

УДК 621.396

**МНОГОУРОВНЕВАЯ АДАПТИВНАЯ СИСТЕМА ЗАЩИТЫ КАНАЛОВ СВЯЗИ
БПЛА ОТ РАДИОЭЛЕКТРОННЫХ УГРОЗ В СОВРЕМЕННЫХ УСЛОВИЯХ****Хамайко Светлана Владимировна¹**, аспирантe-mail: HamSv91@mail.ru¹ Морской государственный университет имени адмирала Г.И. Невельского, Владивосток, Россия

Аннотация. В настоящей статье рассматривается актуальная проблема обеспечения защиты каналов управления и навигации беспилотных летательных аппаратов (БПЛА) от современных радиоэлектронных угроз, таких как подавление, спуфинг и перехват. Проанализированы ограничения существующих подходов, основанных на изолированном применении криптографических методов, частотного разнообразия или инерциальной навигации, которые не обеспечивают комплексного противодействия в условиях динамичной радиоэлектронной обстановки.

Ключевые слова: БПЛА, радиоэлектронная защита, глушение, спуфинг, программно-определяемое радио (SDR), адаптивная система, помехоустойчивость, каналы связи.

**A MULTI-LEVEL ADAPTIVE SYSTEM FOR PROTECTING UAV
COMMUNICATION CHANNELS FROM ELECTRONIC THREATS
IN MODERN CONDITIONS****Svetlana V. Khamaiko¹**, Doctoral Studente-mail: HamSv91@mail.ru¹ Admiral Nevelskoy Maritime State University, Vladivostok, Russia

Abstract. This article discusses the urgent problem of ensuring the protection of control and navigation channels of unmanned aerial vehicles (UAVs) from modern electronic threats such as suppression, spoofing and interception. The limitations of existing approaches based on the isolated use of cryptographic methods, frequency diversity, or inertial navigation, which do not provide comprehensive countermeasures in a dynamic electronic environment, are analyzed.

Keywords: UAV, electronic protection, jamming, spoofing, software-defined radio (SDR), adaptive system, noise immunity, communication channels.

Введение

Бурное развитие беспилотной авиации привело к ее широкому применению как в гражданской, так и в специальной сферах. Однако эффективность БПЛА критически зависит от надежности и безопасности каналов связи (управления, телеметрии) и навигации

(GPS/ГЛОНАСС) [1]. Эти каналы стали первоочередной мишенью в современном противостоянии, что ярко продемонстрировали события последних лет [2]. Радиоэлектронные угрозы эволюционировали от простого широкополосного глушения к изощренным видам избирательного спуфинга и кибератакам на протоколы [3].

Существующие решения зачастую носят разрозненный характер: применение протоколов с расширенным спектром (FHSS/DSSS), сквозное шифрование, резервирование инерциальных навигационных систем (ИНС) [4]. Недостатком такого подхода является отсутствие системности и адаптивности. Система не оценивает обстановку в эфире в реальном времени и не может гибко перестраивать параметры связи или алгоритмы поведения БПЛА в ответ на конкретный тип угрозы [5].

Целью работы является разработка концепции многоуровневой адаптивной системы защиты (МАСЗ) каналов связи БПЛА, способной к обнаружению, анализу и автоматизированному противодействию комплексным РЭ-угрозам. Для её достижения решены следующие задачи:

1. Проведена классификация современных РЭ-угроз для БПЛА.
2. Проанализированы недостатки традиционных методов защиты.
3. Предложена архитектура и алгоритмы работы МАСЗ, ключевым элементом которой является модуль ситуационной осведомленности в радиоэфире на базе программно-определяемого радио (SDR), обеспечивающий реализацию адаптивного контура управления по схеме OODA (Observe, Orient, Decide, Act) [6].

1. Классификация угроз и анализ существующих методов защиты

1.1 Классификация угроз каналам связи БПЛА

– **Глушение:** активное создание помех. Подразделяется на: широкополосное, избирательное, следящее и когерентное.

– **Спуфинг:** подделка сигналов. Наиболее опасен навигационный спуфинг (медленный – увод с курса, быстрый – захват контроля) и спуфинг команд управления [5].

– **Перехват и анализ:** пассивный сбор данных для обратной разработки протоколов, пеленгации или подготовки целевой атаки [2].

1.2 Ограничение традиционных подходов

– **Шифрование (AES-256 и др.):** защищает от перехвата и спуфинга команд, но не от глушения и навигационного спуфинга.

– **Протоколы с FHSS/DSSS:** устойчивы к узкополосному глушению, но уязвимы к следящему подавлению и не защищают от спуфинга.

– **Резервирование ИНС/ВО:** компенсирует потерю GPS, но не решает проблему потери канала управления и увеличивает SWaP (Size, Weight and Power).

– **Использование лицензированных частот:** снижает уровень бытовых помех, но не является защитой от целенаправленной РЭБ.

2. Архитектура многоуровневой адаптивной системы защиты (МАСЗ)

Предлагаемая МАСЗ реализуется на двух концах канала связи:

- на наземной контрольной точке (НКТ);
- на борту БПЛА.

Ее ядро составляет контур адаптации, работающий по схеме OODA (Observe, Orient, Decide, Act) [6].

2.1 Ключевые модули системы:

1. Модуль ситуационной осведомленности в радиоэфире: на базе SDR-приемников на НКТ и, опционально, на БПЛА. Постоянно сканирует рабочие и смежные частотные диапазоны [6].

Функции: Измерение уровня шума (RSSI), построение спектрограммы, обнаружение аномалий (узкополосные выбросы, имитация полезного сигнала), пеленгация источника помех.

2. Модуль анализа и классификации угроз: на основе машинного обучения (легкие алгоритмы, например, Random Forest или CNN для спектрограмм) классифицирует тип угрозы (глушение/спуфинг), её интенсивность и предполагаемый источник [5].

3. Модуль принятия решений и адаптации: на основе классификации от МАКУ и текущего состояния БПЛА (запас энергии, этап миссии, положение) выбирает оптимальный ответ из библиотеки протоколов.

4. Исполнительные механизмы:

– Радиочастотный: динамическое переключение между каналами (частотный агрегинг), изменение схемы модуляции и кодирования (адаптивная OFDM), активация режима FHSS с изменяемым паттерном скачков [4];

– Навигационный: верификация GPS/ГЛОНАСС по данным ИНС, визуальной одометрии (VIO) и барометрической высоты. При обнаружении спуфинга – переход на защищенную навигацию без спутников [5];

– Тактический/Поведенческий: изменение миссии в реальном времени: смена высоты полета, маневр уклонения от пеленгуемого источника, переход на режим полного радиомолчания с выполнением автономного миссион-плана.

Рисунок 1 демонстрирует структурную схему многоуровневой адаптивной системы защиты (МАСЗ).

2.2 Алгоритм работы в условиях угрозы

Алгоритм функционирования многоуровневой адаптивной системы защиты (МАСЗ) при обнаружении угроз реализует цикл OODA (Наблюдение – Ориентация – Решение – Действие) [6]:

1. **Наблюдение:** система обнаружения радиоизлучения и электромагнитных помех (СОРЭ) фиксирует аномалии в радиоэфире, такие как превышение порога уровня сигнала (RSSI) или искажение спектрального состава;

2. **Ориентация:** модуль анализа и классификации угроз (МАКУ) анализирует полученные данные и классифицирует тип угрозы. Например: «Обнаружено узкополосное глушение на частоте 2,425 ГГц с признаками следящего подавления» [5];

3. **Решение:** модуль принятия решений (МПР) оценивает контекст ситуации и принимает решение о необходимых мерах. Пример: «Угроза классифицирована как высокая. БПЛА находится на критическом этапе миссии. Команда: переключить управление на резервный канал 915 МГц, изменить паттерн FHSS (частотно-скачковой последовательности), активировать VIO (Виртуальную Инерциальную Ориентацию), начать маневр «зигзаг» для затруднения пеленгации» [4];

4. **Действие:** исполнительные механизмы на наземной контрольной точке (НКТ) и БПЛА выполняют принятые команды. СОРЭ продолжает мониторинг эффективности реализованных мер.

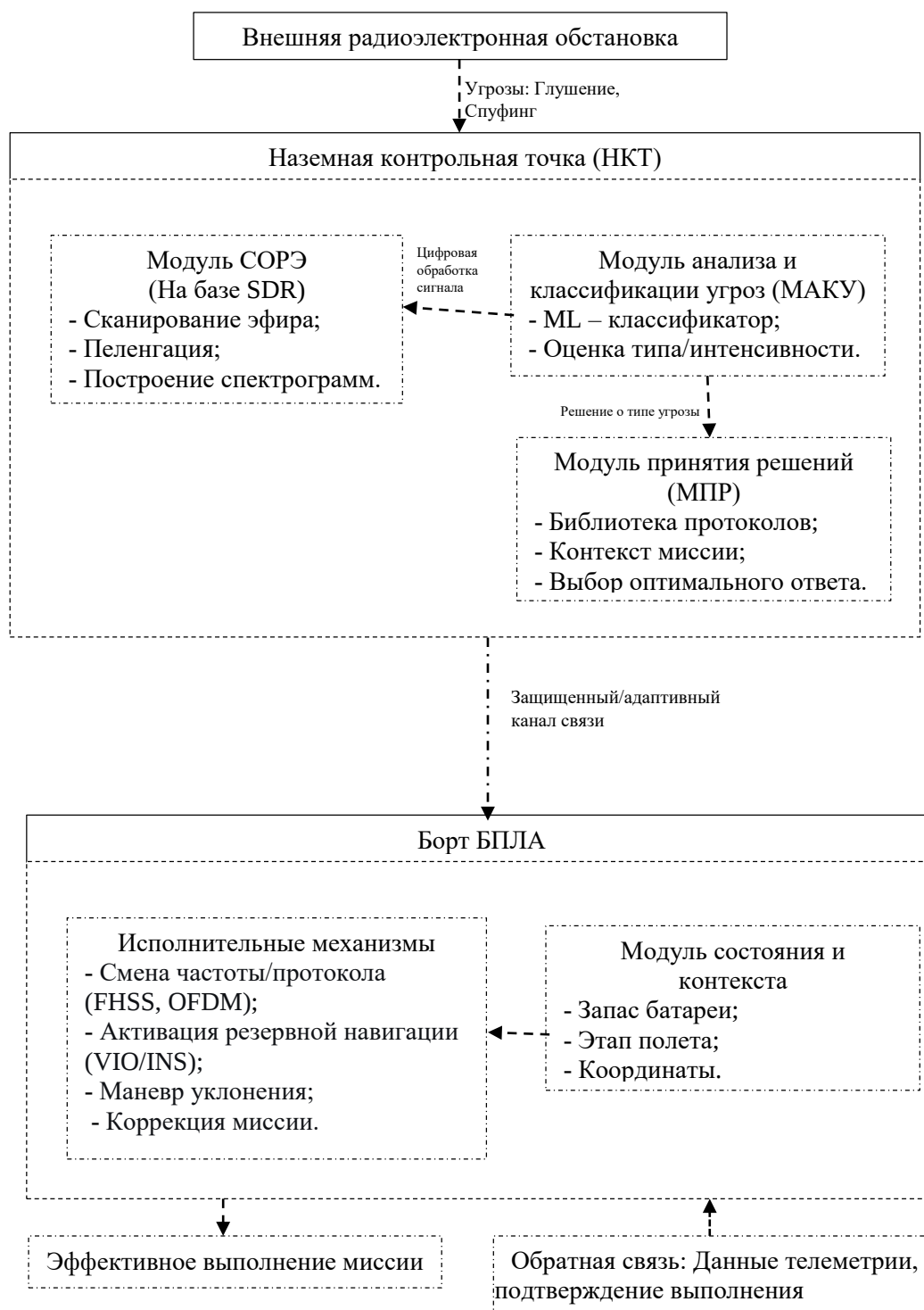


Рисунок 1 – Структурная схема многоуровневой адаптивной системы защиты (МАСЗ)

На рисунке 2 представим спектрограммы различных типов радиоэлектронных угроз.

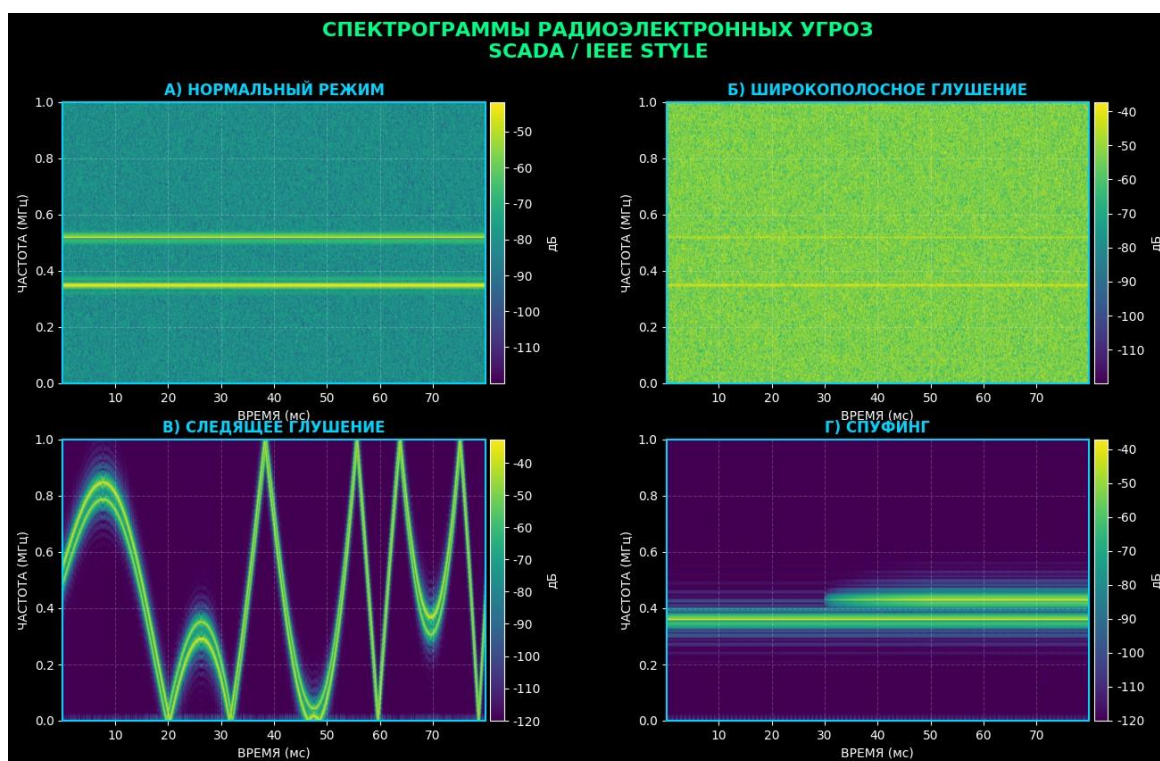


Рисунок 2 – Спектрограммы различных типов радиоэлектронных угроз

Анализ спектрограмм демонстрирует наличие у различных радиоэлектронных угроз уникальных спектрально-временных характеристик. Данный факт обосновывает применение автоматических методов классификации и адаптивной защиты каналов связи.

В частности, идентификация типов угроз осуществляется следующим образом:

- широкополосные помехи выявляются посредством анализа роста уровня фоновых шума;
- следящие помехи обнаруживаются на основе корреляции траекторий сигнала и помехи;
- спуфинг распознается по появлению дополнительных спектральных компонентов.

Полученные результаты подтверждают целесообразность использования многоуровневых интеллектуальных систем защиты, которые способны в режиме реального времени идентифицировать тип угрозы и выбирать соответствующую контрмеру.

3. Сравнительный анализ с существующими системами защиты

В таблице 1 представим результаты сравнительного анализа предложенной многоуровневой адаптивной системы защиты (МАСЗ) с существующими коммерческими и специализированными аналогами [2, 6].

Таблица 1. Сравнительный анализ МАСЗ с существующими коммерческими и специализированными аналогами

Характеристика	DJI AeroScope	DroneShield DroneSentry	Предлагаемая МАСЗ
Обнаружение угроз	Пассивное (только детекция)	Активное (глушение)	Активное + адаптация
Классификация угроз	Отсутствует	Базовая (тип дрона)	ML-классификация (тип, интенсивность, источник)

Адаптация параметров связи	Отсутствует	Отсутствует	Есть (частота, модуляция, протокол)
Резервирование каналов	Отсутствует	Отсутствует	Есть (2–3 независимых канала)
Защита от спуфинга	Отсутствует	Частичная (GPS-фильтрация)	Полная (INS+VIO+верификация)
Интеграция с полётным заданием	Отсутствует	Отсутствует	Есть (коррекция маршрута)
Обратная связь по эффективности	Отсутствует	Отсутствует	Есть (замкнутый контур)

Предлагаемая система MAC3 обладает существенным преимуществом перед аналогами благодаря наличию замкнутого контура адаптации. Данный контур обеспечивает интеграцию процессов обнаружения, классификации угроз, принятия решений и реализации контрмер с механизмом обратной связи по результатам их выполнения.

Заключение

В ходе исследования была разработана концепция многоуровневой адаптивной системы защиты (MAC3) каналов связи беспилотных летательных аппаратов, призванная противостоять современным радиоэлектронным угрозам.

Основные научные и практические результаты работы:

1. Проведена классификация современных радиоэлектронных угроз для БПЛА, выявлены их ключевые спектрально-временные характеристики.
2. Выполнен критический анализ традиционных методов защиты, показавший их фрагментарность и недостаточную эффективность при комплексном радиоэлектронном противодействии.
3. Разработана архитектура MAC3, реализующая замкнутый контур адаптации по принципу OODA. Ключевым элементом является модуль ситуационной осведомленности в радиоэфире (COPЭ) на базе SDR, обеспечивающий непрерывный мониторинг частотного спектра, обнаружение аномалий и пеленгацию источников помех.
4. Проведен сравнительный анализ с существующими системами защиты, демонстрирующий преимущества предлагаемого подхода благодаря наличию замкнутого контура адаптации и интеллектуальной классификации угроз.

Таким образом, разработанная MAC3 представляет собой перспективное решение для обеспечения защищенности беспилотных летательных аппаратов от современных радиоэлектронных угроз.

В рамках дальнейших исследований планируется проведение оптимизации алгоритмов машинного обучения (ML) для бортовых систем беспилотников. Это позволит повысить эффективность работы БПЛА за счет адаптации к динамично изменяющимся условиям полета.

Также предполагается разработка и внедрение систем кооперативной защиты для роев БПЛА. Совместные действия беспилотников, основанные на обмене информацией и координации, обеспечат более надежную защиту от потенциальных угроз.

Еще одним направлением развития является интеграция систем управления БПЛА с технологиями когнитивного радио. Данная интеграция позволит динамически адаптировать частоты связи беспилотников к изменяющимся условиям радио среды, что в свою очередь повысит устойчивость и эффективность передачи данных.

Список литературы:

1. Чугунов Д.В., Петров А.А. Угрозы безопасности беспилотных авиационных систем и методы противодействия // Труды МФТИ. – 2022. – Т.14, №1. – С. 45-59.
2. Strohmeier M., Schafer M., Lenders V., Martinovic I. Reality and Evolution of UAV Security: Lessons from the Skies // IEEE Security & Privacy. – 2023. – Vol. 21, No. 2. – P. 34-44.
3. Humphreys T.E. Detection Strategy for Cryptographic GNSS Anti-Spoofing // IEEE Transactions on Aerospace and Electronic Systems. – 2022. – Vol. 49, No. 2. – P. 1073-1090.
4. Ким В.В., Сидоров А.И. Помехоустойчивые системы управления беспилотными летательными аппаратами. – М.: Техносфера, 2021. – 288 с.
5. Князев А.В., Соловьёв А.Н. Методы защиты беспилотных летательных аппаратов от спуфинга навигационных сигналов // Радиотехника. – 2023. – № 3. – С. 45–52.
6. Иванов И.И., Петров П.П. Применение технологий программно-определяемого радио в системах связи БПЛА // Инфокоммуникационные технологии. – 2022. – Т. 20, № 4. – С. 312–320.

