечні Shahed з українськими SIM-картками.* https://focus.ua/uk/digital/609653.
2. *Росія запускає новітні дрони з LTE-зв'язком по Україні*. https://informer.media/.
3. Чабан, В. (2023). Теоретичне обґрунтування результатів вимірювання аномалії траєкторії космічних апаратів. *ISTCMTM*, *84* (3), 11–15.
4. *LTE Radio Link Budgeting and RF Planning: LTE Encyclopedia*. https://sites.google.com/site/lteencyclopedia/lte-radio-link-budgeting-and-rf-planning.
5. *Ukrainian Defense Ministry Adviser: Belarusian Operators Provide Roaming for Russian Drones.* https://reform.news/en/ukrainian-defense-ministry-adviser-belarusian-operators-provide-roaming-for-russian-drones.
6. *Військові не глушать мобільний зв'язок під час повітряних тривог – джерело у Генштабі.* https://www.ukrinform.ua/rubric-society/4035974-vijskovi-ne-glusat-mobilnij-zvazok-pid-cas-povitranih-trivog-dzerelo-u-genstabi.html.
7. Брусак, І. (2025). Виявлення геодинамічних аномалій у часових рядах ГНСС з використанням методів машинного навчання. *JGD*, *1* (38), 37–48.
8. Ільїн, Д. В., & Шовкошитний, І. І. (2023). Підхід до захисту інформаційно-телекомунікаційних систем на основі автокомпенсаційного принципу адресно-часової селекції аномалій мережевого трафіка. *Сучасні інформаційні технології в сфері безпеки і оборони*, *3* (48), 5–10.
9. Aggarwal, Charu C. (2017). *Outlier Analysis*. (2nd ed.). Springer.

References

1. *Easy to Make – Hard to Defend Against: Why Shahed Drones with Ukrainian SIM Cards Are Dangerous*. https://focus.ua/uk/digital/609653.
2. *Russia Deploys New Drones with LTE Connectivity Over Ukraine*. https://informer.media/.
3. Chaban, V. (2023). Theoretical justification of the results of measuring anomalies in the trajectories of spacecraft. ISTCMTM, *84* (3), 11–15.
4. *Calculation of LTE communication links and radio frequency planning: LTE Encyclopedia*. https://sites.google.com/site/lteencyclopedia/lte-radio-link-budgeting-and-rf-planning.
5. *Advisor to the Ministry of Defense of Ukraine: Belarusian operators provide roaming for Russian drones*. https://reform.news/en/ukrainian-defense-ministry-adviser-belarusian-operators-provide-roaming-for-russian-drones.
6. *The military does not jam mobile communications during air raid alerts—a source in the General Staff*. https://www.ukrinform.ua/rubric-society/4035974-vijskovi-ne-glusat-mobilnij-zvazok-pid-cas-povitranih-trivog-dzerelo-u-genstabi.html.
7. Brusak, I. (2025). Detection of geodynamic anomalies in GNSS time series using machine learning methods. *JGD, 1* (38), 37–48.
8. Ilyin, D. V., & Shovkoshytny, I. I. (2023). An approach to protecting information and telecommunications systems based on the self-compensating principle of address-time selection of network traffic anomalies. *Modern Information Technologies in Security and Defense*, *3* (48), 5–10.
9. Aggarwal, Charu C. (2017). *Outlier Analysis.* (2nd ed.). Springer.

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

An intelligent method for countering enemy unmanned aerial vehicles equipped with LTE modems based on the detection of current anomalies in flight path parameters

Ihor Shovkoshytnyi
Doctor of Military Science, Senior Research
Senior Research Fellow
National Defense University of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: igor65@meta.ua
ORCID: 0000-0001-9245-4111

Oleksii Muromets
PhD student
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: alexlesli77733@gmail.com
ORCID: 0000-0001-9940-511X

Olha Vasylenko
PhD
PhD student
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: nicety@ukr.net
ORCID: 0000-0003-2633-0131

Dmytro Brovchenko
Junior Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: brovchenkodmitry@gmail.com
ORCID: 0009-0001-2665-5836

Abstract. The article addresses the acute problem of countering adversarial strike unmanned aerial vehicles (UAVs) equipped with LTE modems. Such vehicles are capable of transmitting video in real time or from recording via mobile base stations of national telecom operators, as well as receiving commands for course correction. It is shown that the widespread use of 4G/LTE networks for remote control, trajectory adjustment and reconnaissance data transmission significantly reduces the effectiveness of traditional electronic warfare measures. The limitations of classical approaches to countering Shahed-type UAVs are examined, and the necessity of transitioning to flexible organisational and technical countermeasures is substantiated. The aim of the article is to develop an intelligent method for detecting, localising and selectively neutralising UAVs with LTE modems based on the operational analysis of current anomalies in trajectory parameters. A comprehensive approach is proposed, combining analytical methods, formal and fuzzy logic, and neural network models of artificial intelligence to detect anomalies in trajectory parameters based on SIM card positioning data in a cellular network. A set of anomaly criteria is developed: spatial coordinates, absolute and relative speed, heading, rate of change of heading, as well as combined behavioural

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No. 2 (2026)

deviation indicators. An algorithm of the intelligent countermeasure method is described, based on the operational analysis of current anomalies in trajectory parameters of moving objects. An algorithm for selectively blocking anomalous objects' access to network services without shutting down entire base stations is proposed. The method allows implementing selective countermeasures – targeted data transmission blocking, service deactivation – with minimal impact on civilian infrastructure. The research demonstrates that the proposed intelligent approach provides increased effectiveness in neutralising threats from UAVs while preserving network functionality and reducing risks to civilian services, making it suitable for practical implementation in critical infrastructure protection systems. Recommendations are given on integrating the proposed algorithms into operators' network management systems (NMS), creating legal mechanisms for the rapid blocking of International Mobile Subscriber Identity (IMSI), and regularly retraining ML modules. The developed method is suitable for practical implementation in critical infrastructure protection systems.

Keywords: unmanned aerial vehicle, LTE-modem, mobile network operator, cellular network, trajectory parameter anomaly, countermeasures against unmanned aerial vehicles.