УДК 629.5.015 **DOI: 10.31653/2306-5761.36.2024.102-115**

CONTEMPORARY METHODS OF COUNTERING UNMANNED SYSTEMS: TECHNOLOGIES AND PROSPECTS

СУЧАСНІ МЕТОДИ ПРОТИДІЇ БЕЗПІЛОТНИМ СИСТЕМАМ: ТЕХНОЛОГІЇ ТА ПЕРСПЕКТИВИ

O. Melnyk[1], *D.Sc., Associate Professor,* **O. Onishchenko**[2], *D.Sc., Professor,* **S. Kurdiuk**[2], *PhD in Eng., Senior Researcher,* **O. Drozdenko**[3], *PhD in Eng., Associate Professor,* **T. Gavrylyuk**[2], *Junior Researcher,* **D. Burlachenko**[1], *Senior Lecturer*

О. Мельник[1], *д.т.н., доцент,* **О. Онищенко**[2], *д.т.н., професор,* **С. Курдюк**[2], *PhD, ст. дослідник,* **О. Дрозденко**[3], *к.т.н., доцент,* **Т. Гаврилюк**[2], *м.н.с.,* **Д. Бурлаченко**[1], *ст. викладач*

[1]*Odesa National Maritime University*

[1]*Одеський національний морський університет*

[2]*National University "Odesa Maritime Academy"*

[2]*Національний Університет «Одеська Морська Академія»*

[3]*National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"*

[3]*Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"*

ABSTRACT

The rapid expansion of the use of unmanned aerial vehicles (UAVs) in both civilian and military applications has led to an urgent need for advanced technologies to counter them. This study examines the technical, operational, and strategic challenges posed by unmanned systems and proposes a comprehensive approach to countering these threats. In particular, the paper examines current countermeasures, including radio frequency jamming, laser jamming, microwave and acoustic deterrence, and physical interception techniques. Each approach is analyzed for its effectiveness in different operational scenarios, with a special emphasis on the limitations and advantages inherent in each method. Simulation models and experimental results further validate the proposed concept, demonstrating how these technologies can be optimized to protect critical infrastructure from unmanned systems and mitigate risks in challenging environments. The need for hybrid solutions that combine several technologies adapted to the type of UAS and situation parameters is emphasized to provide reliable and flexible protection in both air and maritime environments. The critical role of an interdisciplinary approach is emphasized and potential areas for improving countermeasures in response to the development of UAS capabilities are suggested.

Keywords: unmanned aerial systems, maritime unmanned systems, countermeasures, radio frequency jamming, laser jamming, microwave jamming, acoustic interception, hybrid security systems, interoperability, critical infrastructure protection, interceptor drones, unmanned technologies.

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Безпілотні апарати (БПА) швидко завоювали позиції в багатьох галузях завдяки своїй універсальності, ефективності та здатності виконувати завдання в умовах, що є небезпечними або недоступними для людини. Сьогодні БПА знаходять застосування в найрізноманітніших сферах: від військових і розвідувальних операцій до комерційного та цивільного використання.

У цивільній і комерційній сфері БПА знайшли застосування в картографії, сільському господарстві, моніторингу природних катастроф і навіть у доставці товарів і медикаментів у важкодоступні райони. Оскільки їхнє використання стає дедалі масовим, виникає потреба в регулюванні та забезпеченні безпеки, особливо з урахуванням потенціалу цих апаратів для порушення приватної та державної безпеки [1]. У військових цілях їх широко використовують для розвідки, стеження і виконання бойових операцій, оскільки це дає змогу вести дії на далеких дистанціях і в умовах обмеженої видимості, зберігаючи при цьому безпеку оператора [2].

Водночас функціональні можливості та активне використання БПА створює як технічні, так і правові виклики [3]. Наприклад, останніми роками світове співтовариство зіткнулося зі збільшенням кількості інцидентів, пов'язаних із проникненням безпілотних літальних апаратів (БПЛА) в зони, що охороняються, що наголошує на необхідності розроблення ефективних методів захисту та регулювання [4, 5]. У відповідь на це багато країн почали активне розроблення систем протидії БПЛА, орієнтованих на виявлення, нейтралізацію і перенаправлення безпілотних систем, які можуть становити загрозу. Таким чином дані дослідження підкреслюють необхідність комплексного підходу до протидії БПА, що поєднує в собі кілька технологій для створення багаторівневої системи захисту.

Зі швидким розвитком технологій і поширенням безпілотних апаратів як повітряних, так і морських, на глобальному рівні виникає гостра потреба в розробленні систем протидії та заходів безпеки. Поряд із розширенням функціоналу та масовим впровадженням БПА зростає також і ризик їхнього несанкціонованого використання для порушень безпеки, адже їх можна використовувати для шпигунства, диверсій і загроз інфраструктурі, що вимагає від державних та приватних структур розроблення ефективних та надійних методів їхнього виявлення, нейтралізації та запобігання використанню в заборонених цілях.

Проблема багатьох досліджень полягає в недостатній розробленості універсальних технологій протидії БПЛА, особливо з урахуванням різноманітності типів БПА - від повітряних до морських і підводних які мають різний ступінь автономності і вимагають диференційованих підходів до виявлення і нейтралізації. Існуючі методи захисту і протидії поки що не здатні охопити всі види загроз, що актуалізує необхідність розроблення міждисциплінарних рішень із застосуванням радіоелектронних, лазерних, мережевих, акустичних і оптичних методів.

Основною метою цього дослідження є розробка методологічних принципів побудови комплексної системи протидії БПА, яка об'єднує кілька технологій для забезпечення більш гнучкого та надійного захисту та проведення аналізу наявних методів протидії, оцінки їх технічної та економічної доцільності, а також запропонувати гібридний підхід для підвищення ефективності такої системи в умовах реального застосування.

Аналіз останніх досліджень і публікацій

Сучасний розвиток безпілотних літальних апаратів (БПА) як у повітряному, так і в морському середовищі представляє серйозні виклики для безпеки та стійкості різних об'єктів інфраструктури [1-3]. БПА здатні виконувати завдання розвідки, моніторингу і навіть атаки, залишаючись при цьому непомітними або важкодоступними для традиційних методів протидії. На поточний момент, більшість використовуваних протидійних технологій ґрунтується на радіоелектронному придушенні сигналів GPS і управління, лазерних системах, акустичних бар'єрах і фізичних методах перехоплення. Однак кожне з цих рішень має свої обмеження: наприклад, радіоелектронні методи залежать від лінії зв'язку, лазерні установки чутливі до погодних умов, а фізичне перехоплення ефективне тільки на обмежених відстанях.

Безпілотні апарати (БПА), діляться на повітряні та морські. До повітряних апаратів належать традиційні безплотні летальні апарати (БПЛА), здатні виконувати польоти на різних рівнях автономності. Морські безпілотні апарати (МБПА), зі свого боку, поділяються на підводні та надводні і застосовуються для моніторингу акваторій, дослідницьких місій і

розвідки. За ступенем автономності розрізняють БПА з ручним керуванням, напівавтономні та повністю автономні системи. Ручні та дистанційно керовані апарати вимагають постійного контролю оператора, тоді як напівавтономні виконують задані програми з мінімальним втручанням, а повністю автономні БПА можуть самостійно адаптувати поведінку залежно від умов навколишнього середовища [3,6, 9-11].

Згідно з останніми дослідженнями, БПА здатні використовувати системи навігації GPS, інерціальні навігаційні системи та інші датчики для досягнення високої точності у виконанні завдань, що відкриває широкі можливості для їхнього застосування в найрізноманітніших умовах [7-13]. Своєю чергою, таке зростання можливостей породжує необхідність розроблення адекватних заходів захисту, спрямованих на запобігання використанню БПА у розвідувальних або терористичних цілях, що стає одним із найактуальніших викликів.

Таким чином, використання будь-яких типів БПА та засобів протидії ним [12-16] представляє, як інноваційні можливості застосування, переваги, так і серйозні виклики, які потребують комплексного підходу до їхнього врегулювання та безпечної експлуатації.

Сфери застосування та загрози від безпілотних повітряних і морських апаратів і систем.

Повітряні безпілотні літальні апарати (БПЛА) широко застосовуються в різних галузях, таких як комерція, розвідка і військові операції, завдяки своїй універсальності, доступності та технологічним можливостям. У комерційному секторі БПА активно використовуються для доставки товарів і медикаментів, особливо у важкодоступні регіони. У сільському господарстві вони допомагають моніторити стан полів і застосовувати добрива, що збільшує продуктивність і знижує витрати. У сфері інфраструктури та будівництва БПЛА застосовуються для інспекції об'єктів, виявлення дефектів і моніторингу ходу будівництва. Екологічні служби використовують БПА для моніторингу стану навколишнього середовища, спостереження за змінами в екосистемах і для оцінки наслідків природних катастроф. У військовій сфері БПЛА відіграють важливу роль у розвідці та патрулюванні, даючи змогу отримувати дані про противника на значній відстані, без ризику для оператора. Також вони активно використовуються в тактичних операціях, де можуть виконувати як розвідувальні, так і ударні функції.

Морські безпілотні апарати (МБПА), включно з надводними і підводними безпілотними (неприв’язними, автономними) системами, також набувають дедалі більшого поширення. Надводні МБПА використовуються для моніторингу морських об'єктів, картографування акваторій, охорони, екологічного моніторингу тощо. Вони особливо корисні в океанографічних дослідженнях і в охороні і дослідженні морських ресурсів. Підводні БПА застосовуються для дослідження глибин океанів, виявлення об'єктів на дні, а також для розвідки в складних умовах, недоступних для традиційних суден. У військовій сфері МБПА часто задіяні для розвідки, патрулювання і забезпечення безпеки морських кордонів, евакуації тощо. Їх можна використовувати для виявлення підводних човнів, мін та інших об'єктів, які становлять потенційну загрозу.

На рис. 1 наведені основні сфери застосування БПА, найбільша частка з яких припадає на доставку та логістику. Далі, за популярністю, йдуть сільське господарство та будівництво. Окремо, БПА широко використовуються для охорони та безпеки, у військових операціях, екологічному моніторингу та забезпеченні пожежної безпеки.

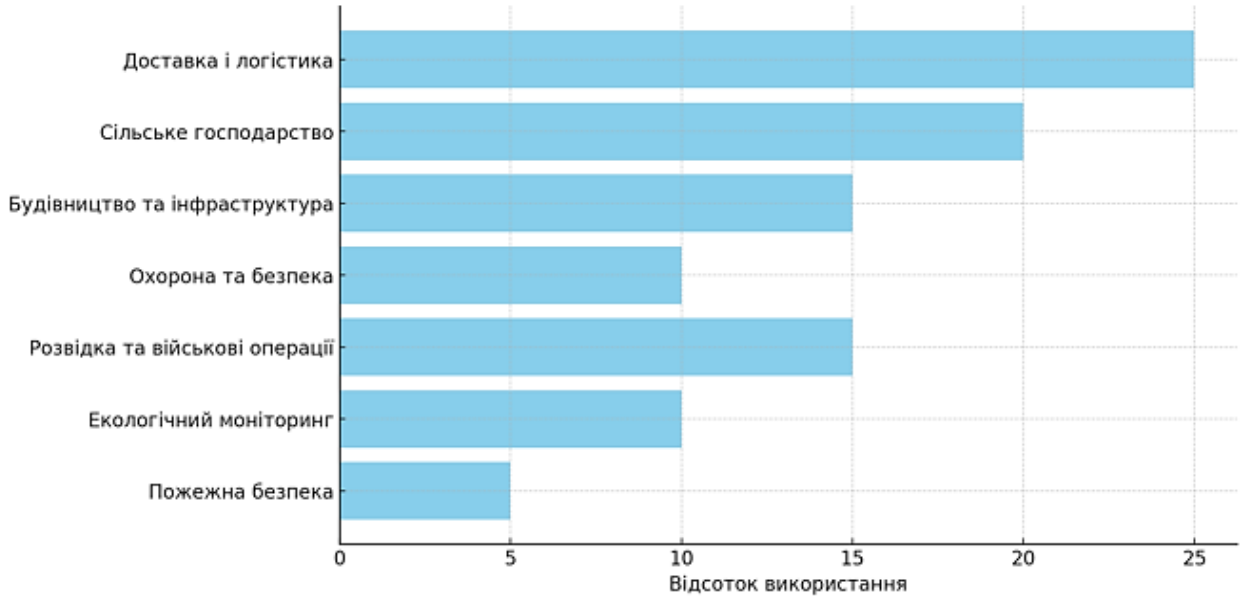

Рис. 1. Основні сфери застосування безпілотних технологій

Однак, широке поширення і використання БПА в різних галузях також створює і низку загроз. Повітряні БПА можуть використовуватися для незаконного проникнення в повітряний простір, шпигунства, збору конфіденційних даних і навіть нанесення точкових терористичних ударів. Такі загрози вимагають посилених заходів контролю та регулювання використання БПЛА. Наприклад, надводні та підводні МБПА можуть бути використані для непомітного спостереження за суднами, що може порушувати конфіденційність пересувань і безпеки. Вони також можуть відстежувати територіальні води, виявляючи місце розташування і маршрути військових кораблів або цивільних суден. В умовах збройних конфліктів МБПА можуть застосовуватися в диверсійних операціях, наприклад, для встановлення підводних вибухових пристроїв, збору даних про позиції противника, забезпечення зв’язку і телеметрії. Це створює необхідність розроблення заходів протидії для захисту морських кордонів і важливих морських та берегових об'єктів від несанкціонованого використання МБПА.

Технології та системи протидії безпілотним системам. Сучасні системи протидії несанкціонованому втручанню БПА включають кілька основних напрямків. В табл. 1 наведені основні технології, що застосовуються для протидії несанкціонованому втручанню повітряних і морських безпілотних апаратів. Головні з них такі, як радіоелектронні методи боротьби, лазерні установки, мікрохвильова та акустична зброя.

Важливим є також фізичне знищення і перехоплення, у тому числі за допомогою протидронових сіток і дронів-перехоплювачів.

Радіоелектронні методи боротьби включають глушіння і підміну сигналів управління і навігації БПА. Це здійснюється за допомогою перешкод на частотах зв'язку між БПЛА та оператором, а також блокування і підміну GPS-сигналів, що порушує систему навігації апарата. Такі методи ефективні, оскільки виводять БПЛА з-під контролю, що може призвести до його вимушеної або керованої іншим оператором посадки або відхилення від заданого курсу. Такі самі методи придушення і глушіння сигналів зв'язку і навігації можна використовувати для МБПА, включно з надводними і підводними апаратами. Однак для підводних МБПА застосування РЕБ обмежене, оскільки під водою сигнали GPS не працюють, і потрібно використовувати інші системи навігації, як-от інерціальні або акустичні. Зараз дуже розвиваються і методи квантової навігації, які вже мають практичне застосування і не залежать від зовнішніх сигналів.

Переваги радіоелектронних методів полягають у їхній відносній дальності дії та відсутності необхідності фізичного контакту з БПА. Однак вони можуть вплинути на роботу інших пристроїв у зоні дії, а також вимагають налаштування частот під конкретні моделі БПА.

Таблиця 1. Технології протидії безпілотним апаратам

Технологія	Опис	Переваги	Недоліки
Радіоелектронні методи (РЕБ)	Блокування каналів управління та навігації, глушіння GPS-сигналів	Ефективно порушує управління БПА та його навігацію	Може вплинути на інші електронні пристрої в зоні дії
Лазерні установки	Низько- та високоенергетичні лазери, спрямовані на виведення з ладу сенсорів або знищення БПЛА	Точне впливання на ціль, без побічних ефектів для навколишнього середовища	Залежність від погодних умов (туман, дощ) та обмежена дальність
Мікрохвильова та акустична зброя	Вплив мікрохвилями на електронні компоненти або акустична дестабілізація гіроскопів	Ефективно порушує роботу електроніки БПА, викликає втрату орієнтації	Небезпека для людей в зоні дії, обмежена дальність дії
Протидронові сітки та дрони-перехоплювачі	Використання антидронових сіток або дронів для фізичного захоплення апаратів, що порушують повітряний чи морський простір	Мінімальний ризик для навколишнього середовища, можливість безпечного приземлення захопленого БПА	Обмежена дальність та складність у застосуванні проти швидких або високолітаючих апаратів

Лазерні системи протидії являють собою низько- і високоенергетичні установки, спрямовані на виведення з ладу сенсорів і корпусу БПА. Низькоенергетичні лазери впливають на сенсори БПА, що робить його нездатним фіксувати об'єкти й орієнтуватися в просторі, порушують роботу відеокамер. Високоенергетичні лазери, своєю чергою, спрямовані на фізичне знищення БПА, пошкоджуючи його корпус. Для надводних БПА лазери можуть бути ефективними, особливо на малій відстані, де вони можуть пошкодити корпус або сенсори БПА. Підводні ж БПА недоступні для лазерного впливу, оскільки вода значно знижує ефективність лазерів, поглинаючи більшу частину їхньої енергії. Переваги лазерних установок полягають у їхній точності та можливості точкового впливу на об'єкт, що мінімізує побічні ефекти. Однак ефективність лазерів залежить від погодних умов (туман, дощ, сніг), що обмежує їх використання в складних метеорологічних і кліматичних умовах.

Мікрохвильова та акустична протидія впливає на електронні системи БПА, дестабілізуючи їхню роботу. Мікрохвильові випромінюючі установки створюють потужні радіохвилі, які пошкоджують внутрішню інформаційну електроніку апарата, що призводить до його виходу з ладу. Акустична зброя, найчастіше, спрямована на дестабілізацію гіроскопу і інклінометрів, що призводить до втрати БПЛА орієнтації. Попри те, що ці методи ефективні для нейтралізації БПА, вони мають обмежений радіус дії і можуть становити небезпеку для людей у зоні їх впливу. Мікрохвильова зброя ефективна для надводних апаратів, де вона може порушити електронні системи МБПА. Для підводних БПА мікрохвилі майже не застосовують, але акустична зброя є ефективним методом, оскільки звукові хвилі добре поширюються у воді. Акустичний вплив також може порушити роботу гіроскопів і навігаційної системи підводних апаратів.

Фізичне перехоплення БПА виконується не тільки за допомогою зброї (наприклад, зенітної), а і за допомогою дронів-перехоплювачів, які можуть автоматично визначати порушника, підходити до нього і випускати сітку, захоплюючи БПЛА і контрольовано приземляючи його на землю. Цей метод мінімізує ризик для довкілля і дає змогу зберегти БПЛА для подальшого аналізу і використання. Однак, перехоплення протидроновими сітками або дронами-перехоплювачами вимагає точного позиціонування і ефективне лише на обмеженій відстані, особливо в умовах високої швидкості або великих висот польоту. З урахуванням різниці в поведінці МБПА, фізичне захоплення надводних безпілотників можливе, особливо з використанням сіток або спеціальних перехоплювачів. Підводні МБПА

можуть бути захоплені за допомогою підводних пасток або спеціалізованих апаратів-перехоплювачів.

Схема на рис. 2 ілюструє системи протидії та різні методи перехоплення БПА.

Сучасні системи протидії безпілотним апаратам включають багато різних технологій, кожна з яких має свої особливості та сфери застосування але важливо враховувати, що ефективність методів може значно різнитися залежно від середовища, в якому використовується безпілотна система - повітряного чи морського. Для повітряних систем, наприклад, більш ефективними є лазерні установки та радіоелектронні методи, які можуть порушити управління та навігацію БПА.

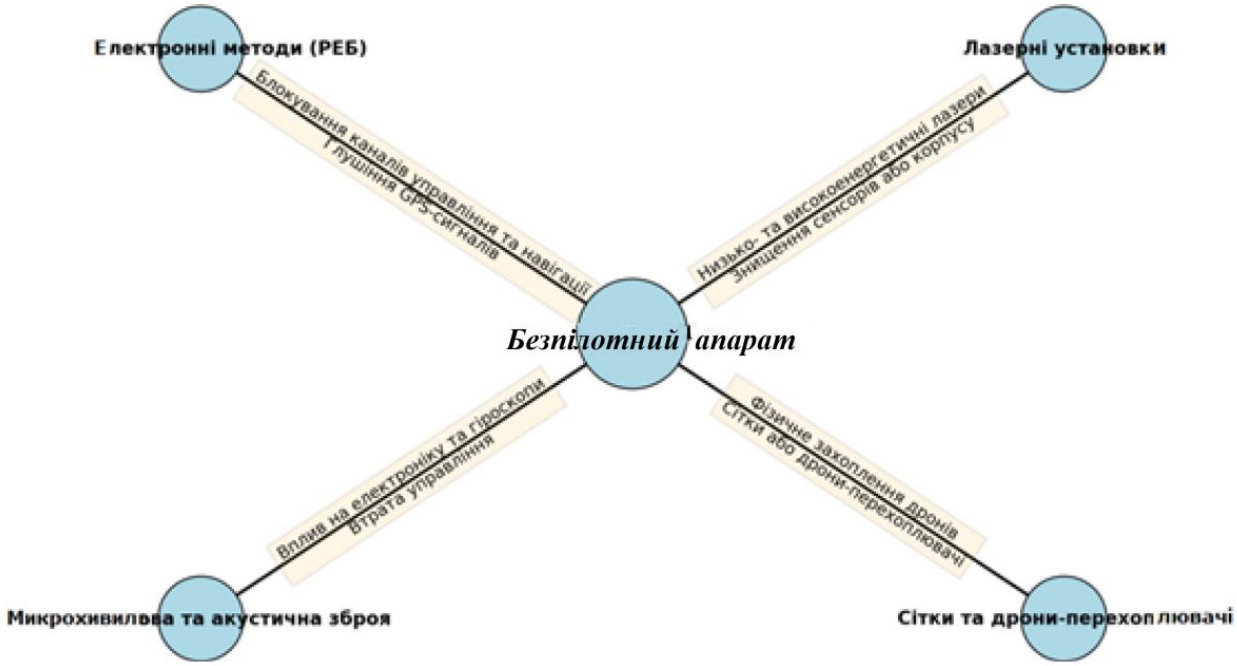

Рис. 2. Найбільш поширені системи протидії БПА

Для МБПА, особливо підводних, краще використовувати акустичну зброю, здатну дезорієнтувати навігаційні системи під водою. У Таблицях 2 та 3 продемонстровано дальність дії, сфери застосування та приклади ситуацій, у яких кожен із методів може бути використаний для протидії як БПЛА так і МБПА.

Таблиця 2. Характеристики та області застосування технологій протидії БПЛА

Технологія	**Дальність дії**	**Області застосування**	**Приклади ситуацій використання**
Радіоелектронні методи (РЕБ)	До кількох км	Прикордонні зони, охоронювані об'єкти	Охорона державних кордонів
Лазерні установки	До 2-3 км	Охоронювані об'єкти, військові бази	Знищення БПА у радіусі прямої видимості
Мікрохвильова зброя	До 300 м - кількох км	Охорона стратегічних об'єктів, військові бази	Захист об'єктів від БПА у ближньому радіусі
Сітки та дрони-перехоплювачі	До 300 м	Місця масового скупчення людей, спортивні заходи	Захоплення БПА-порушників перед місцями скупчення людей або масовими заходами

Таблиця 3. Характеристики та області застосування технологій протидії МБПА

Технологія	Дальність дії	Області застосування	Приклади ситуацій використання
Радіоелектронні методи (РЕБ)	До кількох миль	Охорона портів, стратегічних об'єктів	Захист від надводних і підводних дронів в портах
Лазерні установки	До 2 миль (надводні)	Охорона надводних об'єктів, військові кораблі	Знищення надводних дронів у радіусі прямої видимості
Акустична зброя	До кількох миль під водою	Підводне патрулювання, охорона акваторій	Виявлення і дезорієнтація підводних дронів
Сітки та дрони-перехоплювачі	До 2 кабельтових	Охорона портів, військові зони і спеціальні акваторії	Захоплення надводних порушників в акваторіях порту

На матричній діаграмі (рис. 3) показана ефективність різних технологій протидії для повітряних і морських БПА. Ступінь ефективності оцінювалась експертами за шкалою від 1 до 5, де 5 позначає максимальну ефективність. Можна побачити, що радіоелектронні методи (РЕБ) є високоефективними для обох типів БПА (5 для повітряних, 4 для морських), лазерні установки є більш ефективними для БПЛА (4) і менш ефективними для морських (2), оскільки надводні МБПА обмежують їхнє застосування, тоді як акустична зброя особливо ефективна для підводних морських БПА (5), але менш ефективна для БПЛА (3), і нарешті мережі та дрони-перехоплювачі мають середню ефективність для обох типів (3).

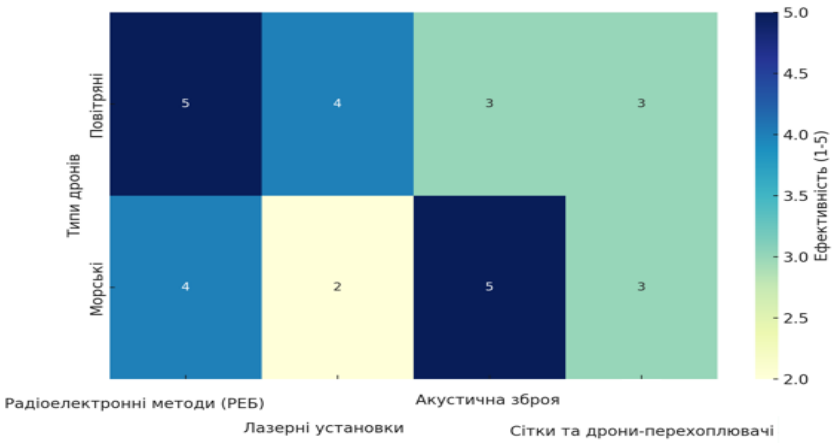

Рис. 3. Ступінь ефективності різних технологій протидії для повітряних і морських безпілотних апаратів

Спеціалізовані технології протидії морським безплотним апаратам. Окремо слід зазначити, що в умовах збільшення використання морських безпілотних апаратів для розвідки, моніторингу та можливих диверсій, проти них розробляються спеціалізовані технології. Ці технології націлені на протидію на підводні і на надводні апарати і містять у собі, як традиційні, так і інноваційні рішення. Такі технології протидії надають комплексний підхід до захисту від МБПА, забезпечуючи безпеку об'єктів і мінімізуючи ризики несанкціонованого проникнення або диверсій (табл. 4).

Таблиця 4. Технології протидії морським безпілотним апаратам і системам

Технологія	Опис	Переваги	Недоліки
Радіочастотне придушення	Створення перешкод в каналах зв'язку, порушення GPS та інших навігаційних сигналів, сигналів зв’язку та телеметрії	Порушення управління МБПА, ефективне для систем з навігацією через GPS	Може вплинути на інші системи зв'язку у зоні дії

Акустичні системи ідентифікації та придушення	Використання гідролокаторів для виявлення, акустичних засобів для дестабілізації сенсорів та комунікацій	Виявлення та дестабілізація підводних БПА на великій відстані	Може викликати небезпеку для навколишнього середовища у зоні дії
Сіткові та фізичні бар'єри	Спеціальні сітки, бони та бар'єри для захисту суден або об'єктів від підводних і надводних БПА	Фізичний бар'єр для захисту від проникнення БПА	Обмеження руху та доступу для безпечного транспортування
Оптичні та інфрачервоні системи виявлення	Візуальні системи для виявлення надводних БПА навіть при поганій видимості	Ефективне виявлення надводних БПА при низькому освітленні	Залежність від умов освітлення та погодних факторів
Електромагнітні імпульси (ЕМІ)	Спрямовані ЕМІ для виведення з ладу електроніки надводних БПА біля критичних об'єктів	Швидке виведення з ладу електроніки при наближенні БПА до об'єктів	Може вплинути на інші електронні пристрої поблизу об'єкта

Представлені в таблиці 4 технології протидії МБПА забезпечують комплексний підхід до захисту стратегічно важливих об'єктів і морських акваторій. Кожна з технологій має свої унікальні переваги і найкраще підходить для певних ситуацій. Наприклад, радіочастотне придушення та електромагнітні імпульси ефективно порушують роботу надводних БПА, особливо під час наближення до критичних об'єктів. Водночас акустичні системи ідеально підходять для виявлення і дестабілізації підводних БПА, мережеві та фізичні бар'єри створюють механічний захист від проникнення. Оптичні та інфрачервоні системи забезпечують візуальний контроль, що особливо важливо в умовах поганої видимості. У поєднанні, комплексно, ці технології створюють багаторівневий захист, мінімізуючи тим самим ризики несанкціонованого проникнення і потенційних загроз, пов'язаних з використанням МБПА.

Порівняльний аналіз методів, представлений у табл. 5, допомагає оцінити кожен метод за ключовими параметрами, включаючи радіус дії, точність, енергозатрати та стійкість до зовнішніх умов.

Таблиця 5. Порівняльний аналіз методів протидії безпілотним технологіям

Метод протидії	Радіус дії	Точність	Енергозатрати	Стійкість до погодних умов	Примітка
Радіочастотне придушення	До кількох км	Висока	Середні	Середня	Ефективно порушує канали зв'язку БПА
Лазерні установки	До 2-3 км	Дуже висока	Високі	Низька	Обмежено у тумані, дощі або снігу
Акустичні системи	До кількох км під водою	Середня	Середні	Висока	Ідеальні для підводних МБПА
Електромагнітні імпульси (ЕМІ)	До 300 м	Висока	Дуже високі	Середня	Може вплинути на електроніку у зоні дії
Сіткові та фізичні бар'єри	До 300 м	Дуже висока	Низькі	Висока	Фізичний захист від проникнення

Наприклад, радіочастотне придушення ефективне для порушення каналів зв'язку, але залежить від фізичних перешкод на шляху радіохвиль. Лазерні установки демонструють високу точність, але їх робота сильно залежить від видимості і фізичних перешкод. Акустичні системи найкраще підходять для підводних умов, тоді як фізичні бар'єри забезпечують максимальну точність та стійкість, хоча потребують встановлення.

Особливі методи боротьби з БПА. Такі методи боротьби з БПА включають більш гнучкі та нестандартні підходи, які доповнюють традиційні технології [12-16]. У цій частині дослідження розглядаються перехоплення управління і хакінг, використання тварин і ручної зброї, а також мобільні переносні пристрої. Перехоплення управління БПА передбачає злом зашифрованих каналів зв'язку і впровадження в його навігаційні системи, що дає змогу контролювати без пілотний апарат. Одним із ключових елементів тут є перехоплення сигналу і спуфінг GPS. Перехоплення сигналу або хакінг передбачає перехоплення керуючого сигналу і отримання доступу до переданих команд. Для цього використовують методи криптоаналізу, особливо якщо канал зв'язку захищений. Наприклад, злом зашифрованого каналу часто здійснюється через методи «грубої сили» або аналіз протоколів зв'язку:

$$P(t) = \sum_{i=1}^{n} K_i \cdot S_i(t), \tag{1}$$

де $P(t)$ - перехоплені дані, K_i - ключ шифрування, а $S_i\,(t)$ - вихідний сигнал.

Спуфінг GPS, або метод підміни навігаційних даних БПА помилковими GPS-координатами. Для цього створюються хибні сигнали, які БПА сприймає як реальні. Параметри спуфінгу можуть бути задані за формулою:

$$G'(x, y, z) = G(x, y, z) + \Delta G, \tag{2}$$

де $G(x,y,z)$ - істинні координати, а ΔG - введена помилка.

Використання хижих птахів для боротьби з дрібними БПА показало свою ефективність у ситуаціях, коли традиційні методи можуть бути обмежені, наприклад, у густонаселених або обмежених зонах. Навчені птахи захоплюють БПА, що мінімізує ризик для оточуючих. Але ці засоби є ще досить екзотичними, але вже є приклади застосування у ЗСУ.

Ручна зброя, адаптована для боротьби з БПА, також є корисним рішенням. Сучасні пристрої можуть пригнічувати сигнали на частотах від 433 до 5800 МГц, що дає змогу вивести з ладу системи управління БПА. Параметри для пристроїв можна задати так:

$$f_{зад} = f_{канал} \pm \Delta f \tag{3}$$

де $f_{\text{зад}}$ — частота придушення, $f_{\text{канал}}$ - частота сигналу БПА, а Δf - частота завадового впливу.

Також використовуються компактні переносні пристрої (РЕБ) для боротьби з безпілотними системами, які розробляються з урахуванням необхідності в мобільності та легкості. Сучасні комплекси, такі як системи типу "електромагнітної рушниці", дають змогу оперативно реагувати на загрози як у польових, так і морських умовах. Ці пристрої, зазвичай, працюють на кількох частотах, блокуючи управління і навігацію БПА. Такий підхід можна описати формулою:

$$P_{блок} = P_{пристр} - L(d), \tag{4}$$

де $P_{\text{блок}}$ - потужність блокування, $P_{\text{пристр}}$ - потужність пристрою, а $L(d)$ - втрати потужності на відстані d.

Додатково для моделювання ефективності радіочастотного придушення та його радіусу дії можна використовувати формулу втрат потужності сигналу залежно від відстані:

$$L(dB) = 20\log_{10}\left(\frac{4\pi d}{\lambda}\right), \quad (5)$$

де $L(dB)$ - втрати потужності сигналу в децибелах, d - відстань до БПА, λ - довжина хвилі сигналу. Дана формула надає змогу розрахувати, наскільки ефективно діятиме радіопридушення залежно від віддаленості БПА. Що більша відстань, то більші втрати потужності, і, відповідно, менш ефективне придушення. Це є корисним для оцінки необхідної потужності передавача за різних сценаріїв, наприклад, під час охорони морських об'єктів від БПА, для оцінки потужності джерела живлення пристрою придушення.

Дане дослідження має перспективну мету - створення методологічних умов та подальше застосування гібридної системи протидії БПА, що поєднує радіоелектронні, лазерні та акустичні методи для досягнення найбільшої ефективності.

Основні етапи роботи такої системи включають наступне.

1. Радіоелектронне придушення GPS і сигналів управління. В умовах поганої видимості або високої ймовірності виникнення перешкод радіоелектронні завади можуть порушувати навігацію БПЛА, знижуючи його керованість. Математична модель постановки перешкод для БПЛА може бути описана наступною формулою:

$$P_{\text{loss}} = P_{\text{signal}} \times (1-\eta)^{d} \quad , \quad (6)$$

де P_{loss} - потужність пригніченого сигналу, P_{signal} - вихідна потужність, η - коефіцієнт ослаблення залежно від використовуваної частоти, і d - відстань до цілі.

2. Використання лазерних установок для нейтралізації апаратів. Лазери спрямовуються і фокусуються на БПА для руйнування його оптики, елементів керування або обшивки/корпусу. Ефективність лазера на конкретній відстані R і погодних умовах розраховується з урахуванням показника заломлення і втрат потужності:

$$P_{\text{impact}} = P_{\text{laser}} \cdot e^{-\alpha \cdot R} \quad , \quad (7)$$

де P_{impact} - потужність на поверхні БПА, P_{laser} - вихідна потужність, α - коефіцієнт ослаблення (залежить від густини повітря і вологості). Чим більше α, тим нижча ефективність лазера, що пояснює вплив погодних умов.

3. Акустичний вплив для порушень навігаційної системи. У разі застосування акустичного впливу потужність акустичного сигналу Pacoustic на відстані d розраховується за формулою:

$$P_{\text{acoustic}} = \frac{P_{\text{source}}}{d^{2}} \quad , \quad (8)$$

де P_{source} - потужність джерела сигналу. Акустичний вплив найбільш ефективний на відстанях до кількох сотень метрів і переважно для морських БПА з простою електронікою.

3. Фізичне перехоплення. Цей метод застосовується для уловлювання БПА за допомогою сіток або спеціалізованих дронів. Важливими факторами при розрахунку ефективності фізичного перехоплення є швидкість і маневреність перехоплювального дрону, а також час на реагування:

$$T_{\text{intercept}} = \frac{D_{\text{initial}}}{V_{\text{intercept}} - V_{\text{target}}}, \quad (9)$$

де $T_{\text{intercept}}$ - час перехоплення, D_{initial} - початкова відстань між дронами, $V_{\text{intercept}}$ - швидкість перехоплення, а V_{target} - швидкість БПА.

Ці методи можна інтегрувати в єдину систему боротьби, яка в реальному часі обирає найбільш ефективний метод протидії залежно від характеристик БПА та умов навколишнього середовища. Така система дає змогу гнучко реагувати на різні загрози, забезпечуючи вищий рівень захисту.

На рис. 4 представлені графіки, що ілюструють ефективність різних систем придушення і перехоплення БПЛА, які дають змогу попередньо оцінити вплив різних параметрів на ефективність кожної системи, а саме:

а) ефективність радіоелектронного придушення - залежність пригніченої потужності сигналу від відстані;

б) вплив вологості на лазерне придушення - зниження потужності лазера зі збільшенням відстані за різних рівнів вологості;

в) ефективність акустичного впливу - зниження акустичної потужності зі збільшенням відстані;

г) час перехоплення - розрахунок часу для фізичного перехоплення БПА залежно від відстані до цілі.

Результати моделювання та експериментальні дані показують ефективність запропонованих методів в умовах реального застосування.

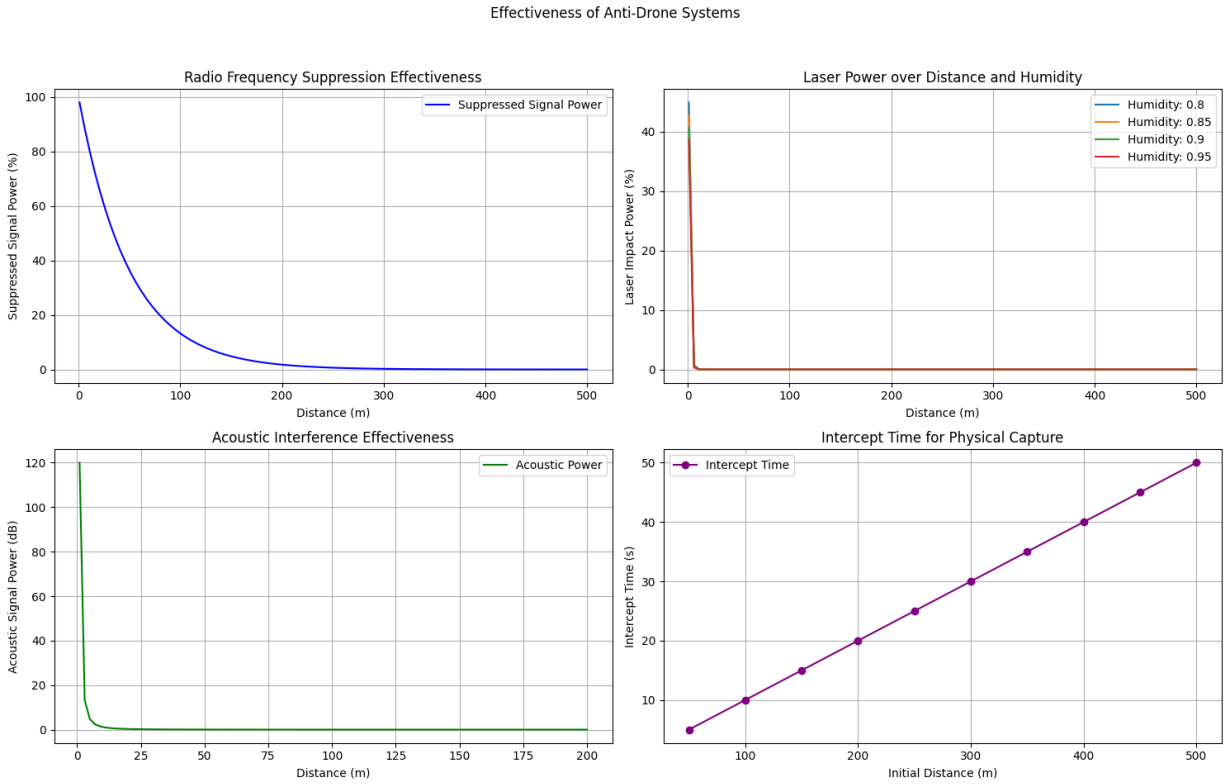

Рис. 4. Ефективність систем придушення і перехоплення безпілотних апаратів

Під час моделювання визначено, що радіопридушення дає змогу успішно порушити роботу GPS і керівних сигналів для більшості застосованих у сучасності БПА на дистанції до 500 метрів. Графік залежності втрат сигналу P_{loss} від відстані d демонструє експоненціальне падіння потужності сигналу, підтверджуючи високу ефективність методу в ближньому радіусі.

Лазерні системи показали високу результативність при перехопленні малих БПА в радіусі до 300 метрів, особливо за ясної погоди. На графіку залежності потужності на поверхні БПА *P*impact від відстані *R* і умов освітленості видно значний спад потужності у разі підвищеної вологості й опадів, підкреслюючи необхідність додаткового захисту в несприятливих умовах.

Що стосується акустичних сигналів, то вони ефективно впливають на малі БПА, особливо в морському середовищі, де на відстані до 200 метрів вдається придушити навігаційну систему БПА. Це показано на графіку залежності потужності акустичного сигналу *P*acoustic від відстані, що підтверджує ефективність методу при близькому контакті.

У сценаріях, коли потрібна нейтралізація БПА без його руйнування, фізичне перехоплення продемонструвало високу точність. Моделювання показує, що дрон-перехоплювач може досягти цілі на відстані до 100 метрів за $T_{\text{intercept}}$ секунд, з урахуванням відмінностей у швидкості та маневреності.

Результати показують, що запропонована методологія побудови перспективної системи протидії БПА має низку значних переваг, включно з гнучкістю, стійкістю до різних умов та економічністю. Тим не менш, кожен метод має обмеження, які роблять інтеграцію декількох технологій важливою для забезпечення надійності, безпечності використання і капіталовкладень.

Слід підкреслити що застосування комбінованого підходу дає змогу суттєво підвищити рівень захисту. Наприклад, лазери і радіоелектронне придушення можуть працювати паралельно, що забезпечує перехоплення БПА в умовах обмеженої видимості. Аналіз підтверджує, що комбінування лазерного придушення та акустичного впливу значно знижує ризик порушення роботи систем спостереження і наведення. Експериментальні дані показали, що різні методи мають різну ефективність залежно від погодних умов, навколишнього середовища і типів БПА. Тоді як лазери відмінно працюють за ясної погоди, акустичне та радіоелектронне придушення більш стійкі до умов вологості та опадів. Розгляд витрат на встановлення та обслуговування кожної системи показав, що радіоелектронне придушення та акустичні системи вимагають менших витрат порівняно з лазерними установками, що робить їх більш прийнятними для застосування у великих масштабах.

Розробки, інновації та подальші перспективи. Станом на сьогодні, різні країни активно розроблюють різні технології для захисту від БПА в умовах суші, повітря і моря. Серед ключових рішень - автономні системи виявлення і придушення, які включають сенсори, здатні автоматично ідентифікувати БПА і реагувати на них. Спеціалізовані дрони-перехоплювачі, оснащені сітками або системами блокування, демонструють високу ефективність у повітряному просторі, захоплюючи і нейтралізуючи порушників. Також створюються портативні засоби придушення, які можна використовувати в польових умовах: такі пристрої здатні блокувати управління БПА на дистанції, пригнічуючи GPS, радіоканали і телеметрію. Ці технології пропонують комплексні рішення для захисту стратегічних об'єктів у найрізноманітніших умовах і застосовуються військовими та охоронними структурами по всьому світу.

Сучасні тенденції у протидії безпілотним технологіям спрямовані на створення ефективних, адаптивних і автоматизованих систем. Застосування штучного інтелекту (ШІ) відіграє важливу роль у розвитку цих технологій, даючи змогу автоматизувати процес виявлення та нейтралізації БПА. Системи на основі ШІ здатні аналізувати і прогнозувати поведінку БПА, його маршрут, що робить їх більш ефективними і мінімізує необхідність втручання оператора.

У майбутньому слід очікувати появи універсальних систем, які ефективно захищатимуть від загроз, як у повітряному, так і в морському середовищі. Ці системи зможуть об'єднувати різні методи - від радіочастотного придушення і лазерного ураження до використання дронів-перехоплювачів і фізичних бар'єрів. Розвиток технологій ШІ та машинного навчання дасть змогу цим системам адаптуватися до нових видів загроз і

забезпечувати комплексний захист, незалежно від типу БПА і умов навколишнього середовища.

Висновки і перспектива подальшої роботи по даному напрямку

Дане дослідження слід вважати як перший крок до комплексної оцінки сучасних, найбільш поширених, стратегій протидії БПА, спрямованих на зниження операційних ризиків, які що створюються безпілотними системами як у цивільному, так і у військовому контексті. Оцінка різних технологій протидії БПА, включно з радіочастотним придушенням, глушінням, лазерними і мікрохвильовими засобами стримування, акустичними перешкодами і фізичним перехопленням, підкреслює важливість використання багатогранного підходу до загроз від БПА. Кожен захід протидії має унікальні переваги, такі як можливість точного наведення на ціль за допомогою лазерних систем або зона дії радіочастотних перешкод. Однак у кожного з них є й обмеження, які можуть знизити ефективність у конкретних умовах навколишнього середовища або експлуатації. Саме комплексне оцінювання, з урахуванням кошторису,безпеки використання та ефективності застосування є напрямком подальших досліджень.

Експериментальні випробування доводять, що жодне рішення для технологій протидії БПА не може забезпечити надійний захист від різних загроз з їх боку; натомість найвищої ефективності можна досягти, якщо використати гібридний підхід, який об'єднує декілька заходів протидії одночасно. Результати цього дослідження пропонують використання адаптивних, ситуаційних систем, які можуть динамічно підлаштовуватися під мінливу поведінку БПА, погодні умови і рівень загрози. Крім того, наведені прості принципи оцінки часу захоплення, швидкості придушення та енергоспоживання кожного контрзаходу закладають основу для майбутньої розробки адаптивних систем реагування. Саме тому подальші дослідження мають бути спрямовані на підвищення оперативної сумісності цих систем та вдосконалення алгоритмів управління для забезпечення швидкого реагування та мінімального споживання енергії. Оскільки технології БПА продовжують розвиватися, витонченість зі швидкість заходів у відповідь на ці загрози також має зростати.

ЛІТЕРАТУРА

[1] Yilmaz, A. (2024). Enhancing UAV crew performance and safety: A technology and innovation management perspective. *Sosyal Mucit Academic Review*, 5. https://doi.org/10.54733/smar.1512893

[2] Bamburry, D. (2015). Drones: Designed for product delivery. *Design Management Review*, 26, 40-48. https://doi.org/10.1111/drev.12315

[3] Karve International. (2024). The global impact of Ukraine's drone revolution on military forces. Retrieved from https://www.karveinternational.com/insights/the-global-impact-of-ukraines-drone-revolution-on-military-forces

[4] Zrelli, I., Rejeb, A., Abusulaiman, R., AlSahafi, R., Rejeb, K., & Iranmanesh, M. (2024). Drone applications in logistics and supply chain management: A systematic review using latent Dirichlet allocation. *Arabian Journal for Science and Engineering*, 49. https://doi.org/10.1007/s13369-023-08681-0

[5] Shafik, W., Matinkhah, S. M., & Shokoor, F. (2023). Cybersecurity in unmanned aerial vehicles: A review. *International Journal on Smart Sensing and Intelligent Systems*, 16. https://doi.org/10.2478/ijssis-2023-0012

[6] Haddal, C. C., & Gertler, J. (2010). Homeland security: Unmanned aerial vehicles and border surveillance. *Congressional Research Service*, 11.

[7] Sahawneh, L., & Ponton, J. (2017). Autonomy in drones: Applications and impacts. *International Journal of Robotics Research*, 36(2), 234-245.

[8] Elmokadem, T., & Savkin, A. (2021). Towards fully autonomous UAVs: A survey. *Sensors*, 21, 6223. https://doi.org/10.3390/s21186223

[9] Melnyk, O., Volianska, Y., Onishchenko, O., Onyshchenko, S., Kononova, O., & Vasalatii, N. (2022). Development of computer-based remote technologies and course control systems for autonomous surface ships. *International Journal of Computer Science and Network Security*, 22(09), 183-188. https://doi.org/10.22937/IJCSNS.2022.22.9.27

[10] Melnyk, O., Onishchenko, O., Onyshchenko, S., Voloshyn, A., Kalinichenko, Y., Rossomakha, O., Naleva, G., & Rossomakha, O. (2022). Autonomous ships concept and mathematical models application in their steering process control. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 16(3), 553-559. https://doi.org/10.12716/1001.16.03.18

[11] Мельник, О. М. (2023). Безекіпажне судноплавство як розвиток технологічних інновацій в морських перевезеннях [Unmanned shipping as a development of technological innovations in maritime transportation]. *Вчені записки ТНУ ім. Вернадського. Технічні науки*, 34(73) № 2, 152-157. https://doi.org/10.32782/2663-5941/2023.2.2/26

[12] Pascarella, D., & Gigante, G. (2022). A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones. *Drones*, 6(3), 65. DOI: 10.3390/drones6030065.

[13] Gonzalez-Jorge, H., Aldao, E., Fontenla-Carrera, G., Veiga-López, F., Balvís, E., & Ríos-Otero, E. (2024). Counter Drone Technology: A Review. *Preprints*. DOI: 10.20944/preprints202402.0551.v1.

[14] Gupta, N., & Ashraf, A. (2020). Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges and Future Trends. *arXiv Preprint*. DOI: 10.48550/arXiv.2008.12461.

[15] Tan, X., Wang, Z., & Sun, H. (2021). Toward Counter-Unmanned Aerial Vehicles: Detection, Jamming, and Anti-Jamming. *Sensors*, 21(8), 2656. DOI: 10.3390/s21082656.

[16] Anand, V., & Muthukumar, N. (2021). A Survey on Counter-Drone Solutions for High Security Environments. *Journal of Cyber Security Technology*, 5(4), 227-245. DOI: 10.1080/23742917.2021.1919809.