

ТЕХНОЛОГІЇ ТА СИСТЕМИ ПРОТИДІЇ ЗАГРОЗАМ ВІД МАЛИХ ДРОНІВ

Кравчук С.О., Кравчук І.М.

*Навчально-науковий Інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна
E-mail:sakravchuk@ukr.net*

TECHNOLOGIES AND SYSTEMS FOR COUNTERING THREATS FROM SMALL DRONES

Technologies to counter drones (drone swarms) can have different purposes, but at the same time play an important role in ensuring security. All systems for countering drone threats can be divided into two broad categories: Monitoring Equipment and Countermeasures.

Технології протидії дронам (роям дронів) можуть мати різні призначення, але при цьому відігравати важливу роль у забезпеченні безпеки. У мирний час технології протидії дронам застосовуються для забезпечення безпеки повітряного простору навколо критично важливих об'єктів інфраструктури та великих заходів, таких як енергетичні вузли, спортивні ігри та музичні фестивалі, а також для захисту певних персон, приватних володінь та протидії проти будь-якої контрабанди в повітрі. У воєнний час (або в період терористичних атак) такі технології використовуються для захисту баз, складів, полігонів, військових кораблів, конвоїв та наземних підрозділів. Технології протидії дронам, для реалізації яких часто застосовуються неоднорідні сенсорні системи, у будь-якому своєму призначенні є складними багатоетапними процесами, що включають взаємодію між рядом окремих систем/об'єктів/сенсорів, а також між цими системами/об'єктами і оператором (людиною або штучним інтелектом) [1-3].

Усі системи опору загрозам дронів можна розділити на дві великі категорії: обладнання моніторингу та засоби протидії (Monitoring Equipment and Countermeasures).

Обладнання для моніторингу дронів може бути пасивним (простий огляд та прослуховування) або активним (випромінює сигнал та аналізує відбитий) і може виконувати такі функції: виявлення; класифікація та ідентифікація (розпізнавання); пошук та відстеження; оповіщення (якщо потрібно).

Більшість устаткування неспроможна виконувати одночасно всі перелічені вище функції, що знижує їх ефективність. У кращому випадку системи моніторингу повинні виявляти, ідентифікувати, визначати місцезнаходження і відстежувати дрон, що наближається. Залежно від типу системи, що використовується, сенсору, що виробляє початкове виявлення (наприклад, радіолокація), може знадобитися «перехресна передача» вторинним сенсорам, таким як оптичні матриці або електронні ідентифікаційні елементи, щоб підтвердити, що виявлений об'єкт, по суті, є дроном (а не птахом), а також визначити його точне місцезнаходження з відстеженням його переміщення.

Вторинні сенсори також можуть служити для надання додаткової інформації про дрон, яка допоможе визначити його намір. Наприклад, відеокамера може показати, чи дрон несе небезпечне навантаження – бомбу, озброєння.

Грунтуючись на інформації від усіх сенсорів системи моніторингу, оператор у дуже обмежений час має ухвалити рішення про те, як реагувати на виявлений дрон. Це не завжди може включати активацію системи протидії/захисту, особливо в мирний час.

Для перехоплення дрону застосовуються засоби протидії, що може призвести в залежності від техніки, що використовується, до різних наслідків. Наприклад, посадка дрону на землю (у разі глушіння чи спуфінгу), активація режиму «повернення додому», захоплення дрона (простими мережами), його повне чи часткове знищення.

Системи моніторингу дронів. Існують такі типи обладнання для моніторингу дронів: радіочастотні аналізатори (Radio Frequency (RF) Analyzers), акустичні датчики (мікрофони), оптичні датчики (камери), радар.

Радіочастотні аналізатори - це пасивні радіопристрою, які складаються з однієї або декількох антен для прийому радіохвиль та процесора для аналізу радіочастотного спектру. Вони використовуються на коротких відстанях для виявлення каналу радіозв'язку між дроном та його станцією, що управляє. При цьому деякі з них можуть визначати найпоширеніші моделі дронів або MAC-адреси як дрону, так і станції управління, особливо це стосується роботи в діапазоні Wi-Fi. Інші системи також можуть тріангулювати положення дрона та його станції керування при використанні декількох радіомодулів, розміщених у віддаленні один від одного.

Система з акустичних сенсорів (мікрофонів) є групою/набором мікрофонів, які вловлюють звук, що видається дроном, і визначають за допомогою тріангуляції напрямок на нього. Така пасивна система виявляє всі дрони в ближній зоні, у тому числі працюючі автономно. Виявляє дрони в умовах перешкод від землі. Однак дальність роботи акустичної системи обмежена невеликою відстанню до 500 м і дуже погано працює у шумній обстановці.

Оптичні сенсори (камери, матриці) можуть бути стандартними відеокамерами денного світла, так і інфрачервоними або тепловізійними. Вони надає зображення дрона та його корисного навантаження. Оптичні датчики мають високий рівень помилкових спрацьовувань, і погана робота у темряві, тумані та інших атмосферних турбулентності.

Радар – пристрій використовує радіохвилі для виявлення об'єкта. Радар випромінює сигнал і отримує відбитий сигнал від дрона, вимірює напрямок і відстань (положення) до об'єкта. Більшість радарів посилають свій радіосигнал у вигляді пакета, а потім прослуховують «луна». Багато радарів спроектовані так, щоб не виявляти дрібні цілі. Вони призначені для відстеження великих об'єктів, як-от літаки.

Системи для протидії дронам. У випадку заходи протидії дронам можна розділити на: фізичне знищення, нейтралізація, управління (захоплення). До обладнання протидії дронам відносяться: Radio Frequency Jammers, GPS

Spoofers, High Power Microwave (HPM) devices, Nets and Guns, High-energy lasers, Birds of Prey.

Подавлювачі радіочастот або радіочастотний глушник (Radio Frequency Jammers) - це стаціонарний або портативний пристрій, який передає через радіоканал великий потік енергії у бік дрону, маскуючи сигнал оператора. Така дія може призвести до того, що дрон здійснює керовану посадку в поточному положенні, повертається в задане користувачем домашнє місце, безконтрольно падає на землю або летить у випадковому напрямку. Такі пристрої можуть призвести до непередбачуваної поведінки дрона та створити радіоперешкоди іншим радіозасобам.

GPS-ошуканці посилають свій новий сигнал дрону, підміняючи зв'язок із супутниками GPS, які використовуються для навігації. Таким чином, дрон «обманюється» та отримує дезорієнтацію. Динамічно змінюючи GPS-координати в режимі реального часу, такий пристрій може контролювати положення дрону. Як тільки управління буде отримано, дрон може бути спрямований, наприклад, у «потрібному напрямку». Однак застосування таких пристроїв обмежено малою дальністю та можливістю впливу на (глушіння) інших засобів радіозв'язку.

Мікрохвильові пристрої високої потужності генерують великий електромагнітний імпульс (ЕМІ), здатний вивести з експлуатації електронні пристрої. ЕМІ створює перешкоди в радіоканалах та ушкоджує електронні схеми дронів (а також будь-які інші електронні пристрої в межах досяжності). Дані пристрої можуть ефективно не кінетично зупинити дрон, але вони створюють ризик ненавмисного порушення зв'язку або знищення інших електронних пристроїв у зоні дії, а дрон при їх дії миттєво безконтрольно падає на землю.

Сітки та зброя. Стрілянина сітками по дрону або інше контактування сітки з дроном викликає його зупинку та падіння. Така стрілянина мережею може бути реалізована із Землі з дальністю до 300 м, з іншого дрона або за допомогою підвісної мережі, яка розгортається зі спеціального «мережевого» дрону.

Високоенергетичні лазери є потужним енергетично оптичним приладом, що виробляє дуже сильно сфокусований пучок світла в лазерний промінь. Лазер вражає дрон, руйнуючи структуру та/або електроніку, проте має високу вартість, ризик побічної шкоди та великі габарити.

Література

1. Advanced in the telecommunications 2019: monograph / by edited M.Y. Ilchenko, S.O. Kravchuk, Kyiv, 2019, 336 p. (ISBN 978-617-7734-12-2).
2. Kaidenko, M., Kravchuk, S. (2023). Principles of Constructing Communication and Control Systems Protected from the Effects of Jamming Attacks for Small-Sized Unmanned Aerial Vehicles. In: Ilchenko, M., Uryvsky, L., Globa, L. (eds) Progress in Advanced Information and Communication Technology and Systems. MCiT 2021. Lecture Notes in Networks and Systems, vol 548. Springer, Cham. (ISSN2367-3370, E-ISSN2367-3389) – pp. 399-418, https://doi.org/10.1007/978-3-031-16368-5_20
3. Kaidenko M., Kravchuk S. Protection against the effect of different classes of attacks on UAV control channels // Information and Telecommunication Sciences. – No. 1 (2022) . – p. 35-43, DOI: <https://doi.org/10.20535/2411-2976.12022.35-43>