<https://doi.org/10.38013/2542-0542-2021-2-35-41>

УДК 629.3.066.32

Комплекс перехвата управления БПЛА

Э. А. Аджухунов, О. В. Николаев

Федеральное государственное автономное учреждение «Военный инновационный технополис «ЭРА», Анапа, Российская Федерация

В работе представлен вариант решения задачи перехвата управления беспилотников по радиоканалу, а также используется спуфинг сигналов глобальной навигационной системы (GPS, ГЛОНАСС). В ходе работы была проведена разработка структурной схемы, алгоритма работы комплекса, а также получены экспериментальные данные.

Ключевые слова: БПЛА, спуфинг, перехват управления

Для цитирования: Аджухунов Э. А., Николаев О. В. Комплекс перехвата управления БПЛА // Вестник Концерна ВКО «Алмаз – Антей». 2021. № 2. С. 35–41. <https://doi.org/10.38013/2542-0542-2021-2-35-41>

For citation: Adzhakhunov E. A., Nikolaev O. V. UAV control hack system // Vestnik Koncerna VKO "Almaz – Antey". 2021. No. 2. P. 35–41. <https://doi.org/10.38013/2542-0542-2021-2-35-41>

Поступила 22.01.2021 Отрецензирована 17.02.2021 Одобрена 09.03.2021 Опубликована 18.06.2021

Введение

Задачи перехвата БПЛА в настоящее время решаются в основном с использованием заградительных помех, физического воздействия. Данные методы имеют существенный недостаток: полное или частичное разрушение БПЛА, что может привести к разрушению объектов и нанесению вреда здоровью человека. Также существенное развитие приобретают системы с полным перехватом управления по радиоканалу и системы, использующие спуфинг атаки, но данные устройства используют каждый метод в отдельности, что может приводить к переключению системы управления беспилотником на другой способ управления [1].

Общая схема управления БПЛА по радиоканалу представлена на рисунке 1. С пульта управления подаются заданные команды на приемник БПЛА, после приема данные передаются на полетный контроллер, который включает в себя реализацию и распределение всех основных функций беспилотника.

На основе принятой команды и показаний датчиков, которые реализованы на конкретном аппарате, встроенное программное обеспечение на основе определенного алгоритма отправляет управляющие сигналы на двигатели БПЛА. Следовательно, полетный контроллер является своего рода «мозгом» летательного аппарата [2].

Вид, модуляция и частота управляющих сигналов зависят от протокола связи между передатчиком и приемником на борту БПЛА. Протоколы, используемые в передатчиках, часто реализованы только одним производителем. Некоторые бренды позволяют использовать несколько протоколов, в зависимости от имеющихся приемников.

Приведем обзор технических характеристик распространенных моделей систем управления БПЛА в таблице 1.

Все рассмотренное оборудование работает на частотах от 2,4 до 2,485 ГГц с модуляцией *QPSK* (*Quadrature Phase Shift Keying* – квадратурной фазовой манипуляции) и *GFSK* (*Gaussian Frequency-Shift Keying* – гауссовская частотная манипуляция).

Рис. 1. Общая схема взаимодействия пульта управления и внутренних компонентов БПЛА на основе полетного контроллера Arduino Mega 2560

Таблица 1

Технические характеристики систем управления БПЛА

Оборудование	Частота радиосвязи (ГГц)	Мощность передающего модуля, Вт	Дальность передачи сигнала, м	Чувствительность, dBm	Режим модуляции
DJI Phantom 3 Professional	2,4–2,485	0,2	2000	–99	QPSK
Syma	2,4–2,485	0,1	1000	–90	GFSK
Radiolink at9s	2,4–2,485	0,1	1500	–98	QPSK
Flymind XT11	2,4–2,485	0,15	800	–98	QPSK
Spektrum DX8	2,4–2,485	0,2	1200	–90	GFSK
FlySky FS i6	2,4–2,485	0,1	900	–93	GFSK

Разработка комплекса

В ходе исследований был разработан комплекс на основе приемо-передатчика, который принимает управляющие сигналы с пульта управления БПЛА, производит обработку и имитацию управляющих сигналов. Одновременно с этим данный приемо-передатчик передает ложные координаты ГНСС. Приемопередатчик был разработан по методике программно-определяемой радиосистемы (SDR) [3].

На рисунке 2 представлена структурная схема разработанного комплекса, где АС – антенная система, АПК – антенный переключатель, ППФ – полосно-пропускающий фильтр, КДМ – квадратурный демодулятор, КМ – квадратурный модулятор, МШУ – малошумящий усилитель, УМ – усилитель мощности, АЦП – аналогово-цифровой преобразователь, ЦАП – цифро-аналоговый преобразователь, БОС – блок обработки сигналов.

В таблице 2 приведены обобщенные технические характеристики комплекса перехвата управления.

Посредством микропроцессора на управляющие контакты входного СВЧ-переключателя поступает определенный логический сигнал. С помощью этого сигнала происходит переключение между каналами переключателя. Тем самым происходит переключение между сигналами антенны, передатчика и приемника. Далее сигнал поступает на каскад усиления, в данном случае на малошумящий усилитель (МШУ), где происходит усиление сигнала и последующая его селекция полосно-пропускающим фильтром (ППФ).

Для учета квадратурной фазовой манипуляции (QPSK) и избежания потери информации, заложенной в фазе, в качестве сигнала гетеродина формируется сигнал комплексной экспоненты, или, иначе говоря, синусоидальный и косинусоидальный сигнал одновременно.

В результате происходит деление на квадратурные компоненты I и Q путем смешивания с сигналом гетеродина, который регулируется синтезатором частот с ФАПЧ.

АС – антенная система

АПК – антенный переключатель

МШУ – маломощный усилитель

ППФ – полосно-пропускающий усилитель

АЦП – аналого-цифровой преобразователь

КМ – квадратурный модулятор

КДМ – квадратурный демодулятор

БОС – блок обработки сигналов

ЦАП – цифро-аналоговый преобразователь

УМ – усилитель мощности

Рис. 2. Структурная схема комплекса по перехвату БПЛА

Таблица 2

Технические характеристики разрабатываемого комплекса

Частота	2,4–2,485 ГГц – для управления по радиоканалу, 1,246–1,602 ГГц – для спуфинга
Чувствительность приемника	–102 дБм
Коэффициент усиления приемного тракта	12 дБ
Коэффициент шума приемной части	7 дБ
Мощность передатчика	1 Вт

Сигналы оцифровываются в АЦП и подаются на микропроцессор, где происходит фильтрация и обработка сигнала, выявление протокола управления и генерация своих сигналов управления. Процесс сравнения осуществляется с помощью метода корреляционного анализа сигналов [4].

После генерации сигналов в БОС происходит цифро-аналоговое преобразование, селекция и усиление сигналов управления.

Параллельно происходит генерация и передача ложных координат ГНСС. Указывается группировка спутников GPS через файл эфемерид GPS-трансляции. Файл эфемерид ежедневного GPS-вещания (*brdc*) представляет собой слияние отдельных файлов навигации в один.

Эти файлы используются для генерации смоделированной псевдодальности и доплеровского режима для спутников GPS в поле зрения. Эти смоделированные данные о дальности затем используются для генерации оцифрованных выборок *I/Q* для сигнала GPS.

Для увеличения скорости вычислений блок обработки сигналов строится на базе программируемой-логической интегральной схемы (ПЛИС) *Artix7* [5].

Детально рассмотрим входной модуль антенного переключателя. Входной модуль представляет собой СВЧ-переключатель, к которому подключаются приемный тракт, передающий тракт и антенна через соответствующий переход. Структурная схема входного СВЧ-блока представлена на рисунке 3.

Рис. 3. Структурная схема входного СВЧ-блока

В качестве переключателя была выбрана микросхема *HMC595A* от производителя *Analog Devices*. На рисунке 4 представлена схема электрическая принципиальная соответствующего модуля. Подключение данной микросхемы простое и не требует сложных схемотехнических решений. Инвертор

SN74LVC2G04 необходим для реализации управления по одному входу, он выполняет булеву функцию $Y = A$.

Алгоритм работы разработанного модуля СВЧ-переключателя заключается в том, что на управляющий контакт (*CTL*), указанный на схеме электрической принципиальной на рисунке 4, с устройства управления поступает управляющий сигнал, соответствующий высокому и низкому логическому уровню (*High/Low*), который обеспечивает, в соответствии с таблицей истинности микросхемы, поочередное переключение между каналами СВЧ-переключателя (форма управляющего логического сигнала может приходиться с устройства управления в виде сигнала с амплитудно-импульсной модуляцией). К соответствующим выводам (Вход 1, Выход 2) подключаются источники сигнала (приемник, передатчик).

Экспериментальные исследования

В ходе экспериментальных исследований был произведен перехват сигналов управления БПЛА с системой управления *FlySky fsi6*

Рис. 4. Схема электрическая принципиальная входного модуля СВЧ-переключателя

Рис. 5. Записанный поток управляющих пакетов

Рис. 6. Демодулированный сигнал

Рис. 7. Принятый сигнал и график созвездия сигнала

у Radiolink at9s и произведена обработка перехваченных сигналов для выявления протокола управления. На рисунке 5 можно увидеть управляющий сигнал, перехваченный с пульта управления FlySky fsib. По переходам фазы видно, что это частотная модуляция GFSK.

После демодуляции одного управляющего пакета, который представлен на рисунке 6, происходит оцифровка пакета. После декодировки формируются собственные сигналы управления на основе выявленной последовательности битов.

С перехватом и декодировкой сигналов с Radiolink at9s ситуация обстоит иначе, так как модуляция у данной системы управления QPSK.

На рисунке 7 представлен принятый сигнал с помехами и график созвездия, на графике изображено облако образцов фаз, которое не имеет никакой информативности.

Для извлечения протокола без ошибок восстанавливается тактовая частота приемника при помощи цифрового многофазного блока фильтров. Блок выполняет восстановление

Рис. 8. График созвездия сигнала без шумов

тактовой частоты, согласование фильтра приемника для устранения проблемы *ISI*, а также децимацию сигнала и производит выборки со скоростью 1 *sps*. Созвездие сигнала после обработки представлено на рисунке 8.

Произведя дополнительную фильтрацию и пропустив сигнал через цифровой эквалайзер, аппарат демодулирует сигнал с дальнейшей декодировкой протокола управления.

Заключение

Таким образом, в ходе исследований был разработан аппаратно-программный комплекс

на основе программно-аппаратной радиосистемы, который имеет два канала передачи для комбинирования методов перехвата БПЛА. Были проведены экспериментальные исследования комплекса, в ходе которых было подтверждена возможность перехвата протокола управления.

Был произведен анализ сигналов управления двух разных систем управления с *GFSK* и *QPSK* модуляциями соответственно.

Результаты, полученные в ходе работы, дают базу для дальнейших исследований в сфере радиоэлектронной борьбы и модернизаций комплекса перехвата управления БПЛА.

Список литературы

1. Мировое воздушное пространство беззащитно перед БПЛА, считают эксперты. URL: <https://ria.ru/20181221/1548394586.html> (дата обращения: 20.10.2020).
2. Hofmann-Wellenhof B., Lichtenegger H., Wasle E. GNSS – global navigation satellite systems: GPS, Glonass and more, 1st ed. Springer-Verlag Wien, 2008.
3. Аджухонов Э. А. Комплекс перехвата управления и спуфинга сигналов ГНСС БАС: дипломный проект. Томск: ТУСУР, 2020.
4. Кудряков С. А. Радиотехнические цепи и сигналы. СПб., 2015.
5. Artix-7. URL: <https://www.xilinx.com/products/silicon-devices/fpga/artix-7.html> (дата обращения: 21.11.2020).

Об авторах

Аджухонов Эльдар Ахмаджанович – старший оператор научной роты Федерального государственного автономного учреждения «Военный инновационный технополис «ЭРА», Анапа, Российская Федерация.
Область научных интересов: системы связи, обработка сигналов, радионавигация.

Николаев Олег Владимирович – старший оператор научной роты Федерального государственного автономного учреждения «Военный инновационный технополис «ЭРА», Анапа, Российская Федерация.
Область научных интересов: embedded технологии, ML, DS, AI.

UAV control hack system

Adzhakhunov E. A., Nikolaev O. V.

Federal State Independent Institution (FSII) "Military Innovative Technopolis "ERA", Anapa, Russian Federation

The paper presents an alternative solution to the problem of drone hacking over a radio channel and uses signal spoofing of a global positioning system (GPS, GLONASS). Within the framework of the study, block diagram and operation algorithm of the system were developed and experimental data were obtained.

Keywords: UAV, spoofing, hacking

Information about the authors

Adzhakhunov Eldar Akhmadzhanovich – Senior Operator, Research Company, Federal State Independent Institution (FSII) "Military Innovative Technopolis "ERA", Anapa, Russian Federation.

Science research interests: communication systems, signal processing, radio navigation.

Nikolaev Oleg Vladimirovich – Senior Operator, Research Company, Federal State Independent Institution (FSII) "Military Innovative Technopolis "ERA", Anapa, Russian Federation.

Science research interests: embedded technologies, ML, DS, AI.