УДК 004.056.5, 004.773, 004.85 DOI https://doi.org/10.35546/kntu2078-4481.2026.1.33

О. В. ГРИНЕНКО
аспірант кафедри комп'ютерних наук
Сумський державний університет
ORCID: 0009-0008-7062-1108

В. К. ОБОДЯК
кандидат технічних наук, доцент,
доцент кафедри кібербезпеки
Сумський державний університет
ORCID: 0000-0002-8539-1252

М. С. ОТРОЩЕНКО
аспірант кафедри комп'ютерних наук
Сумський державний університет
ORCID: 0000-0001-5064-6780

І. О. ПУГАЧ
асистент кафедри кібербезпеки,
аспірант кафедри управління імені Олега Балацького
Сумський державний університет
ORCID: 0009-0002-9644-9357

А. О. ТЕНИЦЬКА
аспірант кафедри комп'ютерних наук
Сумський державний університет
ORCID: 0000-0002-2526-8842

КІБЕРАТАКИ НА БОРТОВІ СИСТЕМИ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ТА МЕТОДИ ПРОТИДІЇ НА ОСНОВІ МАШИННОГО НАВЧАННЯ

У статті досліджуються сучасні кіберзагрози для безпілотних літальних апаратів та методи їх виявлення в умовах зростаючої автономності БПЛА. Традиційні підходи до виявлення GPS-спуфінгу, засновані на методах глибокого навчання, показують обмежену ефективність у динамічних умовах експлуатації. Такі підходи залежні від стабільності середовища, наявності інфраструктури зв'язку та характеризуються високою обчислювальною складністю. Інтеграція інформаційно-екстремального машинного навчання дозволяє здійснювати виявлення підміни навігаційних сигналів з використанням компактних інваріантних дескрипторів, забезпечуючи стійкість до геометричних перетворень та можливість роботи з обмеженими обсягами навчальних даних.

Розглянуто комплексну систематизацію кіберзагроз для автономних БПЛА, включно з радіоелектронною боротьбою, фізичними та апаратними загрозами, загрозами для багатодронових систем та атаками на моделі машинного навчання. Проведено порівняльний аналіз існуючих методів виявлення GPS-спуфінгу, який показав що підходи на основі LSTM, MLP, CNN демонструють точність від 78 % до 95 %, але їх ефективність різко знижується при динамічних змінах середовища.

Окрім технічних аспектів, у дослідженні також розглянуто еволюцію загроз, зокрема: появу більш досконалих методів спуфінгу, використання спрямованих антен глушіння для порушення роботи на великих висотах, вразливість інерційних навігаційних систем до цільової дестабілізації через мікровібрації та акустичні впливи, а також специфіку атак на рої дронів з асиметричними можливостями. Підкреслено важливість розробки інтегрованих захисних методів, які дозволяють підвищити надійність навігаційних систем у складних геопросторових умовах. Досліджено що adversarial-атаки виступають двосторонньою загрозою: вони можуть обманювати системи розпізнавання цілей, змушуючи БПЛА не виявляти ворожі транспортні засоби або неправильно класифікувати перешкоди.

Метою дослідження є виявлення як потенціалу, так і обмежень існуючих методів виявлення кіберзагроз для БПЛА, а також обґрунтування перспективності застосування інформаційно-екстремального машинного навчання з урахуванням технічних обмежень та операційних вимог. Автори зазначають що найбільш дієвим підходом визнано гібридну модель захисту, яка поєднує ІЕМН з використанням радіально-кутових дескрипторів,

© О. В. Гриненко, В. К. Ободяк, М. С. Отрощенко, І. О. Пугач, А. О. Теницька, 2026
Стаття поширюється на умовах відкритої ліцензії CC BY 4.0

використання сенсорів та адаптивну фільтрацію. Це забезпечує вищу надійність, точність виявлення відхилень траєкторій польоту та зменшення похибок у сучасних умовах радіоелектронної боротьби.

Ключові слова: *безпілотні літальні апарати, кібербезпека БПЛА, GPS-спуфінг, інформаційно-екстремальне машинне навчання, виявлення загроз, навігаційна безпека.*

O. V. HRYNENKO
Postgraduate Student at the Department of Computer Science
Sumy State University
ORCID: 0009-0008-7062-1108

V. K. OBODIAK
Candidate of Technical Science, Associate Professor,
Associate Professor at the Cybersecurity Department
Sumy State University
ORCID: 0000-0002-8539-1252

M. S. OTROSHCHENKO
Postgraduate Student at the Department of Computer Science
Sumy State University
ORCID: 0000-0001-5064-6780

I. O. PUHACH
Assistant at the Cybersecurity Department,
Postgraduate Student at the Oleg Balatsky Department of Management
Sumy State University
ORCID: 0009-0002-9644-9357

A. O. TENYTSKA
Postgraduate Student at the Department of Computer Science
Sumy State University
ORCID: 0000-0002-2526-8842

CYBERATTACKS ON ON-BOARD SYSTEMS OF UNMANNED AERIAL VEHICLES AND METHODS OF COUNTERING THEM BASED ON MACHINE LEARNING

The article examines modern cyber threats to unmanned aerial vehicles and methods for their detection in the context of increasing UAV autonomy. Traditional approaches to detecting GPS spoofing, based on deep learning methods, show limited effectiveness in dynamic operating conditions. Such approaches depend on the stability of the environment, the availability of communication infrastructure and are characterized by high computational complexity. The integration of information-extreme machine learning allows for the detection of navigation signal substitution using compact invariant descriptors, ensuring resistance to geometric transformations and the ability to work with limited amounts of training data.

A comprehensive systematization of cyber threats to autonomous UAVs is considered, including electronic warfare, physical and hardware threats, threats to multi-drone systems and attacks on machine learning models. A comparative analysis of existing GPS spoofing detection methods was conducted, which showed that approaches based on LSTM, MLP, CNN demonstrate accuracy from 78 % to 95 %, but their effectiveness decreases sharply with dynamic changes in the environment.

In addition to technical aspects, the study also considers the evolution of threats, in particular: the emergence of more advanced spoofing methods, the use of directional jamming antennas to disrupt operation at high altitudes, the vulnerability of inertial navigation systems to target destabilization due to microvibrations and acoustic effects, as well as the specificity of attacks on drone swarms with asymmetric capabilities. The importance of developing integrated protective methods that can increase the reliability of navigation systems in complex geospatial conditions is emphasized. It is studied that adversarial attacks are a two-sided threat: they can deceive target recognition systems, forcing UAVs not to detect enemy vehicles or incorrectly classify obstacles.

The aim of the study is to identify both the potential and limitations of existing methods for detecting cyber threats to UAVs, as well as to substantiate the prospects for the application of information-extreme machine learning, taking into account technical limitations and operational requirements. The authors note that the most effective approach is a hybrid protection model that combines IEMN with the use of radial-angular descriptors, the use of sensors and adaptive filtering. This provides higher reliability, accuracy of detecting flight path deviations and reducing errors in modern conditions of electronic warfare.

Key words: *unmanned aerial vehicles, UAV cybersecurity, GPS spoofing, information-extreme machine learning, threat detection, navigational security.*

Постановка проблеми

Розвиток технологій безпілотних літальних апаратів (БПЛА) протягом останнього десятиліття започаткував суттєву трансформацію у різноманітних сферах діяльності. Застосування БПЛА охоплює широкий спектр – від військової розвідки до моніторингу інфраструктури, логістики та рятувальних операцій, демонструючи високу технологічну ефективність. Ця динаміка зумовлена комплексом операційних переваг, зокрема економічною ефективністю, високою маневреністю та можливістю функціонування у небезпечних середовищах, а також безперервним технологічним розвитком у напрямках мініатюризації та підвищення автономності.

Однак широке впровадження БПЛА створило серйозні виклики у забезпеченні безпеки навігаційних систем. Сучасні БПЛА функціонують як інтегровані апаратно-програмні платформи, критично залежні від цифрової інфраструктури та мережевої взаємодії. Така залежність формує комплекс вразливостей для здійснення кібератак. Задокументовані інциденти свідчать, що БПЛА належать до класу систем з підвищеним ризиком через значну кількість мережевих та операційних вразливостей.

У сукупності це формує складне та динамічне середовище загроз, у якому порушення цілісності навігаційних даних, втручання у канали зв'язку чи вплив на бортові модулі можуть призводити до суттєвих відхилень траєкторії польоту або навіть повної втрати керованості. Актуальним завданням постає розроблення науково обґрунтованих підходів до підвищення стійкості навігаційних систем.

Аналіз останніх досліджень і публікацій

Інтенсивний розвиток навігаційних систем безпілотних літальних апаратів протягом останніх років свідчить про зміну пріоритетів у дослідженнях кібербезпеки навігаційних систем безпілотних літальних апаратів. Розвиток програмно-орієнтованих бортових платформ і використання алгоритмів штучного інтелекту в задачах навігації зумовили зниження уваги до традиційних методів фізичного захисту та класичного шифрування каналів зв'язку. Натомість у сучасних роботах переважають підходи, спрямовані на забезпечення стійкості моделей машинного навчання, виявлення та нейтралізацію інтелектуальних атак типу спуфінгу, а також формування багаторівневих архітектур захисту на основі концепції нульової довіри.

Значна частина останніх публікацій присвячена вразливостям навігаційних систем. Дослідники констатують перехід від класичного глушіння GNSS-сигналів до складних сценаріїв спуфінгу, спрямованих на маніпуляцію часовими мітками, що є критичним для корекції дрейфу гіроскопів в інерціальних системах [1]. Окрему увагу в літературі приділено вразливостям детекторів аномалій на базі машинного навчання. Зокрема, у роботах 2025 року доведено, що класифікатори на основі методу опорних векторів (SVM) можуть бути скомпрометовані через спеціально модифіковані сигнали з додаванням шуму або незначним зсувом даних, що знижує точність розпізнавання до критичних показників [2].

Зростання автономності безпілотних літальних апаратів зумовило активізацію досліджень у сфері безпеки систем візуальної навігації, зокрема алгоритмів VIO та SLAM. У сучасних роботах показано, що цілеспрямоване формування візуального середовища зі спеціально підібраними патернами може істотно підвищувати похибку оцінювання руху та призводити до дестабілізації польоту БПЛА [3]. Також досліджуються загрози типу «троянський кінь» у згорткових нейромережах, активація яких відбувається під час розпізнавання специфічних візуальних тригерів, що експериментально підтверджено для навігаційного фреймворку DroNet [4].

Аналіз публікацій, присвячених застосуванню БПЛА в умовах сучасних збройних конфліктів, зокрема війни в Україні, підтверджує обмежену ефективність периметрових моделей кіберзахисту та обґрунтовує перехід до багаторівневих архітектур безпеки [9–10]. У відповідь на обмеження бортових ресурсів активно досліджуються методи легковагової криптографії, серед яких алгоритм ASCON-128 демонструє переваги за показниками енергоефективності для захисту телеметричних каналів у системах із жорсткими обмеженнями SWaP [11–12]. Паралельно розвиваються підходи архітектури нульової довіри для БПЛА [14] та децентралізовані механізми забезпечення цілісності даних у ройових системах, зокрема SwarmRaft і PTEE-BFT [15–16], а також порушуються питання стандартизації й стійкості ланцюгів постачання компонентів [27–30].

Разом з тим, у більшості наявних досліджень основна увага приділяється криптографічним і мережевим аспектам захисту, тоді як алгоритмічні підходи до виявлення аномалій і цілеспрямованих атак на рівні навігаційних та сенсорних підсистем БПЛА залишаються недостатньо формалізованими та систематизованими. Це зумовлює актуальність розроблення методів інтелектуального аналізу, зокрема на основі інформаційно-екстремального машинного навчання, які дозволяють формувати стійкі вирішальні правила для оперативного виявлення аномальних станів у реальному часі.

Формулювання мети дослідження

Метою статті є обґрунтування нових підходів до підвищення стійкості навігаційних систем автономних БПЛА в умовах радіоелектронної боротьби. Для досягнення цієї мети робота систематизує сучасні вектори кібератак, здійснює критичний аналіз обмежень методів глибокого навчання та аргументує ефективність застосування інформаційно-екстремального машинного навчання з використанням інваріантних радіально-кутових дескрипторів для оперативного виявлення спуфінгу.

Викладення основного матеріалу дослідження

Сучасні дослідження в галузі забезпечення кібербезпеки безпілотних літальних апаратів (БПЛА) демонструють широкий спектр підходів атак. Проведений аналіз літератури свідчить, що кіберзагрози мають комплексний характер і охоплюють майже всі аспекти функціонування автономної платформи: від каналів зв'язку й навігаційних систем до сенсорних модулів та алгоритмів штучного інтелекту (рис. 1).

Відкриті або недостатньо захищені канали зв'язку між БПЛА та наземною станцією залишаються основним вектором вразливості. До цієї категорії належать перехоплення керуючих команд, атаки на протоколи телеметрії, атаки типу MitM та підміна навігаційних сигналів. Дослідження [5] підтверджує, що навіть комерційні канали Wi-Fi можуть бути використані для повного перехоплення контролю над апаратом.

Окремий клас загроз становлять атаки на навігаційні системи. Глушіння (Jamming) GPS є однією з найпоширеніших форм через низький поріг входження: слабкі супутникові сигнали легко пригнічуються системами РЕБ. Ефективність глушіння залежить від потужності сигналу та відстані до джерела шуму, а його вплив здатен знизити показники завершення місії на 40 % [6].

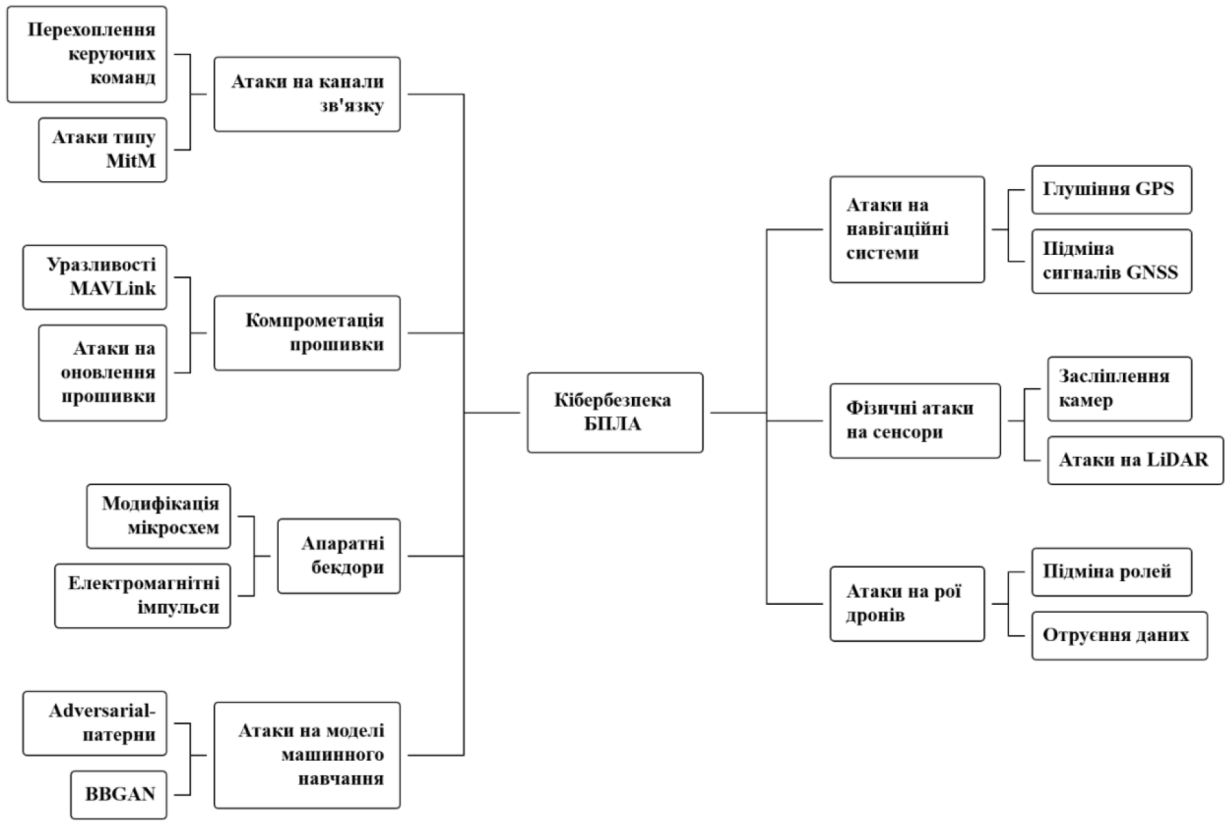

Рис. 1. Види кіберзагроз безпілотних літальних апаратів

Однак значно небезпечнішою загрозою є спуфінг (Spoofing) – підміна навігаційних сигналів [7]. На відміну від глушіння, суфер може змусити БПЛА згенерувати хибне навігаційне рішення (PVT) та відхилитися від маршруту, не викликаючи спрацювання аварійних протоколів. Дослідження [8] показують, що штучна генерація GPS-сигналів призводить до помилок позиціонування у 20–45 метрів, що є критичним для автономних місій. Починаючи з кінця 2024 року, фіксується використання спрямованих антен для спуфінгу на великих висотах, що вимагає більш складних алгоритмів аналізу модуляції сигналу для виявлення атак.

Крім того, зростання автономності БПЛА актуалізувало загрози для бортових сенсорів та моделей машинного навчання. Фізичні атаки, такі як засліплення камер лазерами або акустичний вплив на гіроскопи IMU [13], здатні дестабілізувати роботу алгоритмів SLAM. Паралельно розвиваються adversarial-атаки на нейромережі: спеціально сформовані патерни на об'єктах або місцевості змушують системи комп'ютерного зору ігнорувати цілі або неправильно їх класифікувати [15-16]. Також доведено можливість data-poisoning атак, коли отруєння навчальної вибірки призводить до систематичних помилок навігації у реальних бойових умовах [17].

Сучасна парадигма використання безпілотних літальних апаратів (БПЛА) характеризується стрімким переходом від дистанційного керування до повної автономності, що докорінно змінює модель загроз безпеці. Проведений аналіз наукової літератури дозволяє стверджувати, що кібернетичний вплив на такі системи набув

ознак мультивекторності, охоплюючи фізичний, канальний та прикладний рівні функціонування платформи. Домінуючим вектором вразливості залишаються канали інформаційного обміну між бортовим сегментом та наземною інфраструктурою, де незахищеність протоколів телеметрії створює передумови для реалізації атак типу «людина посередині» та несанкціонованої модифікації польотних завдань.

Особливої критичності в умовах радіоелектронної боротьби набувають атаки на підсистеми глобальної навігації, де окрім примітивного глушіння, значну небезпеку становить когерентний спуфінг. Цей вид інтелектуальної атаки дозволяє зловмиснику маніпулювати розрахунком координатно-часового рішення приймача, призводячи до неконтрольованого відхилення БПЛА від маршруту з похибкою позиціонування до 45 метрів [7–8]. Додатково ситуація ускладнюється зростанням загроз для сенсорних систем та алгоритмів штучного інтелекту, зокрема через реалізацію adversarial-атак, здатних дезорієнтувати системи комп'ютерного зору шляхом внесення непомітних збурень у вхідні дані [15–16].

Аналіз існуючих методів протидії цим загрозам демонструє домінування підходів на основі глибокого навчання (Deep Learning), таких як згорткові та рекурентні нейронні мережі. Попри високу номінальну точність у межах 78–95 %, практична імплементація цих алгоритмів на борту автономних БПЛА стикається з фундаментальними обмеженнями стохастичної природи нейромереж [18–19]. Висока обчислювальна складність та енергоємність суперечать жорстким вимогам до масогабаритних показників тактичних дронів, а критична залежність від репрезентативності навчальної вибірки унеможливлює швидку адаптацію до динамічних змін сигнально-завадової обстановки. Зазначені обмеження зумовлюють необхідність зміни наукової парадигми в напрямку використання детермінованих методів з високою навчальною здатністю, серед яких найбільш перспективним є інформаційно-екстремальне машинне навчання (ІЕМН).

На відміну від традиційних методів мінімізації помилки, ІЕМН базується на максимізації інформаційної спроможності системи розпізнавання в процесі навчання, що дозволяє будувати надійні вирішальні правила навіть за умови перетину класів та мінімального обсягу навчальної вибірки. Ключовою науковою новизною запропонованого підходу є використання спеціалізованих радіально-кутових дескрипторів, які формуються у полярній системі координат. Така структура забезпечує математичну інваріантність ознак до афінних перетворень, дозволяючи системі ідентифікувати патерни атак незалежно від кута крену БПЛА, висоти польоту чи ракурсу спостереження без необхідності ресурсомісткої аугментації даних.

Для практичної реалізації цього методу розроблено концептуальну схему гібридної системи захисту (рис. 2), яка інтегрує модуль ІЕМН у контур навігації БПЛА. Архітектура передбачає попередню обробку сигналів від сенсорів методами адаптивної фільтрації для усунення високочастотних шумів з подальшим аналізом структури сигналу через систему інваріантних дескрипторів.

За таких умов інформаційно-екстремальне машинне навчання є перспективним підходом, оскільки оперує компактними, стійкими до перетворень і високодискретними дескрипторами [20]. Зокрема, у дослідженнях з розпізнавання об'єктів показано, що дескриптори, побудовані на радіально-кутовому розподілі ознак, забезпечують стійкість до геометричних перетворень, включаючи обертання й масштабування [20–21].

Рис. 2. Концептуальна схема гібридної системи захисту автономного БПЛА

Використання таких інваріантних структур ознак у межах ІЕМН відкриває можливість підвищення надійності ідентифікації GPS-спуфінгу за рахунок точнішого трактування відхилень траєкторій польоту та зменшення похибок у динамічних умовах. Для автономних БПЛА, що працюють у складних геопросторових умовах, найбільш критичними залишаються атаки на навігаційні підсистеми, канали зв'язку та моделі машинного навчання, що визначає необхідність розроблення інтегрованих захисних методів, включно з адаптивною фільтрацією, багатосенсорною інтеграцією та інформаційно-екстремальними підходами до оцінки надійності навігаційних даних.

Висновки

Результати огляду наявних атак свідчать про системну багаторівневу природу кіберзагроз автономним БПЛА, які реалізуються на радіоелектронному, апаратному, програмному та інтелектуальному рівнях. Найбільш небезпечними залишаються GPS-джемінг і спуфінг, причому останній здатний призводити до суттєвих помилок позиціонування та втрати контролю над траєкторією польоту. Зростаючу складність демонструють також апаратні атаки та загрози для багатодронових систем, що характеризуються каскадним поширенням через децентралізовані протоколи координації. Окремий клас ризиків формують атаки на моделі машинного навчання, критичність яких зростає разом із рівнем автономності БПЛА.

Порівняльний аналіз методів виявлення GPS-спуфінгу виявив обмеження сучасних підходів, зокрема залежність глибоких нейронних моделей від умов середовища та обчислювальних ресурсів. Інформаційно-екстремальне машинне навчання розглядається як перспективна альтернатива завдяки можливості роботи з компактними інваріантними дескрипторами, зменшеними вимогами до навчальних даних та інтерпретованістю результатів. Використання радіально-кутових дескрипторів дозволяє підвищити надійність виявлення спуфінгу в динамічних умовах польоту.

Подальші дослідження доцільно спрямувати на розробку гібридних методів захисту, що поєднують ІЕМН, багатосенсорну фузію та адаптивну фільтрацію, а також на створення інтерпретованих і ресурсоощадних систем безпеки для автономних і багатодронових платформ. Забезпечення кібербезпеки БПЛА потребує інтегрованих практичних рішень, здатних забезпечити баланс між надійністю, обчислювальною ефективністю та стійкістю до еволюційних кіберзагроз.

Список використаної літератури

1. Impact Assessment of GNSS Spoofing Attacks on INS/GNSS Integrated Navigation System / L. Yang et al. Sensors. 2018. Vol. 18, no. 5. P. 1433. URL: https://doi.org/10.3390/s18051433

2. An S., Jang D. J., Lee E.-K. Adversarial Evasion Attacks on SVM-Based GPS Spoofing Detection Systems. Sensors. 2025. Vol. 25, no. 19. URL: https://doi.org/10.3390/s25196062

3. Black-box Adversarial Attacks on CNN-based SLAM Algorithms / M. R. Gkeka et al. arXiv preprint arXiv. 2025. URL: https://arxiv.org/abs/2505.24654

4. An Experimental Study of Trojan Vulnerabilities in UAV Autonomous Landing / R. Ahmari et al. ArXiv. 2025. URL: https://arxiv.org/abs/2510.20932

5. Behind The Wings: The Case of Reverse Engineering and Drone Hijacking in DJI Enhanced Wi-Fi Protocol / D. Pratama et al. P. 2023. URL: https://arxiv.org/abs/2309.05913

6. Protecting Autonomous UAVs from GPS Spoofing and Jamming: A Comparative Analysis of Detection and Mitigation Techniques / P. C. Joeaneke et al. Journal of Engineering Research and Reports. 2024. Vol. 26, no. 10. P. 71–92. URL: https://doi.org/10.9734/jerr/2024/v26i101291

7. Threats from and Countermeasures for Unmanned Aerial and Underwater Vehicles / W. Khawaja et al. Sensors. 2022. Vol. 22, no. 10. P. 3896. URL: https://doi.org/10.3390/s22103896

8. On the requirements for successful GPS spoofing attacks. ACM Transactions on Information and System Security / N. O. Tippenhauer et al. CCS '11: Proceedings of the 18th ACM conference on Computer and communications security. 2011. Vol. 18. P. 75–86. URL: https://doi.org/10.1145/2046707.2046719

9. Renu Y., Sarveshwaran V. A Review of Cyber Security Challenges and Solutions in Unmanned Aerial Vehicles (UAVs). Inteligencia Artificial. 2025. Vol. 28, no. 75. P. 199–219. URL: https://doi.org/10.4114/intartif.vol28iss75pp199-219

10. A Comprehensive Survey of Unmanned Aerial Systems' Risks and Mitigation Strategies / S. Shrestha et al. 2025. ArXiv. URL: https://doi.org/10.48550/arXiv.2506.10327.

11. Patel A., Cherukuri A. K. Analysis of Light-Weight Cryptography Algorithms for UAV-Networks. ArXiv. 2025. URL: https://arxiv.org/abs/2504.04063

12. Skorobahatko M., Voitsekhovskyi A. Lightweight Cryptography in UAV systems. Theoretical and Applied Cybersecurity. 2025. Vol. 7, no. 1. URL: https://doi.org/10.20535/tacs.2664-29132025.1.326898

13. MARS: Defending Unmanned Aerial Vehicles From Attacks on Inertial Sensors with Model-based Anomaly Detection and Recovery / H. Meng et al. arXiv. 2025. URL: https://arxiv.org/abs/2505.00924

14. Data collection using unmanned aerial vehicles for Internet of Things platforms / S. Goudarzi et al. Computers & Electrical Engineering. 2019. Vol. 75. P. 1–15. URL: https://doi.org/10.1016/j.compeleceng.2019.01.028

15. Goodfellow I. J., Shlens J., Szegedy C. Explaining and Harnessing Adversarial Examples. arXiv. 2015. URL: https://arxiv.org/abs/1412.6572

16. Athalye A., Carlini N., Wagner D. Obfuscated gradients give a false sense of security: Circumventing defenses to adversarial examples. Proceedings of the 35th International Conference on Machine Learning. 2018. URL: https://arxiv.org/abs/1802.00420

17. Physical Adversarial Examples for Object Detectors / K. Eykholt et al. Proceedings of the 12th USENIX Workshop on Offensive Technologies. 2018. URL: https://doi.org/10.48550/arXiv.1807.07769

18. Sarıkaya B. S., Bahtiyar Ş. A survey on security of UAV and deep reinforcement learning. Ad Hoc Networks. 2024. P. 103642. URL: https://doi.org/10.1016/j.adhoc.2024.103642

19. Couturier A., Akhloufi M. A. A Review on Deep Learning for UAV Absolute Visual Localization. Drones. 2024. Vol. 8, no. 11. P. 622. URL: https://doi.org/10.3390/drones8110622

20. Naumenko I., Myronenko M., Savchenko T. Information-extreme machine training of on-board recognition system with optimization of RGB-component digital images. RADIOELECTRONIC AND COMPUTER SYSTEMS. 2021. No. 4. P. 59–70. URL: https://doi.org/10.32620/reks.2021.4.05

21. Information-extreme machine learning of a cyber attack detection system / A. Dovbysh et al. RADIOELECTRONIC AND COMPUTER SYSTEMS. 2022. No. 3. P. 121–131. URL: https://doi.org/10.32620/reks.2022.3.09

References

1. Yang, L., Sihai, L., Qiangwen, F., & Zhenbo, L. (2018). Impact Assessment of GNSS Spoofing Attacks on INS/GNSS Integrated Navigation System. Sensors, 18(5), 1433. https://doi.org/10.3390/s18051433

2. An, S., Jang, D. J., & Lee, E.-K. (2025). Adversarial Evasion Attacks on SVM-Based GPS Spoofing Detection Systems. Sensors, 25(19). https://doi.org/10.3390/s25196062

3. Gkeka, M. R., Sun, B., Smirni, E., Antonopoulos, C. D., Lalis, S., & Bellas, N. (2025). Black-box Adversarial Attacks on CNN-based SLAM Algorithms. arXiv preprint arXiv. https://arxiv.org/abs/2505.24654

4. Ahmari, R., Mohammadi, A., Hemmati, V., Mynuddin, M., Mahmoud, M. N., Kebria, P., Homaifar, A., & Saif, M. (2025). An Experimental Study of Trojan Vulnerabilities in UAV Autonomous Landing. ArXiv. https://arxiv.org/abs/2510.20932

5. Pratama, D., Moon, J., Laksmono, A. M. A., Yun, D., Muhammad, I., Jeong, B., Ji, J., & Kim, H. (2023). Behind The Wings: The Case of Reverse Engineering and Drone Hijacking in DJI Enhanced Wi-Fi Protocol. 2023. https://arxiv.org/abs/2309.05913

6. Joeaneke, P. C., Val, O. O., Olaniyi, O. O., Ogungbemi, O. S., Olisa, A. O., & Akinola, O. I. (2024). Protecting Autonomous UAVs from GPS Spoofing and Jamming: A Comparative Analysis of Detection and Mitigation Techniques. Journal of Engineering Research and Reports, 26(10), 71–92. https://doi.org/10.9734/jerr/2024/v26i101291

7. Khawaja, W., Semkin, V., Ratyal, N. I., Yaqoob, Q., Gul, J., & Guvenc, I. (2022). Threats from and Countermeasures for Unmanned Aerial and Underwater Vehicles. Sensors, 22(10), 3896. https://doi.org/10.3390/s22103896

8. Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., & Čapkun, S. (2011). On the requirements for successful GPS spoofing attacks. ACM Transactions on Information and System Security. CCS '11: Proceedings of the 18th ACM conference on Computer and communications security, 18, 75–86. https://doi.org/10.1145/2046707.2046719

9. Renu, Y., & Sarveshwaran, V. (2025). A Review of Cyber Security Challenges and Solutions in Unmanned Aerial Vehicles (UAVs). Inteligencia Artificial, 28(75), 199–219. https://doi.org/10.4114/intartif.vol28iss75pp199-219

10. Shrestha, S., Ababneh, M., Misra, S., Cathey, H. M., Vishwanathan, R., Jansen, M., Choi, J., Bobba, R., & Jang, Y. (2025). A Comprehensive Survey of Unmanned Aerial Systems' Risks and Mitigation Strategies. ArXiv. https://doi.org/10.48550/arXiv.2506.10327

11. Patel, A., & Cherukuri, A. K. (2025). Analysis of Light-Weight Cryptography Algorithms for UAV-Networks. ArXiv. https://arxiv.org/abs/2504.04063

12. Skorobahatko, M., & Voitsekhovskyi, A. (2025). Lightweight Cryptography in UAV systems. Theoretical and Applied Cybersecurity, 7(1). https://doi.org/10.20535/tacs.2664-29132025.1.326898

13. Meng, H., Luo, S., Liang, Z., Huang, Q., Khazraei, A., & Pajic, M. (2025). MARS: Defending Unmanned Aerial Vehicles From Attacks on Inertial Sensors with Model-based Anomaly Detection and Recovery. arXiv. https://arxiv.org/abs/2505.00924

14. Goudarzi, S., Kama, N., Anisi, M. H., Zeadally, S., & Mumtaz, S. (2019). Data collection using unmanned aerial vehicles for Internet of Things platforms. Computers & Electrical Engineering, 75, 1–15. https://doi.org/10.1016/j.compeleceng.2019.01.028

15. Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). Explaining and Harnessing Adversarial Examples. arXiv. https://arxiv.org/abs/1412.6572

16. Athalye, A., Carlini, N., & Wagner, D. (2018). Obfuscated gradients give a false sense of security: Circumventing defenses to adversarial examples. Proceedings of the 35th International Conference on Machine Learning. https://arxiv.org/abs/1802.00420

17. Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Tramer, F., Prakash, A., Kohno, T., & Song, D. (2018). Physical Adversarial Examples for Object Detectors. Proceedings of the 12th USENIX Workshop on Offensive Technologies. https://doi.org/10.48550/arXiv.1807.07769

18. Sarıkaya, B. S., & Bahtiyar, Ş. (2024). A survey on security of UAV and deep reinforcement learning. Ad Hoc Networks, 103642. https://doi.org/10.1016/j.adhoc.2024.103642

19. Couturier, A., & Akhloufi, M. A. (2024). A Review on Deep Learning for UAV Absolute Visual Localization. Drones, 8(11), 622. https://doi.org/10.3390/drones8110622

20. Naumenko, I., Myronenko, M., & Savchenko, T. (2021). Information-extreme machine training of on-board recognition system with optimization of RGB-component digital images. RADIOELECTRONIC AND COMPUTER SYSTEMS, (4), 59–70. https://doi.org/10.32620/reks.2021.4.05

21. Dovbysh, A., Liubchak, V., Shelehov, I., Simonovskiy, J., & Tenytska, A. (2022). Information-extreme machine learning of a cyber attack detection system. RADIOELECTRONIC AND COMPUTER SYSTEMS, (3), 121–131. https://doi.org/10.32620/reks.2022.3.09

Дата першого надходження статті до видання: 10.01.2026
Дата прийняття статті до друку після рецензування: 13.02.2026
Дата публікації (оприлюднення) статті: 30.04.2026