

## УДК 621.384.3

*Б.В. Сокол, студент гр. ПО-62м, В.Г. Колобродов, д.т.н., проф.,  
С.Г. Балінський, к.т.н., доц., І.В. Карпенко, студентка гр. ПО-62м  
КПІ ім. Ігоря Сікорського*

# ОПТИЧНІ ТА РАДІОЧАСТОТНІ МЕТОДИ І ЗАСОБИ ПРОТИДІЇ БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТАМ

**Анотація.** В даній роботі досліджено способи і методи протидії безпілотним літальним апаратам, а також вивчені існуючі технічні рішення країн світу. Важливість питання зростає з кожним роком у зв'язку з поширенням безпілотних літальних апаратів в комерції, тому гостро стоїть питання про безпеку їх використання. У зв'язку з підвищенням попиту відбулося зниження цін на складові, а також поширилось програмне забезпечення, що полегшує діяльність по створенню серій апаратів для військового застосування, але в той же час і збільшилася кількість у терористичних групах.

**Ключові слова:** безпілотні літальні апарати, оптичні та радіочастотні методи протидії.

## ВСТУП

Безпілотні літальні апарати (БПЛА) все більше знаходять широке застосування в нашому житті. Зокрема, в сільському господарстві БПЛА з GPS-навігацією використовуються при запиленні полів, чим досягається значна економія хімікатів і більш ретельна обробка посівів у порівнянні з традиційною пілотованою авіацією.

БПЛА використовуються для доставки медикаментів і гуманітарних вантажів в важкодоступні райони. Вони можуть застосовуватися для перевірки ліній електропередач і трубопроводів. ДСНС використовує дрони для моніторингу і прогнозування надзвичайних ситуацій та контролю за небезпечними об'єктами. Відстеження пробок на дорогах і заторів на річках під час льодоходу це мала частина того, що можна доручити беспілотникам.

На жаль, технічний прогрес в області безпілотної літальної техніки має і зворотний бік – існує можливість використання БПЛА в терористичних і розвідувальних цілях. В останні роки БПЛА активно розвиваються як напрям авіаційної військової техніки як в країнах Заходу, так і в нашій країні. Відсутність екіпажу, а значить і складних систем життєзабезпечення на борту, дає можливість БПЛА збільшувати дальність і тривалість польоту і корисне навантаження. Поява безпілотних апаратів є загальною тенденцією роботизації в збройних силах різних країн. БПЛА також стають засобом боротьби з міжнародним тероризмом, що досить сильно змінює традиційні методи ведення війни.

## МЕТОДИ ПРОТИДІЇ БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТАМ

В зв'язку з масовим поширенням дронів, багато структур, що забезпечують безпеку своїх країн, стали розробляти нові технології протидії літальним апаратам, але спочатку ціль потрібно виявити. Сучасні системи виявлення літальних апаратів представляють собою комплекс із радіолокаційних та оптичних систем. Перший елемент системи – це радар, що працює SHF(СВЧ)-діапазоні, невеликої потужності, але цього цілком вистачає, щоб виявляти цілі на відстані в декілька кілометрів. Далі в справу вступає спеціальна відеоспостережувальна система далекого виявлення, яка складається з декількох

камер, що можуть працювати в інфрачервоному та видимому діапазоні. Камери розпізнають відстежені радаром цілі, і передають інформацію для подальшої обробки оператором [1].

Одним з недоліків у дронів є конструктивна вразливість гіроскопів. Без цього пристрою не обходиться практично жоден дрон – без нього неможливий стійкий політ, і воно відповідає за зміни в просторовій орієнтації. Гіроскоп, як механічна система має резонансну частоту, якщо її підібрати, то пристрій увійде в резонанс і буде видавати невірні показання, які приведуть до аварії [2].

ВМФ США проводять випробування малопотужної лазерної системи, яка здатна виявляти, відстежувати і знищувати рухомі повітряні цілі на полі бою. Система розроблена компанією Boeing і здатна знищувати цілі, які наближаються до корабля: дрони, артилерійські снаряди та невеликі літаки, що низько летять. Такі системи прийнято називати LWS (Laser Weapon System), це одна з найбільш компактних систем лазерного захисту з числа розроблюваних в даний час, що забезпечує їй високу мобільність. Лазер здатний виявляти цілі на відстані до 35 км, ефективна зона ураження радіусом до 1.6 км [3].

Основою системи є твердотільний лазер, який працює в інфрачервоному діапазоні. Також він може працювати і в низькоенергетичному режимі для виведення з ладу сенсорів цілі, або в високоенергетичному – для знищення. Потужність до 30 кВт. Час знищення цілі – близько 2 секунд.

Зараз на озброєнні багатьох армій є велика кількість різноманітних систем радіоелектронної боротьби. Для успішного виведення з ладу ворожого дрона потрібно встановити частоти, на яких здійснюється управління апаратом, а потім «забити» їх перешкодами. У деяких дронів передбачений варіант обриву зв'язку з оператором [4]. У цьому випадку, якщо канал зв'язку втрачений, дрон переходить у відповідний режим роботи – автоматика перестає реагувати на всі сигнали ззовні і відповідно до заданої програми веде БПЛА до заздалегідь визначеного місця посадки, використовуючи систему GPS або ГЛОНАСС. Апарат використовує супутникову навігацію і визначає своє місце розташування, напрямок руху, відстань до оператора або точки посадки, щоб мати можливість повернутися на базу.

Щоб не допустити «евакуацію» дрона, засоби радіоелектронної боротьби повинні придушувати не тільки канал управління, але і сигнали навігаційної системи. В результаті успішного «глушіння» всіх цих сигналів противник, з високою ймовірністю, позбудеться техніки, що потрапила в зону дії системи радіоелектронної боротьби (РЕБ). Варто виділити зростаючий спектр засобів мобільних систем РЕБ, які часом називають "кібер гвинтівками". І не дивлячись на простоту і відносну дешевизну в порівнянні зі станціями РЕБ у неї є досить істотний недолік - вона використовує можливість передачі сигналів на частоті каналу керування безпілотною. Так можна вивести з ладу лише деякі моделі дронів, а не будь-який існуючий апарат. Автономним безпілотною, які не отримують будь-якого сигналу ззовні, така система не загрожує.

Системи перехоплення управління безпілотних літальних апаратів звичай доповнюють системи РЕБ або є самостійними комплексами, розгорнутими в певних межах міста. Серед основних способів злому БПЛА можна перерахувати наступні:

1. Злом шифрованого каналу або підміна даних авторизації і отримання за рахунок цього доступу до управління дроном.

2. Використання вразливостей програмного забезпечення, в тому числі переповнення буфера.

3. Використання інтерфейсів і каналів даних оригінального програмного забезпечення для "протягування" стороннього коду.

Дорогі БПЛА, які використовуються поліцією або іншими державними структурами, службами ДСНС і окремими компаніями в приватному секторі, досить просто зламати і викласти.

Існують лише дві основні вразливості, завдяки яким можливе перехоплення керування БПЛА:

1. Для зв'язку по Wi-Fi між модулем контролю безпілотного апарату і пристроєм управління як правило використовується дуже слабе шифрування, так як відомо, що WEP (Wired Equivalent Privacy) можна зламати за кілька секунд. Причому атакуючий може досить просто потрапити в з'єднання між дроном і оператором, перебуваючи на відстані близько ста метрів, і послати БПЛА неправдиву команду або відключити його від вихідної мережі.

2. Чіп Хбее, який використовується багатьма моделями дронів, небезпечний. Незважаючи на те, що Хбее підтримує шифрування, але через проблеми з продуктивністю і для виключення затримок між командами оператора і реакцією БПЛА, воно вимикається.

Внаслідок чого зловмисник має можливість здійснити атаку man-in-the-middle, перебуваючи на відстані двох кілометрів від дрона. Атакуючий може перенаправити пакети, заблокувати справжнього оператора, або пропускати всі пакети через себе, але найчастіше відбувається перехоплення керування та викрадення дрона.

Також для протидії використовують «тяжке» озброєння – ракети з головками самонаведення. Інфраредна головка самонаведення – це оптико-електронний пристрій, що працює на принципі виявлення світлових хвиль інфраредного діапазону, випромінюваних ціллю, призначений для ідентифікації цілі на навколишньому фоні і видачі в автоматичний прицільний пристрій сигнал захоплення, а також для вимірювання і видачі в автопілот сигналу кутової швидкості лінії візування. Оптична система, що представляє собою дзеркально-лінзовий об'єктив, встановлений на роторі гіроскопа і обертається разом з ним, збирає теплову енергію, що випромінюється ціллю, в фокальній площині об'єктива, де розташований модулюючий диск (радіально-щілинний растр). Безпосередньо за растром розташований іммерсійний приймач випромінювання, закріплений на внутрішній рамці карданного підвісу. Тепловий потік від цілі фокусується на растрі у вигляді плями. Завдяки нахилу приймального дзеркала при обертанні ротора гіроскопа пляма розсіювання «переноситься» по колу сканування на поверхні растра. На фото-

приймач падають «пачки» імпульсів теплового випромінювання, період проходження яких дорівнює періоду обертання (огинає частота) гіроскопа. Фотоприймач перетворює імпульси теплового випромінювання в електричний сигнал, який несе в собі інформацію про величину і напрямку кутової неузгодженості між оптичною віссю об'єктива і лінією візування мети.

## **ВИСНОВОК**

Підводячи підсумок застосовуваних методів і способів протидії, можна дати досить високу оцінку існуючої у світі можливості протистояти дронам, які вже кілька років успішно використовуються у військовій сфері. Існуючі розробки, оптичних та радіочастотних засобів протидії безпілотним літальним апаратам здатні досить ефективно боротися з порушниками, але все ж таки існують певні труднощі у їх виявленні, насамперед, це стосується невеликих за габаритами БПЛА та тих які використовують засоби маскування. Також, все ще гостро стоїть питання в області захисту приватності громадян у зв'язку з масовим поширенням дронів, які часто застосовують для зйомки великих груп людей під час заходів. Тому питання про відстеження БПЛА і контролем за дозволеною для них діяльністю на сьогоднішній момент залишається одним з найактуальніших.

## **СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Blighter. AUDS Anti-UAV Defence System // Counter Drone and Counter UAS Technology from Blighter Surveillance Systems. URL: <http://www.blighter.com/products/auds-anti-uav-defence-system.html>
2. (дата звернення 26.03.2018)
3. Son, Y., Shin, H., Kim, D., Park, Y., Noh, J., Choi, K., Kim, Y. (2015). Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors. *Usenix Security*, 881–896.
4. Jeff Stone. US Marines Test Boeing Laser To Knock Down Drones, Enemy Artillery// *International Business Times*. URL: <http://www.ibtimes.com/us-marines-test-boeing-laser-knock-down-drones-enemy-artillery-2011610> (дата звернення: 24.03.2018).
5. Williams, S., & McClelland, K. (2017). U.S. Patent No. 9,587,535. Washington, DC: U.S. Patent and Trademark Office.