ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ РАДІОКАНАЛІВ УПРАВЛІННЯ БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ

Переметчик Д.О., Смірнов А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному світі безпілотні літальні апарати (БПЛА) набувають усе більшого поширення в різних галузях, включаючи військову справу, сільське господарство, наукові дослідження, моніторинг навколишнього середовища, логістику та охорону правопорядку [1]. Однак з розвитком технологій зростають і ризики, пов’язані з безпекою систем управління безпілотниками, особливо радіоканалів, через які здійснюється їхній контроль і керування.

Метою доповіді є аналіз захищеності радіоканалів управління безпілотними літальними апаратами.

Одним із ключових аспектів безпеки БПЛА є забезпечення захищеності радіоканалів управління, які можуть бути вразливими до різних типів атак: перехоплення сигналу, втручання, глушіння або навіть захоплення управління апаратом [2]. Розвиток технологій БПЛА йде в ногу з розвитком засобів радіозв'язку, але разом з цим збільшуються ризики кібератак, зокрема перехоплення сигналу, спуфінг (підробка сигналу) і джемінг (глушіння сигналу). Особливу увагу викликають загрози, пов'язані з перехопленням даних, переданих через відкриті канали зв'язку, та можливістю зовнішнього втручання у роботу дронів. Зважаючи на підвищення кількості атак на радіоканали БПЛА, дослідження методів захисту стає вкрай актуальним. В роботі розглянуті сучасні методи шифрування та автентифікації, засоби захисту від глушіння та підміни сигналу, а також перспективи використання нових технологій для підвищення безпеки систем управління БПЛА. До найпоширеніших загроз належать:

– перехоплення сигналу БПЛА, що дозволить контролювати дії дрону або отримати важливу інформацію;

– спуфінг – коли зловмисник підробляє сигнал оператора, що може призвести до зміни маршруту польоту БПЛА або виконання небажаних команд;

– джемінг – глушіння радіоканалів, що може призвести до втрати управління дроном або його аварії;

– кібератаки на інфраструктуру – атаки на елементи системи управління, такі як наземні станції або сервери передачі даних.

Для захисту радіоканалів управління БПЛА пропонується низка методів і технологій, які забезпечують конфіденційність, цілісність та доступність сигналу.

Список літератури

1. Drone Development from Concept to Flight: Design, assemble, and discover the applications of unmanned aerial vehicles. Smit Sgarma C. 99–108.

2. Mykhatskyi, Oleksii. "Інформаційна безпека радіоканалів безпілотних авіаційних комплексів." *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»* 1.1 (2018): 56-62.