УДК 004.056.53:629.7

МЕТОДИ ПРОНИКНЕННЯ У СИСТЕМУ КЕРУВАННЯ БПЛА

Балай А.Є.
Науковий керівник – к.т.н., доц. Чумаков В.І.
Харківський національний університет радіоелектроніки, каф. ПЕЕА
м. Харків, Україна
тел. +38(095) 060-36-21

Unmanned Aerial Vehicles (UAVs), commonly known as drones, are used commercially, recreationally, and even militarily. However, the proliferation of UAVs has also raised new security concerns, especially with regard to hacking UAVs. A hacked drone can be used by an adversary for a variety of purposes, such as surveillance, sabotage, or to cause physical or material harm. A hacked drone can be redirected to veer off course or crash into a specific target, which can cause significant damage. In addition, information gathered by a hacked drone can be used to compromise sensitive data. Thus, it is critical for military individuals and organizations to take steps to protect against hacked UAVs and implement robust encryption and authentication protocols to avoid potential vulnerabilities.

З розвитком технологій і поширенням безпілотних літальних апаратів, зріс інтерес до їхньої безпеки. Злам безпілотних дронів - це серйозна загроза, яку можуть використати зловмисники для збору конфіденційної інформації, проникнення в захищені зони або навіть для створення аварійних ситуацій. У цьому контексті вкрай важливо розуміти, як саме можуть бути здійснені атаки на безпілотники і як їх можна захистити.

Дрони використовують супутникову геолокацію, щоб визначати своє положення і слідувати за заздалегідь заданою траєкторією польоту. Однак їхня залежність від GPS робить їх уразливими для кібератак, таких як спуфінг, коли зловмисники передають помилкові сигнали, змушуючи приймач дрона обчислювати неправильне положення. Це дає змогу зловмисникам контролювати траєкторію польоту дрона і навіть захоплювати його. Цей тип атак уже був використаний для захоплення американського безпілотника-невидимки 2011 року іранською армією. Однак, незважаючи на це, геолокацію дронів все ще можна використовувати для визначення їхнього становища та напрямку, необхідні спеціальні пристрої, які допомагатимуть уникати хибних сигналів.

Дослідники розробили метод виявлення спуфінг-атак, використовуючи GPS-приймачі, які вже присутні в дронах. Вони називають це методом "зміщення годинника", який виявляє різницю між часовими базами супутників і спуфера. Цей метод не вимагає додаткових компонентів або обчислювальних потужностей для вилучення даних і

може бути реалізований на літаючому безпілотнику для перевірки в реальних умовах.

Однак можливо, що зловмисник може синхронізувати час із супутниками, що може обійти цей метод.

Злом дрона може статися, якщо зловмисник отримає доступ до серверів FTP і root, які зазвичай не захищені паролем. Щойно зловмисник отримає доступ до цих серверів, він може легко отримати контроль над дроном. Це може призвести до серйозних наслідків, таких як втрата контролю над дроном і його знищення, а також можливі порушення приватності та безпеки даних, які можуть зберігатися на борту дрона. У зв'язку з цим, необхідно забезпечити належний рівень безпеки для всіх серверів, пов'язаних з управлінням дроном, і стежити за їхнім захистом від несанкціонованого доступу.

Рис. 1. Пристрій для перехоплення радіочастот від 1 МГц до 6 Ггц HackRF One.

З розширенням використання безпілотних літальних апаратів і розвитком їхніх технологій зріс інтерес до питань безпеки. Дрони використовують супутникову геолокацію для визначення свого місця розташування і проходження заздалегідь заданої траєкторії польоту. Однак через те, що вони залежать від GPS, вони стають уразливими для кібератак. У зв'язку з цим вкрай важливо розуміти, у який спосіб можуть бути здійснені атаки на безпілотники і як їх можна захистити.

Список використаних джерел:

1. Truong V. (2020). GNSS interference detection for autonomous UAV, 32(1), 42-60.

2. Thomas Brewster (2015). Watch GPS Attacks That Can Kill DJI Drones Or Bypass White House Ban, 2(1), 4-7.

3. Younes Al Younes (2016). Model-free approach for control, fault diagnosis, and fault-tolerant control : with application to a quadrotor UAV 25(4), 43-72.

4. Ralph DeFrangesco, Stephanie DeFrangesco (2022). The Big Book of Drones, ISBN 9781032062822.