

Міністерство освіти і науки України
Сумський державний університет
Шосткинський інститут Сумського державного університету
Фармацевтична компанія «Фармак»
Управління освіти Шосткинської міської ради
Виконавчий комітет Шосткинської міської ради

ОСВІТА, НАУКА ТА ВИРОБНИЦТВО: РОЗВИТОК ТА ПЕРСПЕКТИВИ

МАТЕРІАЛИ III Всеукраїнської науково-методичної конференції

(Шостка, 19 квітня 2018 року)



Суми
Сумський державний університет
2018

СПОСОБИ ЗАХИСТУ ВІД АТАК БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

К.В. Пархоменко, А.В. Булашенко

Київський політехнічний інститут ім. Ігоря Сікорського
kostya.parkhomenko@gmail.com, an_bulashenko@i.ua

Останнім часом, в умовах АТО на сході України, що пов'язана з Російською агресією, знову набрало великого поширення використання безпілотних літальних апаратів (БПЛА). БПЛА діляться на апарати розвідувального та атакуючого типів. Під атакуючими БПЛА розуміють великі, озброєні ракетами апарати, що винищують задані цілі. Діяльність волонтерів-розробників засвідчила, що навіть індивідуально зібраний дрон з доступних для вільної купівлі комплектуючих може ефективно використовуватися як зброя [1]. У деяких випадках він діє ефективніше «професійних» способів здійснення атаки: від квадрокоптера, що раптово впав згори та є зарядженим пластидом з гайками, не врятують навіть найбільш натреновані охоронці та найкращі технічні засоби [2]. Актуальність проблеми використання БПЛА зорієнтувала наше дослідження на огляд відомих атакуючих систем та способи захисту від них.

БПЛА з'явилися в мирному житті відносно недавно. На них встановлюються камери, які знімають з повітря різні дії на землі та в повітрі. Ринок заповнений дешевими радіокерованими гелікоптерами та літаками з вже вбудованою камерою. Компанії Amazon та DHL в 2013 році офіційно заявили про намір доставляти покупки за допомогою безпілотників.

Однією з можливостей безпілотників є їх використання як зброї. Справа йде про використання «цивільних» та доступних до покупки безпілотників та їх компонентів як засобу враження слабо захищених цілей [2].

БПЛА типу «камікадзе» є мультикоптером, що містить заряд вибухової речовини. Такий безпілотник може сісти на дах автомобіля, залетіти за огорожу або у вікно приватного володіння та здійснити підриг в потрібній точці. Врятуватися від нього практично неможливо, небезпека такого типу безпілотників в тому, що важко відрізнити його від «літаючих камер».

Другий тип камікадзе називається «пкірувальник». Безпілотник після підтвердження цілі пікірує її, і наближаючись максимально близько, вражає ціль.

БПЛА типу «мул» використовується лише як носій стандартного озброєння. Сьогодні такий безпілотник, здатний збивати як приватні, так і пасажирські літаки, особливо на етапах злету та посадки, при цьому, не видаючи оператора. Ціль буде вражена з високим відсотком ймовірностей.

БПЛА типу «шукач» призначений для автоматичного пошуку та знищення будь-якої конкретної цілі. Такий безпілотник забезпечується спеціальною апаратурою пошуку цього виду цілей. Цей прототип призначений для атаки гелікоптерів. Безпілотник має три напрямки мікрофона. Швидкісні пропелери малого діаметра, що використовуються на безпілотнику, утворюють заваду значно великої частоти, ніж завада літаючого гелікоптера, який виділяється фільтрами. Задача безпілотника – вийти напереріз траєкторії польоту гелікоптера з тим, щоб останній врізався в нього. Вражають, в першу чергу, пілотів, оскільки схема бронювання транспортного гелікоптера передбачає атаку знизу і під невеликими кутами, верхня напівсфера майже завжди відкрита. Випробування показали, що безпілотник надійно знаходить гелікоптер в повітрі та особливо ефективний вночі, коли пілоти віддають перевагу прямолінійним рухам без різких маневрів. Проти цивільного гелікоптеру, що не очікує атаки, такий безпілотник може ефективно використовуватися в будь-який час доби.

Відомо, що системи спостереження та передачі даних американських безпілотників, до теперішнього часу, шифрувалися стандартними методами, або зовсім

не шифрувались. Канал передачі даних з БПЛА в наземний центр керування є слабким місцем безпілотників. Вперше про цей недолік стало відомому в Боснії в 1990-х роках під час військової операції. Це дозволило декілька років безперешкодно перехоплювати дані, що передаються з різних безпілотників, використовуючи апаратуру та програмне забезпечення, що вільно продається.

Можливість перехоплювати дані означає, що будь-який безпілотник, включаючи військові, що забезпечені ракетним озброєнням, може бути спрямований проти будь-якої цілі. Небезпеку становлять також комп'ютерні віруси, факт інфікування безпілотників Predator та Reaper вже були зафіксовані.

Сьогодні на заході набирають популярності два напрямки розвитку виробництва БПЛА. Один з них це розробка атакуючих безпілотників. Поки що, в основному, цим займаються відкриті компанії, що планують у майбутньому продавати свої вироби та технології армії та іншим легальним організаціям. Інший напрям розвитку виробництва БПЛА – розробка засобів протидії безпілотникам.

На сьогодні вразливим місцем безпілотників є широке використання в конструкціях доступних у вільному продажі компонентів для FPV. Говорячи про телеметрію, можна виділити стандартні діапазони частот, такі як 900 МГц, 1.2 ГГц, 1.3 ГГц, 2.4 ГГц, 5.8 ГГц. Потужність передавача значна – від 200 мВт до 1500 мВт, що дозволяє досить точно та наперед визначати наближення безпілотника або його присутність в певній зоні. Непрямою ознакою наявності безпілотника є також сигнал передавача радіокерування. Більшість сучасних безпілотників використовують електричні безколекторні мотори, що споживають струми до 100А. Перемикання обмоток мотора комутатором створює специфічний електромагнітний фон, що дедукується на дистанціях до 100м.

Одними із ефективних способів боротьби проти безпілотників є активна протидія лазерною зброєю. Звичайне вогнепальне озброєння малоефективне проти БПЛА. Проекти лазерної зброї ефективні в плані враження цілей, що низько летять. Ще одним проектом є автоматичні міни та зенітні гармати, що розсікають проліт безпілотника, та ті, що вражаються осколковим снарядом з барометричним датчиком.

Серед розроблених безпечних способів протидії безпілотникам можна виділити такі: постановка радіозавад, в тому числі, проти GPS/Глонасс приймачів, засліплення камер інфрачервоними прожекторами, створення невидимих повітряних вихрових завіс вздовж приватних володінь, в тому числі «розумних завіс», що вмикаються раптово за сигналом з датчиків з метою вразити безпілотник, встановлення захисних мереж, навіть створення спеціальних БПЛА для боротьби з безпілотниками, наприклад, шляхом скидання мереж на небезпечний дрон.

Отже, задача пошуку та знешкодження атакуючих безпілотників є все більше актуальним напрямом робототехніки та безпеки. Простота побудови таких засобів та доступність комплектуючих робить їх небезпечною зброєю. Наразі з цим збільшується необхідність створювати нові активні способи захисту від атак безпілотників, особливо в умовах агресивних дій гібридної війни Росії проти України.

Список використаних джерел

1. Капаякин В.В. Беспилотные летательные аппараты – новая реальность войны // Проблемы национальной стратегии. – 2015. – № 3 (30). – С.130–145.
2. Dunn D. H. Drones: disembodied aerial warfare and the unarticulated threat / David Hastings Dunn // International Affairs. – 2013. – Vol. 89, iss. 5. – P. 1237–1246.