СПЕЦІАЛЬНІ РОЗРОБКИ

УДК 621.396.96

К.В. Заїчко,
начальник відділу ДНДІ МВС України, м. Київ

ДЕЯКІ АСПЕКТИ ФОРМУВАННЯ ВИМОГ ДО СИСТЕМ ПРОТИДІЇ БЕЗПІЛОТНИМ ПОВІТРЯНИМ СУДНАМ

У зв'язку зі швидким розповсюдженням безпілотних повітряних суден (БПС) широкого використання перед правоохоронними підрозділами набувають завдання унеможливити нанесення шкоди життю та здоров'ю громадян у випадках необережного або зловмисного застосування зазначених засобів.

У статті розглянуто принципи дії основних вузлів БПС широкого використання, проаналізовано канали зв'язку пультів дистанційного керування, приведено приклади формування контрмір для унеможливлення функціонування БПС та пультів дистанційного керування в умовах міської забудови. Запропоновано основні вимоги до вибору та створення систем протидії БПС.

Ключові слова: *безпілотне повітряне судно, контрміри, дистанційний пульт керування, вимоги до систем протидії.*

В связи с быстрым распространением беспилотных воздушных судов (БВС) широкого использования перед правоохранительными подразделениями ставится задача исключить возможность нанесения вреда жизни и здоровью граждан в случаях неосторожных действий или злоумышленного применения БВС.

В статье рассмотрены принципы действия основных узлов БВС широкого использования, проанализированы каналы связи пультов дистанционного управления, приведены примеры формирования контрдействий для исключения функционирования БВС и пультов управления в условиях городской застройки. Предложены основные требования к выбору и созданию систем противодействия БВС.

Ключевые слова: *беспилотное воздушное судно, контрдействия, дистанционный пульт управления, требования к системе противодействия.*

Due to the widespread use of unmanned aerial vehicles the tasks of law enforcement units are to prevent damage to life and health of citizens in cases of careless or malicious use of these means. Paper deals with the principles of the operation of the main unmanned aerial vehicles nodes of wide use, the channels of communication of remote control remote control are analyzed, examples of the formation of counter measures are made to prevent the operation of unmanned aerial vehicles and remote control in the conditions of urban development. The basic requirements for selection and creation of systems of counteraction to unmanned aerial vehicles are offered.

Keywords: *unmanned aerial vehicle, contrmeasures, remote control unit, requirements for counteraction systems.*

Безпілотні повітряні судна (БПС) є засобами, що активно використовують під час проведення спортивних заходів, фестивалей та інших видів розваг. Популяризація та зменшення вартості, покращення технічних характеристик БПС сприяють їх широкому та швидкому розповсюдженню. За оцінками аналітиків обсяги зростання ринку такого виду продукції в найближчому десятилітті будуть становити близько 30–50 %.

У засобах масової інформації дедалі частіше описуються випадки, коли з вини пілотів-початківців (у тому числі правопорушників) з використанням БПС трапляються як травматичні події, так і більш серйозні аварії, що супроводжуються людськими жертвами [1].

Одне з головних завдань правоохоронних органів – безпека життєдіяльності людей. На часі необхідність протидії протиправним застосуванням БПС. У зв'язку з цим, постає низка важливих питань щодо функцій систем протидії БПС, якими мають бути оснащені правоохоронці, щоб від їх впливу не було нанесено більшої шкоди (у випадку спроб застосування вибухових та ін. засобів).

Види загроз, що утворюються від використання БПС, було розглянуто у попередніх матеріалах [2]. Аспекти правового регулювання використання БПС виходять за рамки цієї статті. Можна зауважити, що (на момент підготовки матеріалів статті) реєстрації відповідно до чинного законодавства не підлягають у Державному реєстрі цивільних повітряних суден України безпілотні повітряні судна, максимальна злітна вага яких не перевищує 20 кг і які використовуються для розваг та спортивної діяльності (ст. 39, ч. 8 ПКУ) [3]. Отже, будь-яка особа може придбати без перешкод БПС відповідної дозволеної конфігурації і використовувати його на свій розсуд, крім місць, де використання БПС обмежено нормативно-правовими документами.

Нині у вільному продажу присутня достатня кількість пристроїв та систем протидії БПС. Для формування вимог до таких систем необхідне розуміння параметрів та характеристик БПС. Тож необхідно визначити види, на які система протидії буде мати відповідний вплив. Згідно з однією із запропонованих класифікацій [2] БПС можна розділити таким чином:

– дистанційно керовані – безпосередньо керуються оператором у зоні видимості через наземну станцію (пульт керування);

– дистанційно керовані – працюють автономно, але можуть потенційно керуватися пілотом (оператором), що використовують виключно зворотній зв'язок, через інші підсистеми контролю;

– автоматичні – виконують попередньо запрограмовані дії без керування пілотом та не мають можливості змінювати план дій під час польоту або адаптуватися до зовнішніх змін, але багаторазово можуть перепрограмуватися перед кожним вильотом з урахуванням зміни оточуючого середовища та зібраного матеріалу на попередніх польотах;

– дистанційно-керовані авіаційною системою – виконують низько-рівневе керування вбудованими системами або наземною станцією, а високо-рівневе керування траєкторії польоту та/або стан контролюється оператором;

– безпілотно-автоматичні – польотом керують вбудовані безпілотні автоматичні системи без втручання оператора або з використанням наземної станції, які можуть бути перепрограмовані з урахуванням змін до середовища або нових цілей [2].

Зосередимо увагу на першому типі з перерахованих вище БПС в аспекті опрацювання технічних заходів протидії. Як об'єкт протидії розглянемо модель БПС вартістю до кількох тис. у.о., що здатні підіймати корисний вантаж в межах 1 кг на висоту до 1 км з радіусом дії не менше 1 км та такі, що керуються каналами радіозв'язку з використанням пульта дистанційного керування.

Нерідко для протидії протиправному застосовуванню БПС пропонується використання придушувачів БПС постійної дії в широкій смузі радіочастотного діапазону або багатоканальних систем. Однак в умовах міста така позиція є неприйнятною, оскільки від дії подібних систем буде страждати значна кількість людей. У зоні впливу придушувача можуть бути заблоковані канали зв'язку зареєстрованих користувачів радіочастотного ресурсу (пожежної охорони, швидкої допомоги, поліції, систем оповіщення тощо) та звичайних користувачів ISM-діапазонів. Серед заблокованих пристроїв можуть опинитися автомобільні системи доступу (сигналізації) та деякі види мобільного зв'язку, що є порушенням чинного законодавства [4].

Тож спробуємо дослідити принципи, на яких можуть бути створені системи протидії БПС. Для цього розглянемо, на які саме функціональні модулі БПС варто створювати вплив та можливі наслідки.

На цей час все більше розповсюдження в цивільній сфері отримали FPV – БПС мультикоптери. FPV – це скорочене від англ. First Person View (від першої особи) – це спосіб керування БПС за допомогою відеокамери на борту, яка у реальному часі передає відеодані пілоту мультикоптера, що дозволяє керувати поза зоною зору людини. Мультикоптером будемо вважати БПС, що літає та реалізований за вертолітною схемою с трьома або більше гвинтами і використовує безколекторні електродвигуни та літійполімерні акумулятори як джерела енергії. Керують такими засобами дистанційно за радіоканалом контроллера (керування польоту) БПС та пульта радіокерування. Загальна схема керування показана на рис. 1. З пульта керування подаються задані команди на приймач БПС, після прийняття дані передаються на контроллер (керування польоту), який включає в себе реалізацію і розподілення усіх основних функцій мультикоптера. На основі прийнятої команди та показів датчиків, які реалізовані на конкретному апараті, вбудоване програмне забезпечення на основі певного алгоритму відправляє сигнали керування на двигуни БПС. Відповідно, контроллер є "мозком" апарату.

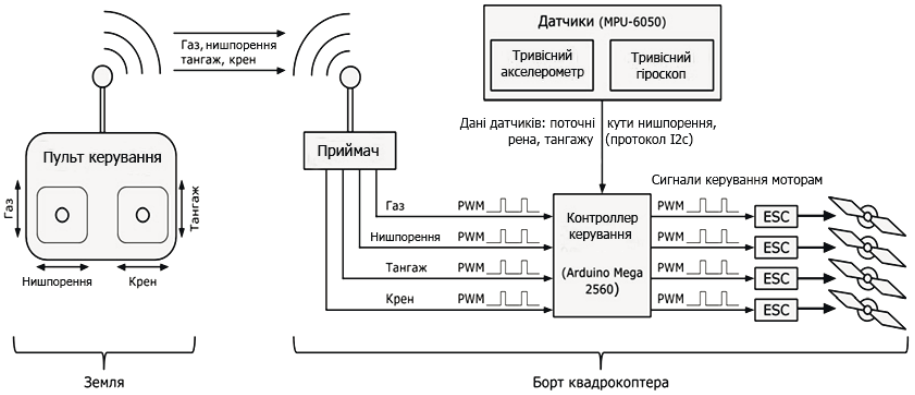

Рис. 1. Загальна схема взаємодії пульта керування та внутрішніх компонентів БПС на основі контроллера польоту.

Наведений приклад функціонування БПС дає змогу отримати уявлення щодо завдань головних модулів та можливості при здійсненні впливу як на канал керування, так і на канал позиціювання, а за необхідності створення адресних завад – вплив на контролер керування (у випадку інтелектуального впливу).

У системах протидії як основні заходи будемо розглядати вплив на радіоканал керування. Тож зосередимо увагу на безпроводових каналах зв'язку для дистанційного керування мультикоптерами. Відповідно до норм ряду країн ЄС канали зв'язку БПС загального користування мають бути не кодованими. Таких принципів дотримуються більшість виробників БПС, що є постачальниками продуктів, які серійно виготовляються, для ринку розваг та спорту.

Згідно з даними найбільшого розповсюдження отримали моделі БПС, орієнтовані на FPV взаємодії з пілотом [6]. До основних складових FPV систем можна віднести такі частини: камера, відеопередавач, відеоприймач, дисплей. Для передавання відеосигналу використовуються різні частотні діапазони. Найбільш розповсюджені частоти для передачі відео з БПС (серійного виготовлення):

- 900 МГц,
- 1,2–1,3 ГГц,
- 5,8 ГГц.

На цей час для передавання потокового відео з камери БПС більшість пристроїв використовують частоти діапазону 5,8 ГГц. Кожна частота має встановлену кількість каналів. На частоті 5,8 ГГц – 32 канали, що дає змогу пілотам підбирати вільні канали при одночасних польотах. Розглянуті характеристики обладнання керування деяких БПС загального користування, з можливістю пілотувати апарат від першої особи, найбільш розповсюджені згідно з даними станом на 2016 рік подані у таблиці 1.

Таблиця 1

Характеристики радіообладнання розповсюджених БПС загального призначення

	Частота радіозв'язку	**Потужність передавального модуля**	**Дальність передачі сингала**
DJI Phantom 3 Professional	2,4 – 2,483	20 dBm (відповідність FCC); 16 dBm (відповідність CE). За інформацією на RCGroups DJI Phantom 3 у Європі самостійно (автоматично за даними GPS) зменшує потужність передавача.	FCC: до 5 км (на відкритому просторі); CE: до 3,5 км (на відкритому просторі).
DJI Phantom 3 Standart	5,725 – 5,825 (Японія: 0,922 – 0,927)	20 dBm (відповідність FCC); 16 dBm (відповідність CE).	FCC: 1200 м; CE: 500 м (на відкритому просторі, в 120 м над точкою зльоту).
DJI Phantom 4 Professional	2,4 – 2,483	23 dBm (відповідність FCC); 17 dBm (відповідність CE).	FCC: 7 км; CE: 3,5 км; SRRC: 4 км.

Квадрокоптери компанії 3D Robotics – 3DR IRIS+, Solo, X8 та інші функціонують на базі контроллера польоту Pixhawk, який передбачає можливість роботи на двох частотах: телеметрія 915 МГц (США) або 433 МГц (ЄС), канал керування – 2,4 ГГц [6]. Згідно з рис. 2 керування здійснюється за допомогою

приймача-передавача 3DR Radio v2 на частоті 433 МГц (або 915 МГц залежно від моделі) та пульта дистанційного керування на частоті 2,4 ГГц. Інформаційний обмін здійснюється в пакетному режимі з використанням протоколу MAVLink. Цей протокол не використовує шифрування та використовується в більшості БПС загального користування літакового та вертолітного типу.

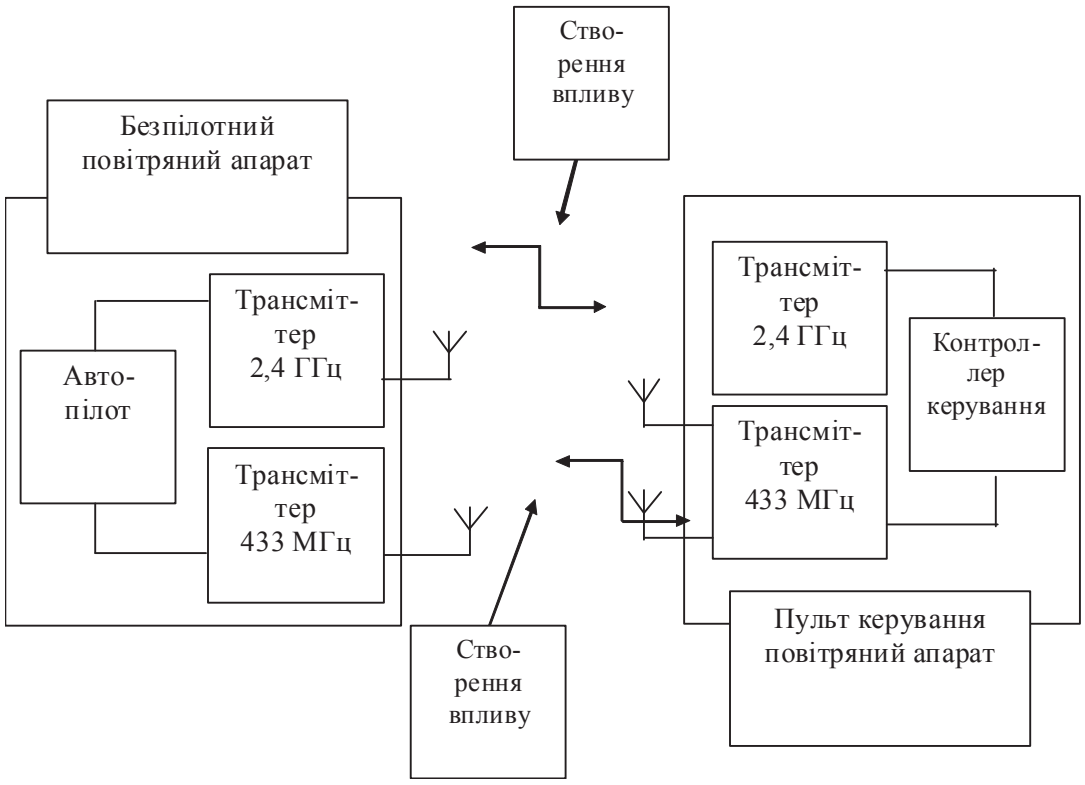

Рис. 2. Функціональна схема впливу на канал зв'язку БПС

Вплив на функціональні модулі БПС можна здійснювати через канал керування окремо на БПС так і на пульт дистанційного керування. Загальна схема створення впливу показана на рис. 2.

Важливе виявлення факту несанкціонованого використання БПС до початку старту та відповідно до виконання цим небезпечного завдання, оскільки відсутні гарантовані поведінки БПС в умовах постійнодіючих завад у радіоканалі (телеметрія та керування) та завад у GPS позиціюванні. За даними виробників, існує декілька сценаріїв, серед яких: поступове зниження висоти, повернення в точку старту та зависання, що в умовах вітру та щільної міської забудови може призвести до небажаних та непередбачуваних наслідків. Системи протидії БПС повинні мати готові сценарії роботи на момент вмикання пульта дистанційного керування.

Зосередимо увагу на особливостях згаданого вище протоколу. Розуміння його роботи дасть змогу формувати адресні контрміри.

MAVLink або Micro Air Vehicle Link – це протокол інформаційної взаємодії з БПС у т.ч. з пристроями, що перебувають на воді, землі і т.д. Зустрічається інша назва – MAV (Micro Air Vehicle) [5]. Протокол MAVLink (рис. 3) розповсюджується під GPL ліцензії (відкрита, що не потребує додаткових умов з її використання)

у вигляді модуля для python та генератора бібліотек під різні мови програмування, у тому числі header-only C/C++ бібліотеки. Є також репозитарії вже згенерованих бібліотек для MAVLink версії v1 та версіїv2.

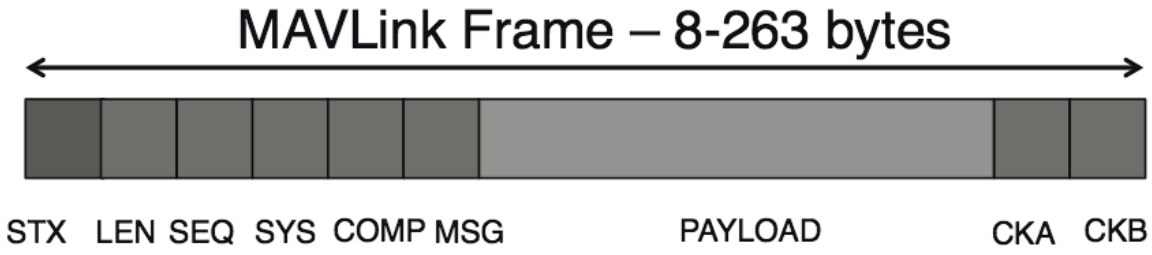

Рис. 3. Загальний вигляд графічного представлення протоколу MAVLink

Як було зазначено, протокол описує інформаційну взаємодію між системами, такими як MAV и GCS (Ground control station) – станція наземного керування, а також їх складовими частинами. Базовою сутністю MAVLink є пакет, що має наступний формат.

Перший байт пакета (**STX**) – це символ початку повідомлення: 0xFD для версії v2.0, 0xFE для версії v1.0, 0x55 для версії v0.9. **LEN** – довжина корисного навантаження (повідомлення). **SEQ** – вміщує лічильник пакета (0-255), який допоможе нам виявити втрату повідомлення. **SYS** (System ID) – ідентифікатор системи, що відправляє, а **COMP** (Component ID) – ідентифікатор компонента, що відправляє. **MSG** (Message ID) – тип повідомлення, від нього залежить, які дані будуть лежати в корисному навантаженні пакета. **PAYLOAD** – корисне навантаження, повідомлення, розміром від 0 до 255 байт. Два останніх байти пакета – **CKA** і **CKB**, нижній та верхній байт, відповідно, містять контрольну суму пакета.

Бібліотека MAVLink дозволяє кодувати та розкодувати пакети відповідно до протоколу, але вона не регламентує, якими апаратними і програмними засобами дані будуть відправлені – це можуть бути TCP/UDP повідомлення, обмін через послідовний порт, що забезпечує двосторонній обмін. Бібліотека обробляє вхідні дані побайтово, добавляючи їх у буфер та сама збирає з них пакет. Кожна система або компонент може одночасно обмінюватися даними за різними джерелами, тоді для кожного джерела назначається спеціальний ідентифікатор, що називається *channel* (канал). MAVLink містить буфер на кожний канал. Розглянемо на кількох прикладах формування підготовки та впливу на канал керування.

Приклад впливу на зазначений вище протокол наведено у [5]. Розглянемо основні кроки. Початок – отримання heartbeat з борту та ООП-обгортку поверх MAVLink. Приклади коду на C++ з використанням Qt. Обґрунтування вибору інструментів, у першу чергу, через те, що планується візуалізувати деякі параметри MAVLink з використанням Qt Quick і Qt Location. Введення AbstractLink, у його інтерфейсі визначає функціональність, що дозволить отримувати та передавати дані у вигляді QByteArray. Наслідники цього класу, UdpLink і SerialLink, забезпечать передачу даних мережею та через послідовний порт.

Інтерфейс класу AbstractLink. Пряму роботу з протоколом MAVLink інкапсулюють у клас MavLinkCommunicator. У його обв'язки будуть входити

отримання даних за каналами зв'язку та декодування їх до пакетів mavlink_message_t, а також відправка повідомлень за каналами зав'язку. Оскільки для кожного каналу зв'язку MAVLink вміщує свій буфер, вводиться словник вказівника на канал зв'язку до ідентифікатора каналу.

Інтерфейс класу MavLinkCommunicator. Розглянемо як відбувається збирання пакету з потоку даних. Оскільки MAVLink зчитує вхідний потік даних побайтово, для цього використовується функція mavlink_parse_char, яка повертає дані повідомлень або NULL, якщо повідомлення не може бути отримане, зберігаючи отриманий символ у внутрішній буфер. MAVLink вміщує буфер для кожного каналу. Такий підхід дозволяє передавати дані з послідовного порту напряму у функцію розбору пакета MAVLink.

Метод збирання пакета класу MavLinkCommunicator. Для отримання корисних даних одного тільки збирання пакета мало. Необхідно отримати з пакета повідомлення, виокреслити корисне навантаження згідно з ідентифікатором msgid. MAVLink має набір вмонтованих типів, під кожний msgid (тип повідомлення) та функції отримання цих повідомлень з пакета. Вводиться ще один абстрактний тип – AbstractHandler, в інтерфейсі цього класу визначають винятково віртуальний слот *processMessage* для обробки повідомлення, отриманого від MavLinkCommunicator'a. За допомогою класу AbstractHandler є можливість вирішити, чи буде можливість обробки того або іншого повідомлення. Наприклад, при обробці повідомлення типу heartbeat. Це базовий пакет, у якому система підтверджує, що вона існує. Варто звернути увагу, що heartbeat – це єдиний тип пакета, який MAVLink забов'язує використовувати. Вводиться обробник повідомлень цього типу – HeartbeatHandler.

Реалізація методу processMessage класу HeartbeatHandler. Якщо налаштувати класи та встановити правильно зв'язок, то є можливість і отримувати heartbeat повідомлення від контролера польоту. Є можливість скористатися парою радіомодемів та мікроконтролером (Raspberry Pi), на якому працює автопілот APM. Теоретично, це може працювати з будь-яким автопілотом, що підтримує поточну версію MAVLink.

Наведені вище приклади доводять можливість організації інтелектуального впливу на пульт керування та безпосередньо на БПС. Такі заходи контрмір мають бути частинами сценарію загальної системи протидії БПС. Спеціалізоване програмне забезпечення системи протидії БПС повинно мати в базі даних образи пультів керування, що постійно оновлюються відповідно до створюваних БПС та систем. Швидка ідентифікація пультів (через ID) дистанційного керування та адресна активація контрмір дасть змогу унеможливити виконання протиправних дій ще до зльоту БПС.

Створення завад та формування програмних кодів, що перехоплюють керування БПС, дасть можливість правоохоронним підрозділам вивести з небезпечної зони БПС порушника.

На основі викладеного матеріалу можна сформувати основні вимоги до вибору систем протидії БПС:

– багатоканальний аналіз сигналів та моніторинг каналів зв'язку на наявність БПС та дистанційних пультів керування;

– ідентифікація БПС за ID-адресами та поповнення бази даних;

– формування списків дозволених та заборонених БПС;

– створення інтелектуальної завади для пультккерування за попередньо сформованими сценаріями та відповідно до списків дозволених та заборонених БПС;
– формування інтелектуального коду для перехоплення БПС;
– моніторинг мереж на наявність БПС та дистанційних пультів керування;
– реєстрація подій, що пов'язана з протидією БПС;
– формування профілів загроз;
– отримання нових даних щодо створюваних систем керування розробниками БПС.

Висновки

З появою та розповсюдженням недорогих БПС та в умовах відсутності чіткого нормативно-правового регулювання обмежень з використання БПС буде збільшуватися навантаження на правоохоронні підрозділи. Виникає необхідність створення бази даних зареєстрованих користувачів БПС. Відповідно, впровадження систем протидії БПС у роботу правоохоронців є актуальним та важливим завданням. Розглянуті принципи дії БПС, пультів керування широкого використання, аналіз каналів їх взаємодії дозволили запропонувати принципи формування контрмір та визначити необхідність інтелектуального впливу (як на БПС, так і на пульт дистанційного керування в умовах міської забудови). Для вибору систем протидії БПС сформовано основні вимоги, що будуть корисними для правоохоронних підрозділів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Monitoring The Sky For Danger. URL: https://dronebusiness.center/monitoring-sky-12596/ (дата звернення: 06.11.2017).
2. *Білогуров В.А., Заїчко К.В.* Огляд систем виявлення та протидії безпілотним повітряним суднам в умовах міської забудови. Сучасна спеціальна техніка. 2016. № 4(47). С. 96–107.
3. Повітряний кодекс України: Закон України від 19 травня 2011 р. № 3393-VI. URL: http://zakon4.rada.gov.ua/laws/show/ 3393-17 (дата звернення: 07.11.2017).
4. Про радіочастотний ресурс України: Закон України від 01.06.2000 № 1770-III. URL: http://zakon.nau.ua/doc/?code=1770-14 (дата звернення: 08.11.2017).
5. Разбираемся в MAVLink. Часть 1. URL: https://habrahabr.ru/post/312300 (дата звернення: 06.11.2017).
6. *Бондарев А.Н., Киричек Р.В.* Обзор беспилотных леталельных аппаратов общего пользования и регулирования воздушного движения в разных странах. Информационные технологии и телекоммуникации. 2016. Т. 4., № 4. С. 13–23.

Отримано 28.11.2017
Рецензент Марченко О.С., к.т.н.