

ПРОГРАММНО-АППАРАТНЫЙ МОДУЛЬ ОБРАБОТКИ ПРОТОКОЛА DRONE-ID ОТ DJI OCUSYNC 2.0

Д.С. Порядин¹, Р.Б. Архипов¹, А.С. Кравченко², С.Л. Сахаров²

¹ ВУНЦ ВВС «ВВА им. проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)

² ФГБОУ ВО ВГЛУ им. Г.Ф. Морозова (г. Воронеж)

Аннотация. В статье рассмотрен способ декодирования протокола «OcuSync-2.0» используемого в БПЛА DJI Mavic, с целью получения информации о местоположении борта и пульта управления

Ключевые слова: беспилотные летательные аппараты, декодирование протокола передачи данных, каналы управления.

DJI OCUSYNC 2.0 HARDWARE AND SOFTWARE MODULE FOR DRONE-ID PROTOCOL PROCESSING

D.S. Poryadin¹, R.B. Arkhipov¹, A.S. Kravchenko², S.L. Saharov²

¹ VUNTS of the Air Force “VVA named after Prof. Zhukovsky and Yu. A. Gagarin”
(Voronezh)

² Voronezh State University of Forestry and Technologies named after G.F. Morozov
(Voronezh)

Abstract. The article discusses a method for decoding the OcuSync-2.0 protocol used in the DJI Mavic UAV in order to obtain information about the location of the board and the control panel

Keywords: unmanned aerial vehicles, data transfer protocol decoding, control channels.

В современном мире нарастает активность применения беспилотных летательных аппаратов различного назначения. Активное использование гражданских БПЛА, в Российской Федерации регламентируется на законодательном уровне и требует соблюдения строго прописанных правил эксплуатации. Технические возможности правоохранительных органов по контролю и обеспечению регламента полётов БПЛА ограничены в виду массовости применения как в гражданском, так и военном сегментах эксплуатации. Но что делать службам безопасности гражданских критически важных объектов, как вариант вкладывать значительные финансовые средства для закупки специальных технических средств мониторинга и противодействия БПЛА различных классов и типов.

В данной статье приводятся практические результаты исследования по мониторингу наиболее распространённого типа БПЛА квадрокоптерного типа

компании «DJI» и техническое решение по локализации как оператора, так и самого борта.

Одним из ключевых кампаний–производителей беспилотных летательных аппаратов является «DJI», чья доля рынка на сегодняшний день занимает более 90 %. Техническое решение на основе декодирования протокола «DJI» и анализа программно-аппаратного обеспечения беспилотника представляет собой набор скриптов на языке программирования «Python3» и аппаратных средств: одноплатного компьютера «Raspberry-Pi5», с установленной на нем системой «DragonPi-OS64» и SDR приёмопередатчика «USRP-D200-mini-i» - показывающего, что данные передающиеся от беспилотника к оператору доступны в зоне радио доступности средствами радиоэлектронной разведки, что ставит под угрозу безопасность и конфиденциальность устройства и оператора, даже на современной «1001 прошивке» дрона, которая скрывает местоположение как БпЛА, так и оператора.

Современные «FPV»-дроны стали незаменимым инструментом во многих отраслях народного хозяйства. Поводом к этому стало обеспечение высокого качества изображения при низкой себестоимости устройства, что открыло перед пользователем новые возможности в фото- и видеосъемки (картографировании) местности. Крупные кампании используют для создания эффектных и ярких шоу-представлений новых продуктов, выступая новым рекламным лозунгом, для доставки посылок с воздуха.

В это же время резко возрастает вопрос обеспечения безопасности, из-за возникновения угроз вмешательства в работу беспилотников или использование их в неправомерных целях злоумышленниками. Например, возможным вектором атаки в данном случае может стать незаконное проникновение небольшого по своим размерам, начинённого опасными химическими веществами или взрывчатыми веществами, «FPV»-дрона на территорию критически важного объекта, такого как администрация города или атомная электростанция, куда незаконное проникновение строго запрещено.

Целью предложенного технического решения по мониторингу полётов БпЛА «DJI» стали декодирование протокола передачи данных между бортом и пультом управления и декодирование передаваемых данных с помощью набора скриптов «Drone-ID OcuSync-2.0». Такая функция должна обеспечиваться мощными средствами защиты информации, обеспечивающими конфиденциальность и целостность передаваемых данных рис. 1.

Предложенное техническое решение рассматривает два возможных варианта декодирования протокола передачи данных: когда оператор «прослушивает» трафик, передаваемый по радиоканалу и, когда оператор имеет физический доступ к БпЛА «DJI». Многие думают, что передаваемые по радиоканалу данные зашифрованы и их конфиденциальности ничего не угрожает, но на самом деле это не так. При помощи набора специальных скриптов и анализа программно-аппаратной части БпЛА, показываем, что доступ к данным возможно получить при наличии соответствующего

оборудования, а именно программно-определяемого радио (SDR) и «Raspberry-Pi5», с установленным на нём операционной системы «DragonPi-OS64» на «Ubuntu».

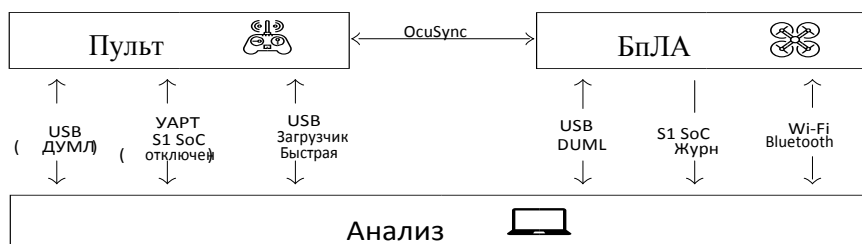


Рисунок 1 – Доступ к данным БПЛА «DJI»

Как в режиме «online» так и режиме пост обработки просмотра передаваемого трафика, оператору средств РЭР предоставляется доступ к пакету – раскрывающего местоположение беспилотного летательного аппарата и его оператора.

В ходе технического исследования прошивки и программного обеспечения БПЛА «DJI Mavic Air 2», связанного с физическим уровнем беспроводной связи, в целях изучения пакетов, использующих протокол «Drone-ID», были получены базовые алгоритмы передачи данных по протоколу «OcuSync-2.0». Визуализацию «сырых» данных, полученных с первого этапа работы приемника, который обнаруживает пакеты-кандидаты, не выполняя еще никакой вторичной обработки информации, можно наблюдать на рис. 2.

Структуру пакета DUML, можно разделить на четыре части: заголовок, транзитный, «command» и полезная нагрузка. Заголовок содержит «магический байт», равный фиксированному значению «0x55», за которым следует длина пакета, номер версии и контрольная сумма заголовка CRC-8. За заголовком следуют транзитные данные, которые используются для установки отправителя/получателя команды DUML. Известно 32 типа отправителя и приемника (например, ПК, мобильное приложение, центральная плата и Wi-Fi). Помимо источника и пункта назначения, транзитная часть пакета содержит уникальный порядковый номер для поддержания порядка следования нескольких пакетов

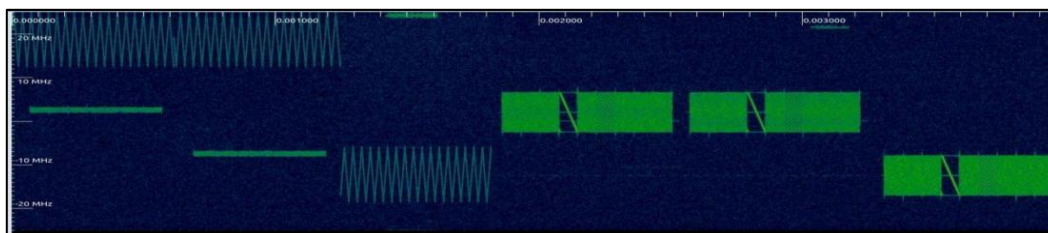


Рисунок 2 – Визуализация исходного файла образца спектрограмма «водопад»

На основе этого были сконфигурированы скрипты, способные принимать, демодулировать и декодировать пакеты протокола «Drone-ID» и выяснили, что они являются незашифрованными, даже при наличии у них обновленной «1001

прошивки» (специальная прошивка, позволяющая скрыть данные местоположения оператора и борта), когда данные точно должны быть скрыты, мы все равно можем получить необходимую для нас полезную информацию (уникальный номер борта и уровень сигнала RSSI). блок-схема скрипта представлена на рис. 3.



Рисунок 3 – Блок-схема алгоритма декодирования протокола «OcuSync-2.0»

Весь эксперимент проводился только с использованием доступной аппаратной частью, с открытым исходным кодом, а именно; тесты проводились на одноплатном компьютере «RaspberryPi5».

Программно-определяемого радио, а именно SDR приёмопередатчика «USRP B200-mini-i» – аппаратная плата, позволяющая быстро проектировать и реализовывать гибкие программно–определяемые системы радиосвязи, с частотным диапазоном от 50 МГц и до 6 ГГц, скоростным подключением USB 3.0., корпус которого выполнен на 3D-принтере и программная реализация на «Python3» с графическим интерфейсом, изображенная на рис. 4 и 5.

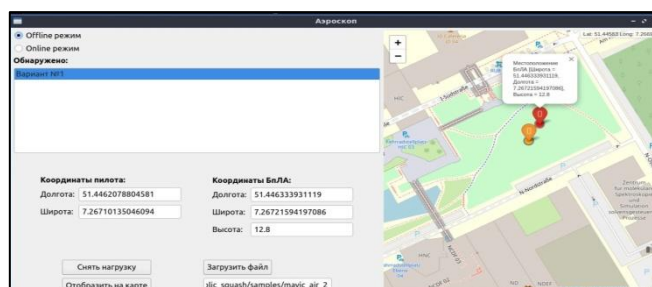
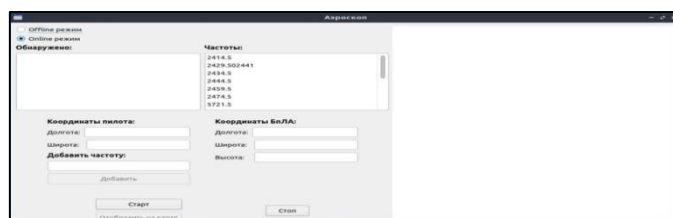


Рисунок 4 – Работа программы в режиме пост обработки



На рис. 5 представлено окно работы программы в динамическом режиме, когда к блоку обработки данных напрямую подключен блок приема через приёмопередатчик, тем самым позволяя вести радиоэлектронную разведку в непосредственной близости с исследуемым объектом.

В динамическом режиме мы постоянно сканируем приемником каждую заданную в базе данных полосу частот, указанных в отдельном блоке «частоты», с периодичностью 1,3 секунды при полосе пропускания 50 МГц, результатом чего получается пакет n-го размера на полосу. В случае нахождения кадров, блокируется полоса записи и возврат к ней происходит только после переключения канала.

Спецификация протокола «OcuSync-2.0», как выяснилось, использует схожие методы и параметры, как в стандарте сотовой связи 4G–LTE. Демодуляция осуществляется переводом радиосигнала в биты и байты, при котором необходимо учитывать: синхронизацию по времени, с целью определения границ OFDM-поднесущей, оценка канала для учета искажений во время радиопередачи и демодуляцию самих поднесущих.

Декодирование будет показывать, являлось ли назначение битов правильным, раскрывая полученный поток битов в структуру протокола «Drone-ID». Здесь возможно как декодирование, так и оповещение о том, что пакет повреждён. Это проверяется с помощью контрольных сумм CRC, включенных в каждый пакет, при соответствующем совпадении нашей калькуляции с исходной.

Данная программа позволяет успешно декодировать как статическую информацию о полетах и передвижении оператора дрона, так и динамическую в реальном времени, показывая хорошую производительность с нашей аппаратной конфигурацией. Декодированные данные свидетельствуют о точной информации местоположения дрона и его оператора, что позволяет полностью восстановить траекторию полета. Тем самым получив как можно больше пакетов, мы сможем получить лучшее разрешение траектории полета. Пример обработки данных в статическом режиме представлены на рис. 6.

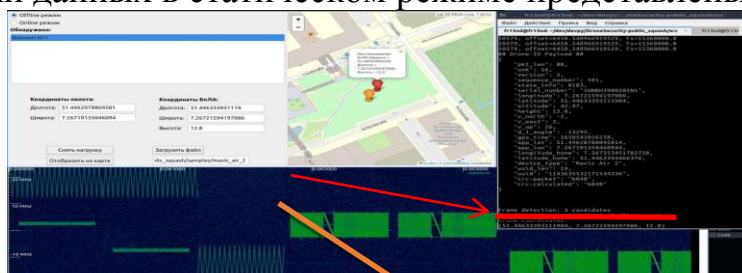


Рисунок 6 – Пример работы программы в автономном режиме



Рисунок 7 – Внешний вид готового программно-аппаратного модуля мониторинга каналов управления и передачи данных БПЛА «DJI»

Тесты показали, что в пределах зоны радио доступности к каналу управления и передачи данных БПЛА можно успешно декодировать передачу данных «DJI» с помощью «Drone-ID OcuSync-2.0», а самое главное мы обнаружили, что передаваемая информация является незащищенной никаким шифрованием, раскрывая точное местоположение дрона и места его управления оператором.

Внешний вид готового программно-аппаратного модуля мониторинга каналов управления и передачи данных БПЛА «DJI» представлен на рисунке 7. Данные результаты исследований будут полезны специалистам по безопасности КВО, охраняемых от НСД, в том числе по средствам БПЛА различных типов и классов.

Список литературы

1. Методы обеспечения стойкости электронной компонентной базы в части обратимых одиночных событий / А.Е. Козюков, Г.А. Распопов, А.И. Янков [и др.] // Моделирование систем и процессов. – 2021. – Т. 14, № 1. – С. 27-32. – DOI: 10.12737/2219-0767-2021-14-1-27-32.
2. Суханов, В.В. Логическое проектирование информационного обеспечения распределенных информационных систем критического применения / В.В. Суханов, О.В. Ланкин // Моделирование систем и процессов. – 2021. – Т. 14, № 2. – С. 67-73. – DOI: 10.12737/2219-0767-2021-14-2-67-73.

References

1. Methods for ensuring the stability of the electronic component base in terms of reversible single events / A. E. Kozyukov, G. A. Raspopov, A. I. Yankov [et al.] // Modeling of systems and processes. 2021. Vol. 14, No. 1. P. 27-32. – DOI: 10.12737/2219-0767-2021-14-1-27-32.
2. Sukhanov V.V., Lankin O.V. Logical design of information support for distributed information systems of critical application // Modeling of systems and processes. 2021. Vol. 14, No. 1. P. 67-73. – DOI: 10.12737/2219-0767-2021-14-1-67-73.