УДК 004.056.53
І. Фомін
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАХИСТ КАНАЛУ УПРАВЛІННЯ БПЛА ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

UDC 004.056.53
I. Fomin

PROTECTION OF UAV CONTROL CHANNEL FROM UNAUTHORIZED ACCESS

Як правило, основний обов’язок, який покладено на комплекси БПЛА(Безпілотний літальний апарат), – проведення розвідки важкодоступних районів, в яких отримання інформації звичайними засобами, включаючи авіарозвідку, ускладнене або ж є небезпечним для здоров’я та навіть життя людей. Крім військового використання застосування комплексів БПЛА відкриває можливість оперативного і недорогого способу обстеження важкодоступних ділянок місцевості, періодичного спостереження заданих районів, цифрового фотографування для використання в геодезичних роботах і у випадках надзвичайних ситуацій. Отримана бортовими засобами моніторингу інформація повинна в режимі реального часу передаватися на пункт управління для обробки і прийняття адекватних рішень.

В наш час найбільшого поширення набули тактичні комплекси мікро і міні-БПЛА. У зв’язку з більшою злітною масою міні-БПЛА за своїм функціональним складом найбільш повно представляє склад бортового обладнання, що відповідає сучасним вимогам до багато-функціонального розвідувального БПЛА.

Спостерігається різке збільшення застосування різних безпілотних авіаційних комплексів у всіх сферах життєдіяльності людини - від торгівлі до військової справи. Безпілотні авіаційні комплекси, як правило, включають в себе оператора (пілот-оператор, пункт управління), безпілотний літальний апарат та канали зв’язку, проте їх захисту від зовнішніх програмно-апаратних впливів, не дивлячись на зростання кількості інцидентів, не приділяється достатньої уваги.

Атаки можуть бути спрямовані на перехоплення управління, виведення з ладу БПЛА, отримання розвідувальної інформації або для подальшої атаки на пілота-оператора і взаємодіючі з ним системи.

Література.

1. Barnard J. Small UAV command-control and communication issues// IEEE on communicating with UAV’s. 2007.
2. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space. – Режим доступу : //www.official-document/cm76/7642/7642.pdf.