УДК 623.746.-519

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ СВЯЗИ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ ОТ АТАК С ИСПОЛЬЗОВАНИЕМ РАДИОЭЛЕТРОННЫХ СРЕДСТВ

Бавбель Е.И., Анискевич А.С.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Алексеев В.Ф. – канд.техн.наук, доцент

Аннотация. Представлен анализ современных методов защиты связи БПЛА. Рассмотрены механизмы защиты радиостанции от атак с использованием радиоэлектронных средств. Основываясь на знаниях из области преимуществ и недостатков этих систем, предлагается внести предложение по повышению устойчивости против глушителя сигнала.

Ключевые слова. Беспилотный летательный аппарат, БПЛА, связь, помехи, сверхширокополосные системы.

Введение. Безопасность связи важна для успешного использования беспилотных летательных аппаратов (БПЛА). С ростом использования БПЛА в военных и гражданских целях они часто несут конфиденциальную информацию, которую злоумышленники могут попытаться заполучить. Хотя беспилотные летательные аппараты состоят из различных модулей, позволяющих им функционировать должным образом, в этих модулях также могут существовать потенциальные уязвимости безопасности. Например, запустив атаку с подменой *GPS* или атаку *Wi-Fi*, злоумышленники могут захватить целевой БПЛА и получить доступ к запрошенной информации [1–5].

Основная часть. В области радиоэлектронной войны современные радиостанции активно реализуют два механизма, определенных в области электронной защиты, а именно: усиление защиты от радиоэлектронных средств и контроль выбросов. Эти механизмы предназначены для защиты радиостанций от воздействия использования частотного спектра, который ухудшает, нейтрализует или полностью блокирует их работоспособность [1, 2]. Меры электронной защиты сводят к минимуму способность противника обнаруживать, отслеживать и перехватывать БПЛА. Механизм управления спектром реализован вне радиостанций и направлен на координацию и устранение конфликтов использования частотного спектра как собственными силами, так и силами противника.

Для подавления помех используются различные виды модуляции: частотную, амплитудную и цифровую модуляции. Однако такая модуляция исходного сигнала сообщения на фиксированной несущей волне делает результирующую сигнальную волну уязвимой для взлома и помех. Такая модулированная волна также может быть демодулирована кем угодно, чтобы получить исходный сигнал сообщения.

Для подавления помех можно предложить методы расширенного спектра (*spread-spectrum* – SS). Развитие данной технологии связано с желанием создать помехоустойчивые системы связи. В процессе исследований расширенному спектру нашлось и другое применение – снижение плотности энергии, высокоточная локация и использование при множественном доступе. Расширенный спектр – это метод модуляции, который защищает сигнал сообщения от помех, шума окружающей среды и 8-сантиметровых помех. Это также обеспечивает безопасную связь и снижает вероятность обнаружения сигнала. В методах расширения спектра исходный узкополосный сигнал сообщения модулируется независимым широкополосным кодовым сигналом [1]. Таким образом, результирующий сигнал имеет более широкую полосу пропускания, а сигнал исходного сообщения «распространяется» по широкому диапазону частот. На стороне приемника тот же широкополосный кодовый сигнал ис-

пользуется для «уменьшения расширения» передаваемого сигнала, чтобы вернуть исходный узкополосный сигнал сообщения, как показано на рисунке 1.

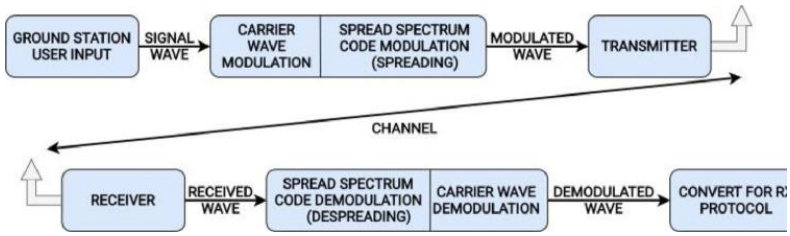

Рисунок 1 – Модуляция с расширенным спектром [1]

Можно предложить классификацию механизмов, которые защищают радиостанции от преднамеренных помех (рисунок 2).

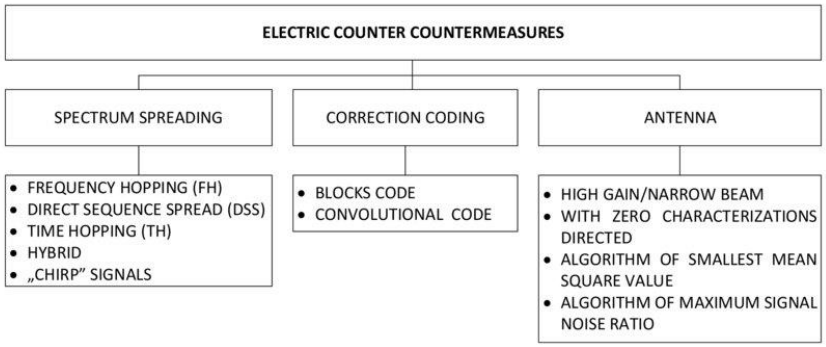

Рисунок 2 – Классификация механизмов, иммунизирующих радиостанции от преднамеренных помех [2]

В диапазоне частот *VHF / UHF* практически применимы механизмы кодирования *SST* (методы расширения спектра, расширение прямой последовательности) и *ECC, FEC* (кодирование с контролем ошибок, прямое кодирование ошибок). Механизмы защиты от помех, связанные с антеннами, не имеют здесь практического применения. Назначение указанных выше механизмов – заставить систему нарушить работоспособность ее ресурсов в области частоты, времени и пространства, тем самым снизив ее эффективность [3].

Система *DSSS (Direct Sequence Spread Spectrum)* имеет относительную простоту из-за отсутствия требования к быстрому синтезатору частот. Переданный сигнал умножается на псевдослучайную последовательность с высокой скоростью передачи битов, что приводит к расширению спектра сигнала и уменьшению его спектральной плотности. Переданный сигнал приобретает шумоподобную форму, что затрудняет обнаружение *LPD (Low Probability of Detection)* и затрудняет перехват *LPI (Low Probability of Intercept)* по отношению к сигналу без рассеяния.

В системе со скачкообразной перестройкой частоты *FH (Frequency Hopping)* несущая частота сигнала изменяется случайным образом в широкой полосе частот. Хотя потенциальный противник может обнаружить сигнал, он не может быть захвачен (низкая вероятность перехвата). Системы, в которых более одного символа попадает на заданную несущую частоту, называются системами с медленно скачкообразной частотой *LFH (Low Frequency Hopping)*. В противном случае мы имеем дело с системой с быстрой скачкообразной перестройкой частоты *FFH (Fast Frequency Hopping).*

Системы *CSS (Chirp Spread Spectrum)* – это системы, которые используют импульсы с монотонно изменяющейся частотой от минимальной частоты *f* 1 до максимальной частоты *f* 2 или наоборот. Разница в этих частотах является хорошей оценкой полосы сигнала. Высокое сопротивление сигнала достигается, когда произведение полосы частот ЛЧМ-сигнала и длительности его импульса намного больше единицы (это сопровождается постоянной спек-

тральной плотностью мощности сигнала). Системы *CSS* особенно полезны, когда ширина полосы сигнала намного превышает скорость двоичных данных (сверхширокополосные системы). Системы *Chirp Spread Spectrum* относятся к классу *LPI* [4–5].

Заключение. Таким образом основная идея заключается в том, что, увеличивая полосу пропускания сигнала, мы делаем неэффективным вмешательство злонамеренного глушения сигнала. Поскольку мощность в руках глушителя ограничена, ему придется распределять фиксированную мощность для передачи помех в широком диапазоне частот, тем самым создавая очень небольшие помехи в конкретном участке сигнала. С другой стороны, если глушилка передает всю свою мощность на определенный участок сигнала, остальная часть сигнала остается свободной от каких-либо помех.

Уровень помех, с которым система с расширенным спектром может справиться и при этом иметь возможность работать на номинальном уровне с заданным уровнем производительности, измеряется с помощью запаса на помехи. Это зависит от результата при обработке, потерь при реализации системы и минимального отношения сигнал/шум, необходимого в приемнике для безошибочной передачи информации.

Список литературы.

1. Халуза, М. Анализ и декодирование радиосигналов для дистанционного управления дронами / М. Халуза, Я. Чехак // Новые тенденции в обработке сигналов (NTSP) – 2016. – С. 1-5. – DOI: 10.1109 / NTSP.2016. 7747781.

2. Matuszewski, Jan. Evaluation of jamming efficiency for the protection of a single ground object / Jan Matuszewski // Proc. SPIE 10715, 2017 Radioelectronic Systems Conference, 107150B (19 April 2018). – https://doi.org/10.1117/12.2316629.

3. Анализ радиолиний связи с беспилотными летательными аппаратами [Электронный ресурс]: – Режим доступа: https://uav-siberia.com/news/analiz-radioliniy-svyazi-s-bespilotnymi-letatelnymi-apparatami/.

4. He D. Communication Security of Unmanned Aerial Vehicles / D. He, S. Chan, M. Guizani // IEEE Wireless Communications. – 2017. – Vol.24, No.4, – Pp.134-139, – DOI: 10.1109/MWC.2016.1600073WC.

5. Вишневский М. Результаты испытаний польской узкополосной радиосвязи SDR / М. Вишневский [и др.]. // Коммуникационные и информационные технологии (KIT). – 2017. –С.1-6. – DOI: 10.23919 / KIT.2017.8109458.

UDC 623.746.-519

ANALYSIS OF METHODS FOR PROTECTING UNMANNED AIRCRAFT COMMUNICATION AGAINST ATTACKS USING RADIO ELECTRONIC EQUIPMENT

Bavbel E.I., Aniskevich A.S.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Alexeev V.F. – PhD of technical sciences

Annotation. The analysis of modern methods of protection of UAV communication is presented. The mechanisms of protection of a radio station from attacks using radio electronic means are considered. Based on the knowledge of the advantages and disadvantages of these systems, it is proposed to make a proposal for improving the immunity against the signal suppressor.

Keywords. Unmanned aerial vehicle, UAV, communications, interference, ultra-wideband systems.