УДК 621.39

ЗАГРОЗИ БЕЗПЕЦІ ТА ПРОБЛЕМИ ВРАЗЛИВОСТІ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Гетьман О.В., Кайденко М.М., Роскошний Д.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: kkk610@ukr.net

Security Threats and UAV Vulnerability Issues

The article discusses the vulnerabilities of unmanned aerial vehicles. The classification of attacks for various features is given. The taxonomy of various types of known attacks, which can be exposed to UAVs, is presented.

Сьогодні безпілотні літальні апарати (БПЛА) використовуються в різних областях, таких як моніторинг, пошуково-рятувальні місії, комерційні послуги, наукові дослідження, сільське господарство, а також у військових цілях. БПЛА корисні в різних областях, але безпека завжди була головною проблемою. Крім того, БПЛА несе конфіденційну інформацію, пов'язану з конфіденційністю людей, і викликає серйозні проблеми, якщо дані використовуються зловмисниками. Було багато спроб вирішити проблеми безпеки БПЛА, але немає типового способу захистити БПЛА від різноманітних атак.

Важливим аспектом атак на БПЛА, включаючи його викрадення, який слід підкреслити, - це цілеспрямована атака, в тому числі і кібератака з точки зору термінології кібервійни [1], яка охоплює експлуатацію, напад, захист і асиметричну відповідь в цілому. Спроба викрадення - це комбінація кібер і електронних операцій/зусиль, а не захоплення одним клацанням миші, оскільки для цього потрібно кілька інструментів і різних методів з областей кібернетичної війни і електронної війни одночасно в серії дій для досягнення своєї мети, особливо коли метою є несанкціоноване використання безпілотника в терористичних цілях, або коли це є військовий БПЛА. Багатоступінчастий характер сучасних атак на БПЛА, заснований на координації індивідуальних дій [2], включає повністю виконану атаку з захопленням БПЛА, або перехопленням інформації. При цьому важливо знати всі вразливості безпілотного апарату та можливі дії зловмисників при атаках на нього.

Основними жертвами порушення безпеки безпілотного апарату є різні компоненти системи, такі як пристрої, мережі та канали зв'язку [3]. При цьому класифікація атак може здійснюватися за різними ознаками.

Всі атаки на БПЛА за місцем нанесення умовно можна розділити на:

- атаки, які здійснюються безпосередньо на БПЛА через безпроводові канал зв’язку, управління та телеметрії;
- атаки, які здійснюються на мережу управління БПЛА;
- атаки, які здійснюються на програмне забезпечення БПЛА.

Атаки на БПЛА за часом здійснення діляться на:

- атаки в реальному масштабі часу;
- атаки з відкладеним часом.

Атаки на БПЛА за цілями нанесення можна розділити на:

- атаки спрямовані на фізичне знищення БПЛА;
- атаки спрямовані на перехоплення управління БПЛА з метою несанкціонованого використання, або викрадення;
- атаки спрямовані на перехоплення інформації про БПЛА та цільової інформації, для отримання якої використовується безпілотний апарат, наприклад відео, дані з датчиків.

Типи атак, які застосовуються зловмисником істотно можуть відрізнятися в залежності від цільового використання БПЛА та способу його управління:

- автономний БПЛА з ручним управлінням оператором з автономного пульта;
- автономний БПЛА з автоматичним управлінням польотом за завданням з автономного пульта;
- автономний БПЛА з мережевим управлінням з використанням безпроводових технологій та мереж;
- мережа БПЛА (рій дронів) з автоматичним управлінням польотом, включаючи мережеве управління.

Загрози безпілотному апарату та корисній інформації, для збору та обробки якої він застосовується, несуть відповідальність за порушення безпеки і призводять до великих втрат з точки зору ресурсів, довіри і доступності [4]. На основі цих вразливостей атаки та їх вплив можна розділити на п'ять основних типів. На рис.1 представлена таксономія різних типів відомих атак на безпілотні апарати, які можуть були застосовані в залежності від цільового використання апарату, його типу та класу і цілей атаки.

Секретність є важливою проблемою для орієнтованої на дані безпеки, які збираються та обробляються за допомогою БПЛА, а обробка даних збільшує можливості загроз та вразливостей. Зловмисник націлений на безпілотний апарат для отримання конфіденційної інформації за допомогою різних підходів.

Цілісність визначає, що дані, які отримуються за допомогою БПЛА повинні бути послідовними, точними та надійними. Нелегітимні користувачі, або зловмисники не повинні змінювати передані дані в процесі обміну ними. Деякі з часто використовуваних механізмів захисту цілісності даних - це хеш-функції, контрольні суми тощо.

Конфіденційність гарантує, що інформація не може передаватися нелегітимним користувачам та бути отримана зловмисниками. Багато атак на БПЛА та наземну станцію управління є наслідком недоліків у безпеці. На конфіденційність впливає нелегітимний доступ для отримання корисної інформації.

Доступність визначається як послуги, що ініціюються негайно, коли це необхідно для підтримання правильної роботи. Доступність інформації полягає в тому, щоб законний користувач безпілотного апарату може отримати доступ до інформації на основі своїх вимог. БПЛА використовуються областях, які орієнтовані на виконання конкретних задач, тому доступність є основною проблемою щодо безпеки.

З новим етапом розвитку технологій пов’язані нові ризики. **Довіра** є важливим активом, і на неї впливають багато вимірюваних та невимірних властивостей, таких як , міцність, надійність, доступність та здатність. Безпека та конфіденційність - це дві, категорії, які впливають на довіру. Довірчі відносини залежать від організацій, які займаються розробкою та експлуатацією БПЛА. Різні загрози довірі виникають через неправильну конфігурацію та обмежене включення механізмів безпеки на етапах розробки та розгортання.

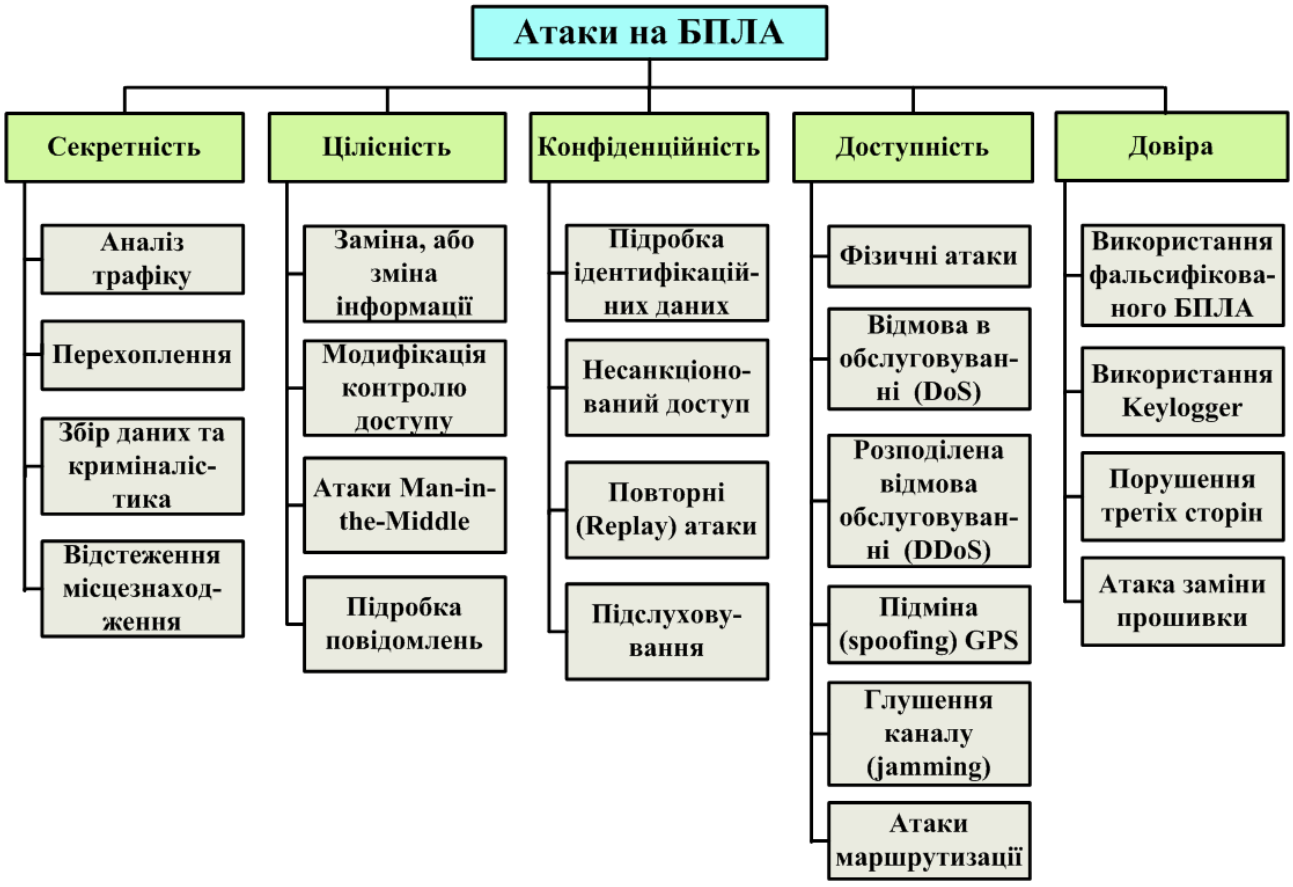

Рис.1. Таксономія різних типів відомих атак на БПЛА.

Література

1. S. M. Giray, "Anatomy of unmanned aerial vehicle hijacking with signal spoofing," *2013 6th International Conference on Recent Advances in Space Technologies (RAST)*, Istanbul, Turkey, 2013, pp. 795-800, doi: 10.1109/RAST.2013.6581320.
2. Yaacoub JP, Noura H, Salman O, Chehab A. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things*. 2020;11:100218. doi:10.1016/j.iot.2020.100218
3. M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits. Taxonomy for description of cross-domain attacks on cps. In Proc. of the 2nd ACM international conference on High confidence networked systems, Philadelphia, Pennsylvania, USA, pages 135–142. ACM, April 2013.
4. K. Mansfield, T. Eveleigh, T. H. Holzer, and S. Sarkani. Unmanned aerial vehicle smart device ground control station cyber security threat model. In Proc. of the IEEE Conference on Technologies for Homeland Security (HST’12),Waltham, MA, USA, November.