УДК 004.056.53:629.7

МЕТОДИ ПРОТИДІЇ НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Світличний М.С.
Науковий керівник – д.т.н., проф. Чумаков В.І.
Харківський національний університет радіоелектроніки, каф. ПЕЕА
м. Харків, Україна
тел. +38(066) 619-77-46.

Unmanned aerial vehicles (UAVs) typically carry sensitive data and equipment that may be at risk of unauthorized access or hacking. Unauthorized access countermeasures in UAVs include technical and procedural measures that help ensure security and protection against such attacks. Among the technical measures, one can note the encryption of data transmitted and stored on the UAV and the use of network protocols with security. Procedural measures include ensuring the physical security of the UAV, prohibiting access to equipment without appropriate authorization, and controlling the activities of personnel who have access to the UAV.

Методи протидії несанкціонованому доступу у безпілотних літальних апаратах включають фізичні, програмні та адміністративні заходи.

Безпілотні літальні апарати (БПЛА) стають все більш поширеними та важливими для забезпечення різноманітних потреб у галузі транспортування, моніторингу, досліджень та іншого. Проте, разом зі зростанням застосування БПЛА, збільшується і ризик несанкціонованого доступу до цих систем, що може призвести до викрадення даних, порушення приватності, або навіть загрози для безпеки.

Для запобігання несанкціонованому доступу до БПЛА використовуються різні методи. Фізичні заходи включають контроль за доступом до фізичних роз'ємів та інтерфейсів БПЛА, застосування захисних кожухів, блокування пам'яті та інші заходи для унеможливлення прямого фізичного доступу до систем. Крім того, до фізичного впливу відноситься використання надпотужного електромагнітного випромінювання, що здійснює безпосередні деструктивні ефекти у радіоелектронних компонентах [1]. Програмні заходи передбачають захист БПЛА від несанкціонованого доступу шляхом застосування різних методів шифрування та аутентифікації, в тому числі алгоритмів з використанням публічних ключів, паролів та інших захисних механізмів. Адміністративні заходи включають контроль за доступом до БПЛА, створення правил використання БПЛА, навчання персоналу правилам використання та взаємодії з системами безпеки. Крім того, здійснюється моніторинг та аудит системи з метою виявлення можливих загроз та виявлення несанкціонованого доступу.

Узагальнюючи, комбінація фізичних, програмних та адміністративних заходів є найбільш ефективним методом захисту БПЛА від несанкціонованого доступу. Кожен з цих методів виконує важливу функцію в захисті системи, і їх комбінація забезпечує повністю захист

системи від загроз. Наприклад, фізичні заходи можуть унеможливити фізичний доступ до БПЛА, програмні заходи забезпечують безпеку під час зберігання та обробки даних, а адміністративні заходи дозволяють контролювати та моніторити доступ до системи та реагувати на можливі загрози. Загалом, відповідальність за захист БПЛА від несанкціонованого доступу лежить на розробниках, операторах та користувачах цих систем.

Застосування комплексу методів захисту дозволить забезпечити надійну захист системи від загроз та зберегти конфіденційність, цілісність та доступність даних, що зберігаються та оброблюються в системі.

Рис. 1. Пульт дистанційного керування дроном з провадженим кодом доступу

Висновуючи, можна сказати, що ефективна система захисту від несанкціонованого доступу у БПЛА має включати як технічні, так і процедурні методи, які забезпечують комплексний підхід до захисту інформації та обладнання від можливих загроз. Оскільки безпека БПЛА важлива для їх надійної роботи та захисту від зловмисників, протидія несанкціонованому доступу має бути невід'ємною частиною їхньої роботи.

Список використаних джерел:

1. Исследования воздействия электромагнитных излучений ультракороткой длительности импульса на радиоэлектронную аппаратуру СВЧ диапазона / Н.П.Гадецкий К.А.Кравцов, И.И.Магда, Ю.В.Прокопенко, В.Е.Новиков, Ю.В.Ткач, В.И. Чумаков / Материалы 6-й Международной Крымской конференции “СВЧ-техника и телекоммуникационные технологии” - Севастополь, 1996. - С.441-446.

2. Lee, H., Lee, J., Lee, Y., Kim, J., & Park, J. (2018). A survey on unmanned aerial vehicle safety and security management. Journal of intelligent & robotic systems, 91(1), 57-70.

3. Ramachandran, G., Shanmuganathan, S., & Srinivasan, V. (2018). Security for unmanned aerial vehicles: A survey. Unmanned Systems, 6(3), 195-217.

4. Tang, Y., & Cheng, X. (2019). An Overview of Security Issues and Countermeasures in Unmanned Aerial Vehicles. IEEE Access, 7, 7877-7891.

5. Weimerskirch, A., & Martin, C. (2020). Towards secure and trustworthy unmanned aerial vehicles: A survey on cybersecurity and safety challenges. Computers & Security, 88, 101612.