



МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение

высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ
ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему «Разработка программной модели безопасного распространения сигнала управления БПЛА»

Исполнитель _____
(подпись)

Белов Александр Александрович
(фамилия, имя, отчество)

Руководитель _____
(подпись)

Чернецова Елена Анатольевна
(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____
(подпись)

Олег Михайлович Лепешкин
(фамилия, имя, отчество)

« _____ » _____ 2026 г.

Санкт-Петербург

2026

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ
ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

«УТВЕРЖДАЮ»

Заведующий кафедрой

_____ Олег Михайлович Лепешкин

(подпись) (фамилия, имя, отчество)

«_____» _____ 20__ года

Задание

на выпускную квалификационную работу

студенту: Белову Александру Александровичу

(фамилия, имя, отчество)

1. Тема Разработка программной модели безопасного распространения сигнала управления БПЛА

закреплена приказом ректора Университета от «__» _____ 20__ года,

№ _____

2. Срок сдачи законченной работы «__» _____ 20__ года

3. Исходные данные к выпускной квалификационной работе:

4. Перечень вопросов, подлежащих разработке (краткое содержание работы):

Введение. Актуальность темы, цели и задачи ВКР

Глава 1 Обзор архитектуры системы связи в системах управления БПЛА

(наименование главы)

Глава 2 Характеристика моделей для предсказания уровня сигнала

(наименование главы)

Глава 3 Разработка программной модели предсказания уровня сигнала
управления БПЛА

(наименование главы)

Заключение. Выводы по работе в целом. Оценка степени решения
поставленных задач. Практические рекомендации.

5. Перечень материалов, представляемых к защите:

– Пояснительная записка;

6. Дата выдачи задания: «__» _____ 20__ года

Руководитель выпускной квалификационной работы

(должность, ученая степень, ученое звание, фамилия, имя, отчество)

(подпись)

Задание принял к исполнению «__» 20__ года

Студент Белов Александр Александрович, ИБ-С20-1

(фамилия, имя, отчество, учебная группа)

(подпись)

РЕФЕРАТ

Дипломная работа: ____ с., ____ рис., ____ табл., ____ приложения, ____ источников литературы.

РАЗРАБОТКА ПРОГРАММНОЙ МОДЕЛИ БЕЗОПАСНОГО РАСПРОСТРАНЕНИЯ СИГНАЛА УПРАВЛЕНИЯ БПЛА.

Объект исследования - Системы связи и управления беспилотными летательными аппаратами (БПЛА).

Предмет исследования – программная модель безопасного распространения сигнала управления БПЛА.

Цель исследования: разработка программной модели предсказания уровня сигнала управления БПЛА.

Задачи исследования:

1. Провести анализ современных проблем безопасности связи в системах управления БПЛА.
2. Исследовать модели предсказания уровня сигнала.
3. Обосновать выбор программной среды для разработки модели предсказания уровня сигнала управления БПЛА.
4. Разработать программную модель предсказания уровня сигнала.
5. Оценка практической значимости по применению программной модели безопасного распространения сигнала управления БПЛА.

Разработана программная модель предсказания уровня сигнала управления для систем связи БПЛА.

СОДЕРЖАНИЕ

ГЛАВА 1. ПРОБЛЕМЫ БЕЗОПАСНОСТИ СВЯЗИ В СИСТЕМАХ УПРАВЛЕНИЯ БПЛА	9
1.1. Архитектура системы связи БПЛА	9
1.1.1. Общая структура систем связи БПЛА.....	9
1.1.2. Каналы связи.....	10
1.1.3. Топологии сетей связи	11
1.1.4. Протоколы связи.....	14
1.1.5. Аппаратные компоненты	18
1.1.6. Программные компоненты	19
1.2 Угрозы безопасности связи в системах управления БПЛА	20
1.2.1 Атаки на программное обеспечение.....	20
1.2.2. Фальсификация видеопотока	21
1.2.3. Подмена системного идентификатора	21
1.2.4. Атаки на каналы связи	21
1.2.5. Атака «подслушивание»	22
1.2.6. DoS-атаки	22
1.2.7. Атаки «человек посередине»	22
1.2.8. Атака «подделка»	23
1.2.9. Атака повторного воспроизведения	23
1.2.10. Атаки на маршрутизацию	23
1.3 Уязвимости систем связи БПЛА	23
1.3.1. Уязвимости программного обеспечения	23
1.3.2. Уязвимости нулевого дня.....	24
1.3.3. Уязвимости каналов связи	24
1.4 Методы и средства защиты связи в системах управления БПЛА	26
1.4.1. Противодействие атакам на программное обеспечение.....	26
1.4.2. Противодействие атакам на каналы связи	26
1.4.3. Противодействие атакам на транспортном уровне	28
1.5 Анализ существующих решений и их недостатки	29

1.6 Выводы по первой главе	34
Глава 2. ХАРАКТЕРИСТИКА МОДЕЛЕЙ ДЛЯ ПРЕДСКАЗАНИЯ УРОВНЯ СИГНАЛА	36
2.1. Эмпирические модели.....	36
2.2. Физические (детерминированные) модели.....	37
2.3. Статические модели	38
2.4. Модели машинного обучения.....	39
2.5. Сравнительный анализ типов моделей	40
2.6. Модель Окамуры.....	43
2.7. Модель Окамура-Хата.....	49
2.8. Модель Ли.....	51
2.9. Модель COST-231-Хата.....	55
2.10. Выводы по второй главе	56
ГЛАВА 3. РАЗРАБОТКА ПРОГРАММНОЙ МОДЕЛИ ПРЕДСКАЗАНИЯ УРОВНЯ СИГНАЛА УПРАВЛЕНИЯ БПЛА.....	57
3.1. Анализ вариантов реализации программной модели	57
3.1.1. Desktopная программа для анализа и сравнения моделей.....	57
3.1.2. Плагин для программ планирования полётных заданий.....	58
3.1.3. Встроенный аппаратный модуль на борту БПЛА	59
3.1.4. Облачная платформа для анализа и предсказания	60
3.1.5. Мобильное приложение для операторов БПЛА	60
3.2. Выбор технологии реализации	62
3.3. Разработка алгоритма предсказания уровня сигнала	63
3.4. Описание функционала программы	64
3.5. Тестирование модели	66
3.6. Анализ результатов работы программы.....	68
3.7. Выводы по третьей главе	71
ЗАКЛЮЧЕНИЕ	73
СПИСОК ЛИТЕРАТУРЫ	76
ПРИЛОЖЕНИЕ А.....	78

ВВЕДЕНИЕ

В последние годы БПЛА стали неотъемлемой частью современных технологий, находя применение в самых разных областях: от мониторинга сельскохозяйственных угодий, картографирования и экологических исследований до доставки грузов, поисково-спасательных операций и военных миссий. Однако эффективность и безопасность их эксплуатации напрямую зависят от надёжности систем связи, обеспечивающих передачу управляющих сигналов и данных телеметрии.

Современные системы управления БПЛА часто сталкиваются с рисками потери связи, перехвата сигналов или их искажения, что может привести к аварийным ситуациям, угрожающим жизни людей и материальным ценностям. В связи с этим разработка программных моделей, обеспечивающих безопасное и устойчивое распространение сигналов управления, становится критически важной задачей. Такие модели должны учитывать не только технические аспекты передачи данных, но и адаптироваться к динамически изменяющимся условиям эксплуатации, включая противодействие киберугрозам и минимизацию влияния помех.

Объект исследования - Системы связи и управления БПЛА.

Предмет исследования – программная модель безопасного распространения сигнала управления БПЛА.

Цель исследования: разработка программной модели предсказания уровня сигнала управления БПЛА.

Задачи исследования:

- 1) Провести анализ современных проблем безопасности связи в системах управления БПЛА.
- 2) Исследовать модели предсказания уровня сигнала.
- 3) Обосновать выбор программной среды для разработки модели предсказания уровня сигнала управления БПЛА.

4) Разработать программную модель предсказания уровня сигнала.

5) Оценка практической значимости по применению программной модели безопасного распространения сигнала управления БПЛА.

Методы исследования: методы теоретического анализа, методы системного анализа и экспериментальные методы.

Выпускная квалификационная работа состоит из следующих разделов: введения, трех глав, заключения и списка использованной литературы.

В первой главе проведен обзор архитектуры системы связи в системах управления БПЛА, также анализ существующих проблем безопасности.

Вторая глава включает в себя характеристику моделей для предсказания уровня сигнала, также их сравнительный анализ для обеспечения безопасного распространения сигнала в системах управления БПЛА.

Третья глава включает в себя разработку программной модели безопасного распространения сигнала управления БПЛА и оценка её практической значимости.

В заключении представлены итоги исследования и основные выводы.

ГЛАВА 1. ПРОБЛЕМЫ БЕЗОПАСНОСТИ СВЯЗИ В СИСТЕМАХ УПРАВЛЕНИЯ БПЛА

1.1. Архитектура системы связи БПЛА

Архитектура системы связи БПЛА — это сложная структура, объединяющая аппаратные и программные компоненты, каналы связи, топологии сетей и протоколы передачи данных. Она обеспечивает надёжную, безопасную и эффективную передачу информации, что критически важно для выполнения миссий и безопасности полётов.

1.1.1. Общая структура систем связи БПЛА

На рисунке 1 показана общая структура систем связи с БПЛА, которая состоит из двух основных типов каналов связи, а именно связь без полезной нагрузки и канала передачи данных.

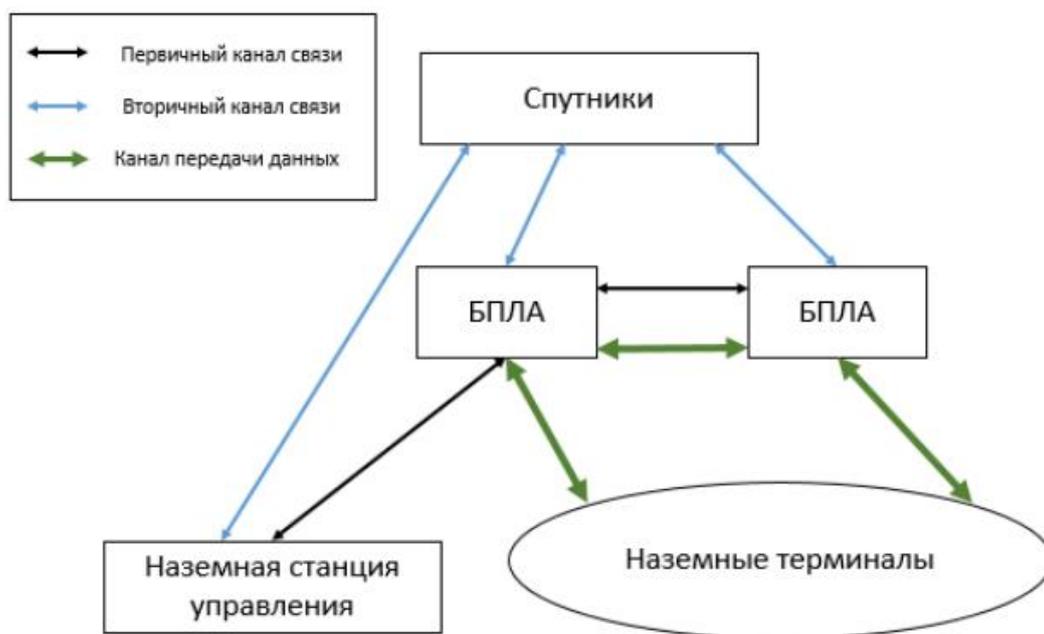


Рисунок 1 – Общая структура систем связи с БПЛА

Линии связи без полезной нагрузки необходимы для обеспечения безопасного использования всех возможных БПЛА. Эти каналы должны поддерживать высоконадёжную, с меньшим количеством задержек и безопасную двустороннюю связь, чаще всего требующую низкую скорость передачи данных, для обмена важной информацией между БПЛА, а также между БПЛА и землей.

Для автономных БПЛА, которые выполняют задачи полагаясь на автоматизированную систему полета без контроля человека в реальном времени, каналы связи без полезной нагрузки также необходимы в случае, когда нужно экстренное вмешательство человека.

1.1.2. Каналы связи

Каналы связи — это специализированные пути передачи данных, обеспечивающие взаимодействие между БПЛА, НСУ, спутниками и другими внешними системами.

В Таблице 1 представлены каналы связи, их назначение и примеры технологий, применяемых для передачи данных. Канал управления обеспечивает передачу команд от оператора к бортовой системе БПЛА, канал телеметрии передаёт данные с борта на наземную станцию в реальном времени, канал видеотрансляции отвечает за передачу видео, а канал навигации — за получение данных GPS/ГЛОНАСС и коррекцию координат.

Таблица 1 – Каналы связи

Канал	Назначение	Примеры технологий
Канал управления	Передача команд от оператора к БПЛА (например, изменение курса, высоты).	MAVLink, PPM, SBUS, 4G/5G, спутниковая связь (Iridium, Inmarsat).
Канал телеметрии	Передача данных с борта БПЛА на ГСУ (координаты, скорость, состояние систем).	MAVLink, LoRa, Wi-Fi, LTE.
Канал видеотрансляции	Передача видео с камер БПЛА в реальном времени.	COFDM, Wi-Fi, 4G/5G, аналоговое видео.
Канал навигации	Получение данных GPS/ГЛОНАСС, коррекция координат.	GPS, ГЛОНАСС, RTK.

Канал управления и канал телеметрии относятся к категории связи без полезной нагрузки, так как обеспечивают передачу команд и служебной информации, необходимой для управления и мониторинга состояния БПЛА.

Канал видеотрансляции и канал навигации относятся к категории каналов передачи данных, так как обеспечивают передачу полезной информации (видео, навигационные данные), необходимой для выполнения задач миссии.

1.1.3. Топологии сетей связи

Различные топологии: "точка-точка", "звезда" и "mesh-сеть". Имеют свои особенности, преимущества и недостатки, что определяет их применимость в зависимости от задач и условий эксплуатации.

Point-to-Point (точка-точка) — прямое соединение между одной НСУ и одним БПЛА. Канал связи устанавливается напрямую, без промежуточных узлов. Приведен пример на рисунке 2.

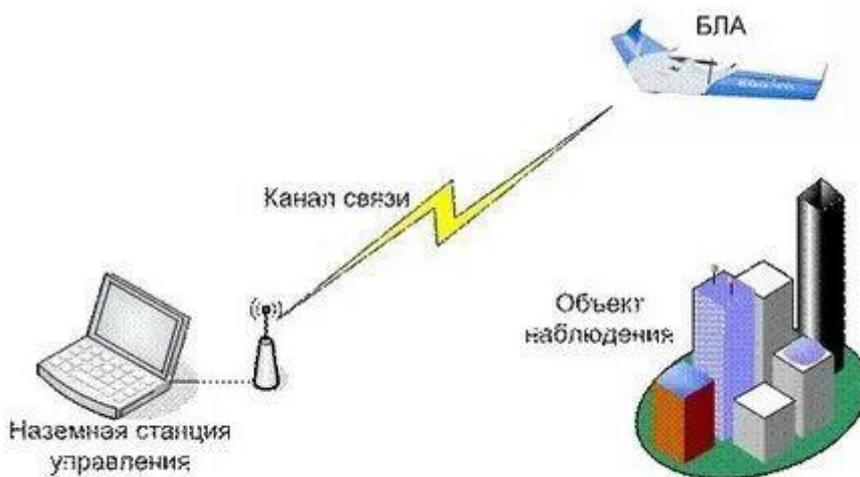


Рисунок 2 –топология сети "точка-точка"

Звезда - один центральный узел (НСУ) управляет несколькими БПЛА. Все БПЛА соединены напрямую с НСУ, но не взаимодействуют друг с другом. Приведен пример на рисунке 3.

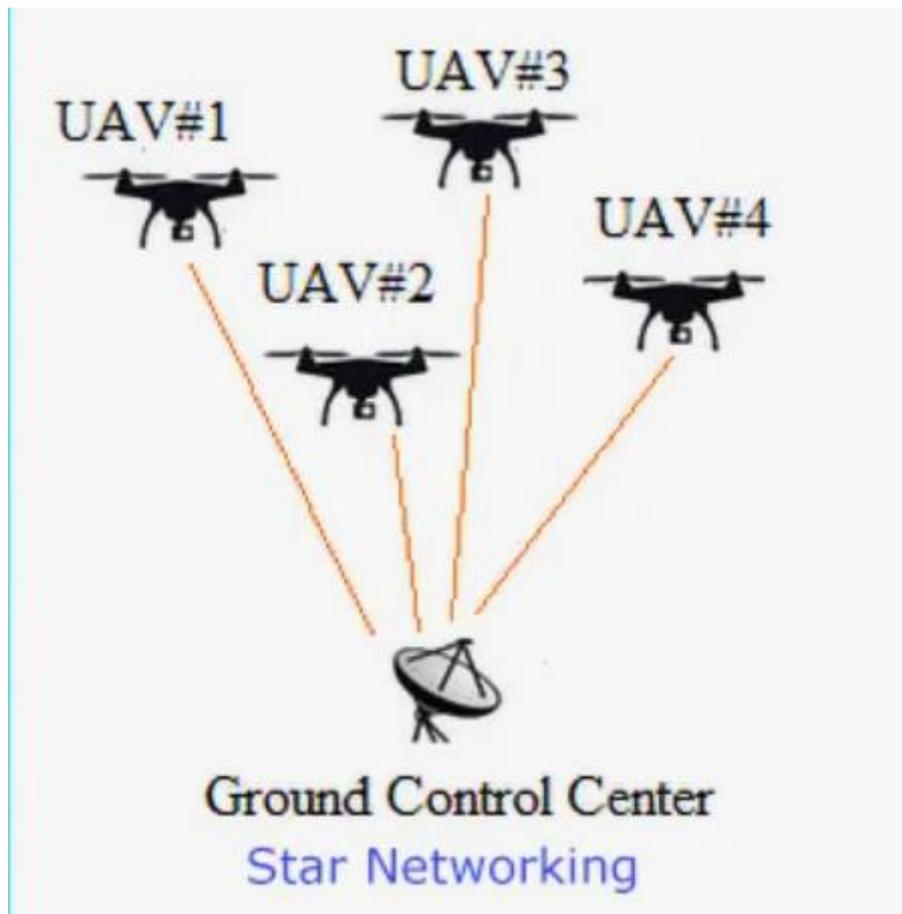


Рисунок 3 – топология сети "Звезда"

Mesh-сеть - БПЛА соединены между собой и могут ретранслировать сигналы. Каждый БПЛА является узлом сети, что позволяет передавать данные через несколько узлов. Приведен пример на рисунке 4.

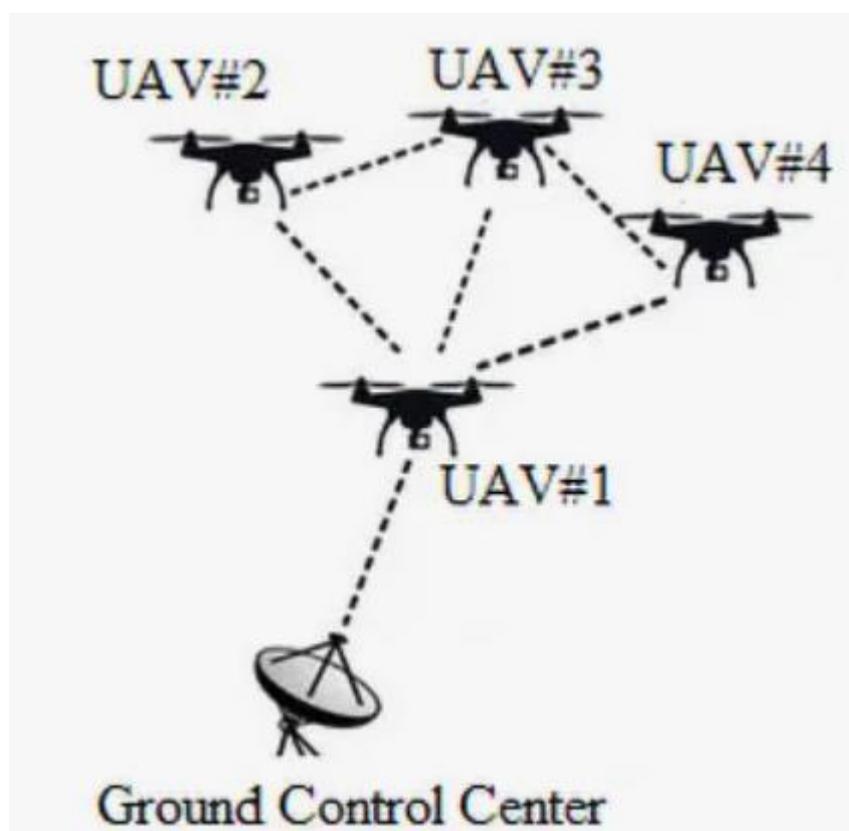


Рисунок 4 – топология сети "Mesh-сеть"

В рамках анализа топологий сетей связи для БПЛА особое внимание уделяется их характеристикам, преимуществам и недостаткам. В Таблице 2 представлены основные параметры топологий сетей связи, что позволяет обосновать выбор архитектуры для разработки программной модели предсказания уровня сигнала управления БПЛА.

Таблица 2 – Характеристики топологий сетей связи

Топология	Преимущества	Недостатки	Применение
Точка-точка	Простота, низкая задержка, надёжность	Ограниченный радиус, нет резервирования	Одиночные БПЛА, простые миссии
Звезда	Централизованное управление, масштабируемость	Единая точка отказа, ограниченная дальность	Групповые полёты, мониторинг

Топология	Преимущества	Недостатки	Применение
Mesh-сеть	Надёжность, расширенный радиус, устойчивость	Сложность управления, задержки, энергопотребление	Роевые системы, сложные миссии

Таким образом, выбор топологии сети связи для БПЛА зависит от специфики решаемых задач, требований к надёжности, масштабируемости и безопасности. Для простых миссий с одиночными аппаратами оптимальной может быть топология "точка-точка", тогда как для сложных группировок БПЛА, включая роевые системы, более подходящими становятся "mesh-сеть" или гибридные решения.

1.1.4. Протоколы связи

Протоколы передачи данных (ППД) — это наборы правил и соглашений, которые определяют, как участники сети обмениваются данными. Они задают форматы сообщений, порядок их передачи, методы обнаружения и исправления ошибок, а также алгоритмы взаимодействия между отправителем и получателем. В таблице 3 представлены характеристики ППД.

Таблица 3 – Характеристики ППД

Протокол	Частота	Скорость передачи данных	Дальность действия	Энергопотребление
LoRa (Long Range)	433 МГц, 868 МГц, 915 МГц	До 50 Кбит/с	До 15 км (при идеальных условиях)	Низкое
WiFi (802.11)	2.4 ГГц / 5 ГГц	До 1 Гбит/с	До 1-2 км (с усилителями вплоть до 5 км)	Высокое
DSSS (Direct Sequence)	2.4 ГГц	До 2 Мбит/с	До 5 км	Среднее

Протокол	Частота	Скорость передачи данных	Дальность действия	Энергопотребление
Spread Spectrum)				
4G/5G (Сотовая связь)	700 МГц – 6 ГГц (4G); 24 ГГц – 100 ГГц (5G)	До 1 Гбит/с (4G); До 10 Гбит/с (5G)	Зависит от покрытия сотовой сети: До 15 км (4G); До 20 км (5G)	Высокое
Zigbee	2.4 ГГц	До 250 Кбит/с	До 1 км (при идеальных условиях)	Низкое
Bluetooth (BLE)	2.4 ГГц	До 2 Мбит/с	До 100м (без усилителей)	Очень низкое
XBee (IEEE 802.15.4)	868 МГц, 900 МГц, 2.4 ГГц	До 250 Кбит/с	До 50 км	Среднее
Iridium (спутниковая связь)	L-диапазон (1616 – 1626.5 МГц)	До 2.4 Кбит/с	Глобальное покрытие	Высокое
OcuSync (DJI)	2.4 ГГц / 5.8 ГГц	До 50 Мбит/с	До 15 км (при идеальных условиях)	Среднее
LTE-M (Long-Term Evolution for Machines)	700 – 2600 МГц	До 1 Мбит/с	До 20 км (в зоне покрытия)	Низкое

Рассмотрим особенности протоколов более подробно.

Протокол LoRa [21] имеет большую дальность связи, до 15 км, высокую помехоустойчивость и минимальное энергопотребление, но также он обладает низкой скоростью передачи видео(не подходит для видео), при увеличении дальности скорость передачи становится равной около 0,3 кбит/с, а также высокой задержкой передачи информации, около 1-10 секунд, в зависимости от загруженности эфира. Если в приоритете является дальность действия, а не скорость передачи данных, то данный ППД идеально подойдет, под такие нужды, как анализ почвы посевов, работа в шахтах и сбор текущих данных.

Протокол Wi-Fi [22] обладает такими особенностями, как передача видео в реальном времени и управлением БПЛА на небольших расстояниях, а также производит синхронизацию с базовыми станциями. К его положительным аспектам можно отнести высокую скорость передачи видео (работе в реальном времени) и широкую доступность оборудования (можно использовать под большое количество задач). Но данный ППД имеет высокое энергопотребление, минимизируя время его работы, а также он чувствителен к помехам от других устройств.

Протокол DSSS [23] имеет возможность работы с телеметрией, обладает надежной связью между оператором и БПЛА. Данный протокол защищен от помехоустойчивости, но обладает малой дальностью действия (относительно аналогов). Если задачей является анализ поверхности почвы или регулировка температуры, то данный протокол будет приоритетным, из-за отсутствия аналогов по таким же характеристикам.

Протокол 4G/5G (Сотовая связь) [24] может быть использован без оператора, за счет полной автоматизации процесса. Производит передачу данных с БПЛА на сервер в режиме реального времени. Благодаря этому протоколу, получается потоковое видео высокой четкости, управление БПЛА можно вести на больших расстояниях (при наличии сети). К его минусам можно отнести наличие покрытия сотовой сети и высокое энергопотребление.

Протокол Zigbee [9] – это беспроводной стандарт для маломощных сетей. Он обладает малым энергопотреблением, хорошей помехоустойчивостью и

имеет возможность работать в сетях Mesh[10]. Данный протокол обладает такими недостатками, как малая дальность и низкая скорость передачи данных. Он может подойти под такие задачи, как связь между группами дронов или быть использован для автоматизированного управления в промышленных зонах, так же его используют для контроля публичных мероприятий.

Bluetooth (BLE – Bluetooth Low Energy)[11], он предназначен для ближней связи и использования низкого энергопотребления, прост в интеграции с мобильными устройствами. Его используют для настройки и калибровки дронов через мобильное приложение, а также для локального управления дронами.

XBee (IEEE 802.15.4)[12] так же поддерживает технологию Mesh, позволяющая взаимодействовать дронам между собой, имеет хорошую дальность вплоть до 50 км, что позволяет использовать данный ППД в поисковых или спасательных операциях, а также для логистики. Но для надежной работы, требуется подходящая инфраструктура, также протокол используют для связи дронов в распределительных системах.

Протокол Iridium(спутниковая связь)[13] имеет глобальное покрытие. Основными отличительными особенностями этого протокола можно считать именно дальность покрытия, но при этом он имеет очень низкую скорость передачи. За счет своих особенностей, его можно использовать в труднодоступных человеку местах, таких как, Арктика, пустыни и моря. Данный ППД повсеместно используют в исследовательских и анализирующих беспилотниках. В случае особой надобности, протокол можно использовать в спасательных операциях. Его главным недостатком является – стоимость, а именно цена обслуживания самой единицы техники.

LTE-M (Long-Term Evolution for Machines)[14] – протокол в мобильных сетях, обладает энергосберегающей передачей данных и возможностью работы через сотовую связь. Ему присуще ограниченная зона покрытия и он не подходит для передачи видео. Данный ППД подойдет для мониторинга дронов и передачи телеметрии.

Таким образом, выбор подходящего протокола передачи данных для беспилотных систем зависит от специфики задачи и условий эксплуатации. Для военных целей предпочтительнее использовать протоколы с высокой степенью безопасности и помехоустойчивости, в то время как в горнодобывающей промышленности и агропромышленности акцент стоит на дальности связи и энергоэффективности.

1.1.5. Аппаратные компоненты

Корпус, изготовленный из лёгких и прочных материалов (углепластик, алюминий), защищает внутренние системы от внешних воздействий. Двигательная установка (электродвигатели или двигатели внутреннего сгорания) в сочетании с пропеллерами обеспечивает тягу и маневренность. Источники питания, такие как литий-полимерные батареи, снабжают энергией все системы, а в некоторых случаях используются топливные элементы или солнечные панели для увеличения времени полёта.

Автопилот (например, Pixhawk или ArduPilot) и бортовые компьютеры (Raspberry Pi, NVIDIA Jetson) управляют полётом, стабилизацией и выполнением миссий, используя данные с навигационных систем (GPS/ГЛОНАСС, IMU, барометры).

Для связи с оператором применяются радиомодули и антенны, а для выполнения специфических задач — полезная нагрузка (камеры, датчики, манипуляторы). Также важны системы безопасности, такие как парашюты и дублирующие системы управления, которые повышают надёжность и безопасность эксплуатации БПЛА.

1.1.6. Программные компоненты

На рисунке 5 представлена общая архитектура БАС.

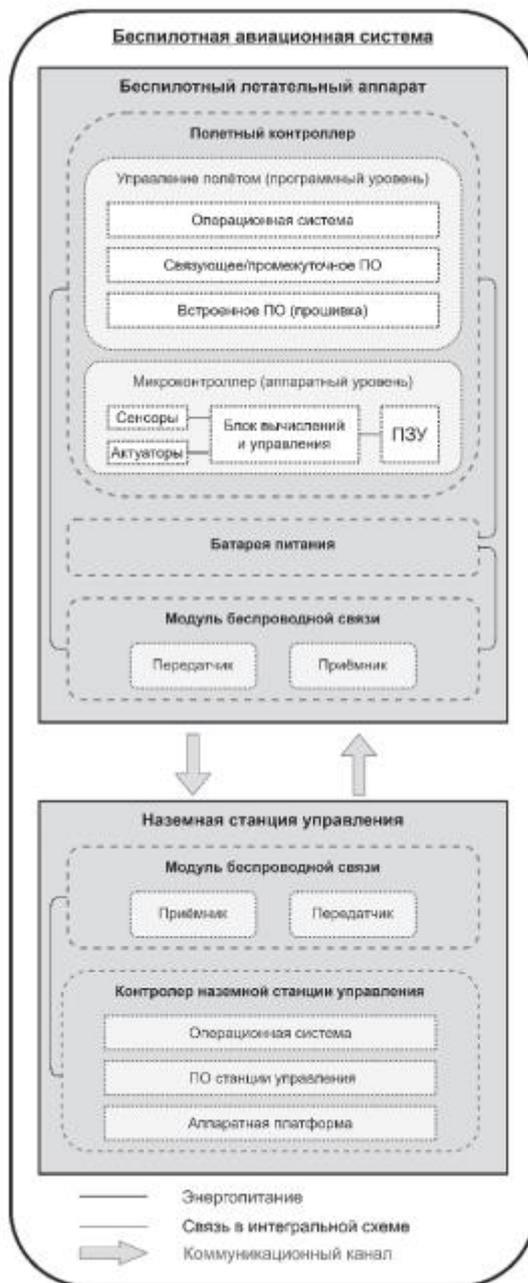


Рисунок 5 – архитектура БАС

Архитектура программного обеспечения БПЛА имеет многоуровневую структуру. Интеграция между этими уровнями составляет полетный стек или полетный контроллер, состоящий из трех основных уровней:

- Микропрограмма (прошивка) является нижним уровнем полетного стека, который предоставляет инструкции из машинного кода процессору полётного контроллера;
- Промежуточное программное обеспечение представляет собой уровень, отвечающий за надлежащее управление полетом путем управления связью между службами, такими как управление, навигация и телекоммуникации;
- Операционная система реального времени обрабатывает данные в режиме реального времени и позволяет программному обеспечению БПЛА управлять различными процессами, такими как полет, видеозапись и планирование маршрута.

Программное обеспечение наземной станции управления также известно, как планировщик миссий. Оно включает в себя человеко-машинный интерфейс, который отображает параметры полета и обычно работает на ноутбуках, планшетах или любых устройствах в полевых условиях.

1.2 Угрозы безопасности связи в системах управления БПЛА

1.2.1 Атаки на программное обеспечение.

Программные атаки на БПЛА включают в себя атаки на операционную систему ПО управления видеопотоком и подмены системных идентификаторов. Потенциальные атаки могут происходить через системное программное обеспечение контроллера полета. В результате скомпрометированное системное ПО приведет к потере БПЛА и их полезной нагрузки. Посылочные коптеры сервиса Prime Air, разработанные Amazon, являются примером гражданских приложений, которые могут подвергаться атакам на уровне операционной системы. Атака на систему доставки потенциально может быть использована для кражи посылки адресата, перевеса груза для потери БПЛА. Атака на операционные системы БПЛА состоит из удаленного внедрения вредоносного программного обеспечения, такого как Maldrone, а затем захвата дрона путем получения контроля над системой. С этой целью злоумышленник может извлечь

криптографический ключ и украсть или скомпрометировать сохраненные незашифрованные данные

1.2.2. Фальсификация видеопотока

Чтобы гарантировать безопасную навигацию и избежать столкновений во время полета, операционной системой используются системные вызовы, которые позволяют захватывать видео с бортовой камеры. Однако хорошо осведомленный с параметрами системы злоумышленник может перехватить системные вызовы для захвата БПЛА. Злоумышленник также может комбинировать фальсификацию с атакой подмены GPS-сигнала для управления БПЛА. В отличие от атак на операционную систему основная цель злоумышленника – поставить под угрозу безопасность навигации и вызвать столкновение БПЛА с другим объектом.

1.2.3. Подмена системного идентификатора

В соответствии с правилами безопасности полета в некоторых странах БПЛА должны предоставлять свой системный идентификатор и местоположение третьим сторонам, таким как федеральные агентства и правоохранительные органы, когда это необходимо. Однако большинство существующих БПЛА не реализуют механизмы шифрования и, следовательно, злоумышленник может выдать себя за третье лицо и выполнить атаку с подменой личности, чтобы скомпрометировать канал связи и получить системный идентификатор БПЛА. Производители БПЛА всё чаще вводят ряд ограничений на программном уровне в свои изделия, например, для запрета их использования противоборствующими сторонами в зоне конфликта. Поэтому становятся популярны альтернативные (неофициальные) обновления прошивок (firmware) гражданских БПЛА. Злоумышленник может распространять микропрограммы обновлений прошивок с логическими ошибками (бэкдор) [4].

1.2.4. Атаки на каналы связи

Атаки на сетевой уровень связи БПЛА включают подслушивание, отказ в обслуживании (DoS), «человек посередине», подделку, атаку повторного воспроизведения и др.

1.2.5. Атака «подслушивание»

Злоумышленник может выполнить атаку с прослушиванием через канал связи БПЛА – наземная станция управления, собирая данные, такие как прямые видеопотоки, показания датчиков и данные GPS, отправленные БПЛА. Поскольку большинство БПЛА избегают шифрования беспроводной связи ради повышения производительности связи, злоумышленник может прослушивать обмениваемую информацию.

1.2.6. DoS-атаки

Злоумышленник может забить канал связи БПЛА случайным трафиком, отправив несколько запросов, что приведет к перегрузке его ресурсов и нарушению его доступности. Воздействие выполнения таких атак на БПЛА может привести к существенному увеличению задержки в сети и снижению качества приложений потокового видео. Другой способ выполнения DoS-атаки – отправка больших пакетов на НСУ в пределах определенного диапазона для отключения управляющего сигнала. Как только сигнал отключается, БПЛА переходит в состояние потери связи, что приводит к сбоям в работе канала передачи данных. В [6] авторы моделировали распределенную DoS-атаку (DDoS) на БПЛА с использованием ботнетов. Атака DDoS была смоделирована путем переполнения сетевого трафика с использованием пакетов протокола пользовательских дейтаграмм (UDP). Этот тип моделирования демонстрирует возможность проведения реальных DDoS-атак на БПЛА. Кроме того, выполнение атак деаутентификации также может лишить оператора возможности управлять БПЛА. Атака деаутентификации – это DoS-атака, состоящая в отправке пакетов деаутентификации на БПЛА для нарушения связи. Пример таких атак демонстрирует Skyjack [3].

1.2.7. Атаки «человек посередине»

В этой одной из самых известных атак злоумышленник контролирует беспроводной канал БПЛА – наземная станция управления и изменяет безопасные пакеты вредоносным содержимым. Атака с воспроизведением видео является примером атаки «человек посередине», когда злоумышленник

обманывает оператора, передавая вредоносные данные в реальном времени. VideoJak является примером таких атак.

1.2.8. Атака «подделка»

Злоумышленник может поставить под угрозу целостность связи БПЛА, передав поддельный запрос на БПЛА, не прошедший проверку подлинности. В этой атаке злоумышленник генерирует вредоносный запрос, выдавая его за законный запрос.

1.2.9. Атака повторного воспроизведения

В сетях БПЛА злоумышленник может выполнить атаку с прослушиванием, чтобы перехватить несколько запросов, а затем воспроизвести достоверные данные на БПЛА. В этом случае БПЛА могут получать повторяющиеся данные, и если не будет реализована защита от повторного воспроизведения, БПЛА не смогут отличить законные запросы от вредоносных.

1.2.10. Атаки на маршрутизацию

В протоколах маршрутизации мобильных одноранговых сетей (MANET) могут возникать различные пассивные и активные атаки, которые состоят из внедрения вредоносных узлов, управления сетевым трафиком или нарушения функций маршрутизации. Большинство существующих атак, нацеленных на протоколы маршрутизации в сетях MANET, можно перенести на протоколы маршрутизации в сетях FANET, поскольку сети FANET являются подкатегорией сетей MANET.

1.3 Уязвимости систем связи БПЛА

1.3.1. Уязвимости программного обеспечения

Уязвимости и угрозы на уровне ПО для БПЛА состоят из вредоносного программного обеспечения и уязвимостей нулевого дня. Наземная станция управления и контроллер полета подвержены влиянию вредоносного программного обеспечения. Угрозы, исходящие от вредоносного ПО для БПЛА, могут привести к потере конфиденциальных данных, целостности и контроля над управляемой системой БПЛА. Доступ злоумышленника к полетному стеку БПЛА потенциально может привести к отключению системы БПЛА, что

приведет к отказу в обслуживании и, следовательно, к срыву полетной задачи. Внедрение такого вредоносного ПО в БПЛА может поставить под угрозу их безопасность. Например, вредоносное ПО Maldrone заражает полетный контроллер вирусом, позволяя злоумышленнику перехватить управление БПЛА [2]. Он воздействует как прокси-сервер контроллера полета БПЛА и связи с датчиками, что позволяет скомпрометированному БПЛА приземляться в любом выбранном месте. SkyJack – это вредоносное ПО для угона БПЛА, которое может быть развернуто злоумышленниками [3]. Данное ПО с помощью беспроводной связи может захватить контроль над другими «легитимными» БПЛА с помощью атаки де-аутентификации Wi-Fi и поставить под угрозу всю систему.

1.3.2. Уязвимости нулевого дня

В полетном стеке БПЛА или программном обеспечении наземной станции управления могут существовать неизвестные уязвимости (например, переполнение буфера, отказ в обслуживании и др.). Эти уязвимости неизвестны производителям БПЛА и могут представлять серьезную угрозу для операторов. Злоумышленники могут постоянно эксплуатировать уязвимости нулевого дня, пока производители БПЛА не выпустят соответствующие исправления. Однако операторам необходимо обновлять свои системы БПЛА для каждого выпущенного исправления.

1.3.3. Уязвимости каналов связи

Уязвимости и угрозы на уровне связи можно классифицировать следующим образом. Уязвимости и угрозы физического и MAC-уровня. Сложность сети беспроводной связи БПЛА – наземная станция управления открывает потенциальные уязвимости. Например, в [5] авторы продемонстрировали три различные атаки, затрагивающие коммерческие беспилотные летательные аппараты на базе Wi-Fi: атака переполнения буфера, атака DoS и атака отравления кэша ARP. Результаты их экспериментов выявили серьезные проблемы с безопасностью беспроводной связи БПЛА – наземная станция управления. Выбор правильного типа технологии беспроводной связи зависит от специфики требований полетной миссии (например, дальности

передачи, рабочей частоты, категории и др.). Однако этот выбор не гарантирует успеха, поскольку должны учитываться вопросы безопасности каждого типа технологии беспроводной связи. Таким образом, фундаментальный вопрос, который остается без ответа, заключается в том, какой тип технологии беспроводной связи обеспечивает высокий уровень безопасности БПЛА для каждой области применения. Сеть БПЛА работает в режиме ad hoc, обычно называемом FANET. Эти сети имеют динамическую топологию и представляют собой критически уязвимую структуру. Увеличение сложности сети управления БПЛА приводит к увеличению уязвимостей. Атаки нацелены в основном на входы данных сенсоров и коммуникационные модули. Угрозы связи с БПЛА, такие как перехват или блокировка канала связи между контроллером полета и наземной станцией управления, могут вызвать потенциальную DoS-атаку. Кроме того, учитывая уникальные характеристики FANET, в том числе задержку и вычислительную мощность для маршрутизации данных, необходимо создавать криптографические алгоритмы для FANET, учитывающие эти характеристики. Злоумышленник может нарушить работу сети БПЛА, отправив вредоносный трафик напрямую через наземную станцию управления или опосредованно через БПЛА. Будь то централизованная или децентрализованная архитектура, наземная станция управления постоянно находится под угрозой со стороны злоумышленника. В обеих архитектурах наземная станция управления представляет собой единую точку отказа всей сети БПЛА. Однако несмотря на то, что механизмы безопасности реализованы для наземной станции управления, злоумышленник всё равно может прервать полетное задание, скомпрометировав летающие БПЛА. Следует подчеркнуть, что в некоторых сценариях полетное задание можно считать успешным, даже если один или несколько БПЛА будут скомпрометированы. В этом случае оператору будет достаточно минимального количества корректно работающих БПЛА.

1.4 Методы и средства защиты связи в системах управления БПЛА

1.4.1. Противодействие атакам на программное обеспечение

Регулярное обновление операционной системы может предотвратить компрометацию БПЛА и их полезной нагрузки. Кроме того, функционирующий межсетевой экран на наземной станции управления может блокировать отправку вредоносного трафика на БПЛА. Программные решения, такие как антивирус и IDS, могут отслеживать сетевой трафик и защищать БПЛА от вредоносных действий. Однако внедрение бортовых IDS является сложной задачей из-за ограничений по вычислениям и энергопотреблению. Также включение механизмов авторизации для системных ресурсов БПЛА может помочь защитить системы БПЛА от выполнения вредоносного кода. Перспективным решением против программных атак является использование программных подходов к аттестации ПО. Они обеспечивают целостность программного обеспечения, работающего в полетном стеке [1]. Решения для удаленной аттестации недороги и обеспечивают надежную легитимность программного стека. Кроме того, оператор должен постоянно обновлять свою операционную систему и внедрять программные решения для аттестации, чтобы проверять легитимность кода, работающего в операционной системе. Однако стоит отметить, что представленные механизмы защиты от программных атак не могут полностью защитить полетный стек от вредоносных действий. Процесс исправления обнаруженных уязвимостей нулевого дня может занять несколько недель, делая БПЛА уязвимыми для злоумышленников.

1.4.2. Противодействие атакам на каналы связи

В литературе предложены различные подходы к обеспечению безопасности при обмене данными с БПЛА. Защита физических свойств канала связи (например, среды передачи, физической топологии и др.) является одним из способов нивелирования атак БПЛА на физическом и MAC-уровне. Учитывая широкое использование БПЛА в различных технологиях беспроводной связи, важно учитывать, что обеспечение безопасности беспроводной связи на физическом и MAC-уровне является сложной задачей из-за характеристик

каждой технологии связи (например, категории, частоты, диапазона и др.). Кроме того, алгоритмы шифрования, такие как AES, могут использоваться при обмене данными на физическом уровне и на уровне MAC. Также могут использоваться нелегитимные пользователи [17]. В дополнение к этому одним из лучших способов безопасного обмена данными является обновление микропрограммы устройства и соответствующего программного обеспечения с помощью выпущенных исправлений безопасности. Использование криптографических примитивов, таких как криптография с открытым ключом, гарантирует целостность и конфиденциальность связи БПЛА. В [12] авторы предложили схему безопасной связи для сети БПЛА с использованием метода широкополосного шифрования на основе иерархической идентификации (HIBBE). Предлагаемый подход гарантирует конфиденциальность сообщения и аутентификацию посредством шифрования на основе идентификации. Результаты их анализа производительности показали, что предложенная схема устойчива к DoS-атакам. В другой работе был представлен безопасный протокол связи, основанный на эффективном безсертификационном механизме инкапсуляции ключей подписи (eCLSCTKEM) [18]. Кроме того, протокол является энергоэффективным и соответствует требованиям безопасности и эффективности для связи с БПЛА. Для защиты коммерческих БПЛА на основе Wi-Fi в [5] представлена комплексная многоуровневая структура безопасности, которая эффективна против основных атак безопасности, таких как атаки с «отравлением» кэша ARP и атаки DoS. В [10] представлено легковесное аппаратное решение FPGA для защиты связи БПЛА – НСУ коммерческими БПЛА на основе Wi-Fi. Решение содержит криптографический механизм, отвечающий за шифрование данных управления связью. Однако включение подходов на основе криптографии потребует дополнительных вычислений, как в наземной станции управления, так и в БПЛА, и увеличения потребления энергии. Следовательно, эти решения могут снизить производительность связи БПЛА – наземная станция управления. Другие решения для обнаружения вторжений на сетевом уровне основаны на использовании методов анализа

пакетов для обеспечения целостности данных и доступности сети БПЛА. В литературе были предложены различные решения безопасности для защиты протоколов маршрутизации MANET от злоумышленников [19; 14]. Эти подходы также могут использоваться в сетях FANET и включают в себя криптографические схемы, такие как аутентификация сообщений, цифровые подписи и хеширование. Существуют также протоколы безопасной маршрутизации для FANET, чтобы гарантировать процесс маршрутизации и надежность при наличии вредоносных узлов. В эту категорию входит использование механизмов безопасности в протоколах маршрутизации. Примеры безопасных протоколов маршрутизации на основе сетей БПЛА: SUANET (безопасная специальная сеть БПЛА), PASER (позиционно зависимая, безопасная и эффективная ячеистая маршрутизация), SUAP (протокол безопасной маршрутизации БПЛА), AODVSEC (Ad hoc On-demand Distance Vector-Secure) и SRPU (протокол безопасной маршрутизации для БПЛА). Каждый из этих протоколов использует определенную стратегию для обеспечения безопасности и конфиденциальности путей маршрутизации. Например, в протоколе SUANET используется стратегия управления ключами между БПЛА для обеспечения конфиденциальности и аутентификации. Напротив, протокол PASER использует криптографические функции для защиты пакетов маршрутизации в сети БПЛА. Протокол маршрутизации SUAP предотвращает лавинную атаку. Протокол маршрутизации AODV-SEC обеспечивает безопасный процесс обнаружения маршрута. Однако реализация безопасных протоколов маршрутизации в реальных сценариях затруднена из-за их сложности и высокой плотности.

1.4.3. Противодействие атакам на транспортном уровне

Чтобы предотвратить раскрытие злоумышленником конфиденциальной информации на транспортном уровне, важно реализовать механизмы безопасности, обеспечивающие конфиденциальность и целостность передаваемых данных (например, криптографические протоколы, безопасный обмен ключами и др.). Для нивелирования атак MAVLink один из подходов

предлагает архитектуру, которая состоит из восстановления и завершения миссии в полете, несмотря на кибератаку. Существуют и другие подходы для защиты протокола связи MAVLink. В [20] исследователи разделили существующие решения безопасности MAVLink на аппаратные и программные решения. В литературе были разработаны конкретные контрмеры, гарантирующие конфиденциальность, целостность и доступность обмениваемых данных. Эти контрмеры состоят из создания решений IDS, внедрения шифрования с проверкой подлинности для предотвращения атак с целью перехвата, обеспечения многоуровневой структуры безопасности и использования безопасных протоколов маршрутизации. Однако стоит отметить, что упомянутые выше меры противодействия коммуникационным атакам БПЛА имеют некоторые ограничения и недостатки. Например, создание решений IDS для предотвращения DoS-атак влияет на производительность каналов связи. Кроме того, проблемы с задержкой возникают при шифровании данных.

1.5 Анализ существующих решений и их недостатки

Таблица 4 – Атаки на систему управления БПЛА

№ п/п	Тип атаки	Контрмеры	Ограничения
1	Вредоносное ПО	Использование межсетевых экранов. Использование антивирусных и IDS решений	Обнаружение вредоносного ПО в режиме реального времени увеличивает вычислительные расходы
2	Уязвимости нулевого дня	Периодическое обновление системы	Некоторые производители могут выпускать патчи неделями

			после обнаружения уязвимостей нулевого дня
3	Атаки на операционные системы	Принятие механизмов авторизации ресурсов системы БПЛА. Аттестация ПО [1]	В сети с несколькими БПЛА управление авторизацией для роя БПЛА является сложной задачей
4	Фальсификация видеопотока	Использование межсетевых экранов. Аттестация ПО [1]	Даже при надлежащих мерах безопасности легитимный пользователь, присоединившийся к сети БПЛА может подделать видеопоток
5	Подмена системного идентификатора	Периодическое обновление системы. Использование межсетевых экранов	Использование методов социальной инженерии может выявить системный идентификатор БПЛА еще во время их изготовления
6	Атака через альтернативное обновление прошивки (firmware)	Установка альтернативных обновлений только из доверенных источников.	Тестирование требует наличия специального стенда или дополнительного времени на работу с

		Тестирование обновления прошивки на стенде или анализ микропрограммы обновления прошивки на логические ошибки и бэкдор	БПЛА вне основной миссии. Анализ кода микропрограммы требует особых навыков и времени
7	Подслушивающие атаки	Использование антиподслушивающего алгоритма связи БПЛА [7]. Применение аутентифицированного шифрования [8]	Подходы, основанные на криптографии, требуют дополнительных вычисления и могут увеличить потребление энергии
8	DoS-атаки	Использование решений класса IDS [9]	Влияние на производительность связи БПЛА. IDS на основе сигнатур не справляется со всеми типами атак.

			IDS на основе аномалий могут страдать от ложных срабатываний
9	Атаки «человек посередине»	Шифрование данных при их передаче [10]. Внедрение методов отпечатков для аутентификации БПЛА [11]	Проблемы с задержкой для критичных ко времени приложений БПЛА
10	Атаки «подделка»	Включение многоуровневой структуры безопасности [5]	Сложность сети увеличивается в сценарии с несколькими БПЛА
11	Атаки повторов	Создание безопасной схемы связи (например, шифрование на основе идентификации) [12] Использование механизмов аутентификации [13]	Повторяющиеся запросы могут загрузить сеть и вызвать возможную DoS-атаку

12	<p>«Черная дыра» «Затопление» атака «Сибил» «Червоточина» «Лишение сна» «Византийская атака» Переадресация</p>	<p>Использование безопасных протоколов маршрутизации [14]</p>	<p>Высокие вычислительные расходы и задержки. Функции безопасности поддерживают не все протоколы маршрутизации</p>
13	<p>Атаки на протоколы связи</p>	<p>Построение высокоуровневой архитектуры отказоустойчивости и надежности, способной восстановить полетное задание, несмотря на атаку [15]. Встраивание сервисов без опасности в аппаратные модули. Использование классических подходов к обеспечению</p>	<p>Поиск компромиссов между производительностью и безопасностью</p>

		безопасности, таких как методы шифрования и подходы IDS. Использование особенностей новых технологий, таких как блокчейн [16]	
--	--	---	--

Анализ угроз в системе управления БПЛА по таблице 4 показал необходимость разработки и апробации новых подходов к обеспечению их информационной безопасности. Следует обратить внимание исследователей и специалистов по информационной безопасности на моделирование угроз с учетом их влияния на физические характеристики БПЛА, быстроедействие бортовых подсистем и полетную миссию в целом.

1.6 Выводы по первой главе

Проведённый анализ показал, что традиционные методы защиты недостаточны для полноценного обеспечения безопасности систем связи БПЛА. Для решения этой проблемы необходим комплексный подход, который может быть реализован только с использованием инструментов анализа и планирования, таких как модели предсказания уровня сигнала.

Глава 2. ХАРАКТЕРИСТИКА МОДЕЛЕЙ ДЛЯ ПРЕДСКАЗАНИЯ УРОВНЯ СИГНАЛА

Модель для прогнозирования уровня сигнала - это математическая или эмпирическая модель, которая позволяет оценить уровень мощности принимаемого радиосигнала на определённом расстоянии от передатчика, с учётом различных факторов: частоты, мощности передатчика, характеристик антенн, рельефа местности, препятствий, атмосферных условий и других параметров.

Такие модели широко используются при проектировании систем радиосвязи, включая системы управления БПЛА, для оценки зоны покрытия, качества связи и планирования размещения базовых станций или ретрансляторов.

Модели для предсказания уровня сигнала делятся на следующие классы:

- Эмпирические модели
- Физические (детерминированные) модели
- Статистические модели
- Модели машинного обучения (ML)

Каждый класс характеризуется набором достоинств и ограничений: требования к данным, интерпретируемость, вычислительная нагрузка, адаптивность.

2.1. Эмпирические модели

Эмпирические модели предсказания уровня сигнала представляют собой математические зависимости, полученные путем статистической обработки больших массивов реальных измерений мощности сигнала в различных условиях распространения радиоволн. Они аппроксимируют медианное значение потерь сигнала как функцию ключевых параметров без детального учета физических процессов (типа многолучевого распространения или дифракции). Такие модели широко применяются в задачах БПЛА для быстрого расчета зон покрытия каналов управления.

Эмпирические модели требуют минимального набора параметров:

- Расстояние между передатчиком и приемником
- Частота несущей
- Высоты антенн
- Тип местности: коэффициент коррекции
- Мощность передатчика и коэффициенты антенн

Данные о рельефе или зданиях не требуются — модель усредняет по классу ландшафта.

Преимущества:

- Высокая скорость расчета
- Простота реализации
- Низкие требования к данным

Недостатки:

- Ограниченный диапазон
- Статичность
- Игнорирование микрорельефа

Примеры моделей: Окамура, Окамура-Хата, COST-231-Хата.

2.2. Физические (детерминированные) модели

Физические (детерминированные) модели предсказания уровня сигнала основаны на строгом решении фундаментальных уравнений электродинамики (уравнений Максвелла) для конкретной геометрии среды распространения, без использования статистических аппроксимаций или эмпирических коэффициентов. Они моделируют траектории электромагнитных волн как лучи, точно рассчитывая отражения, дифракцию, преломления и затухание для заданного рельефа, зданий и антенн. Такие модели дают предсказуемый результат при фиксированных входных данных и применяются для высокоточного анализа зон связи БПЛА в сложных сценариях.

Детерминированные модели требуют высокодетализированной информации о среде:

- 3D-цифровая модель рельефа (DEM/SRTM, шаг 10-30 м)
 - Базы зданий/структур (высота материал, диэлектрическая проницаемость)
 - Параметры антенн: высота, диаграмма направленности, поляризация
 - Радиопараметры: частота, мощность, длина волны
 - Атмосферные: профиль рефракции, влажность, температура
- Данные берутся из GIS (ArcGIS), LiDAR-сканирования или OSM с доработкой.

Преимущества:

- Высочайшая точность: результат детерминирован для конкретной геометрии, без усреднения
- Полный учёт физики
- Универсальность: работает на любом диапазоне
- Визуализация: Построение карт радиополя, идентификация "мертвых зон" для маршрутов БПЛА

Недостатки:

- Вычислительная сложность
- Требования к данным
- Чувствительность к ошибкам
- Нереальное время

Примеры: Knife-Edge Diffraction («дифракция на остром крае», «дифракция на ноже»), FDTD (англ. Finite Difference Time Domain)

2.3. Статические модели

Статистические модели для предсказания уровня сигнала — это математические и вероятностные методы, которые используются для оценки и прогнозирования уровня сигнала в зависимости от различных факторов. Такие модели помогают оптимизировать размещение базовых станций, улучшать покрытие сети и планировать развитие телекоммуникационной инфраструктуры.

Минимальный статический набор (без временных/динамических параметров):

- Расстояние между антеннами
- Частота
- Высоты антенн
- Коэффициент среды или тип ландшафта
- Коэффициенты усиления

Нет нужды в DEM рельефа, погоде или траекториях движения БПЛА.

Преимущества:

- Простота реализации
- Детерминированность
- Низкие требования к данным

Недостатки:

- Отсутствие адаптивности: не моделирует динамику БПЛА (манёвры, скорость) или изменения среды.

- Узкая применимость: только идеальные условия (пустыня, космос); в городах/лесах неприменима.

Примеры: Free Space Path Loss (FSPL), One-Slope, Статическая двухлучевая модель (Two-Ray Static).

2.4. Модели машинного обучения

Модели машинного обучения (МО) для предсказания уровня сигнала — это алгоритмы, которые обучаются на больших массивах реальных данных телеметрии (RSSI, SNR, координаты, рельеф, погода) для аппроксимации или прогнозирования мощности принимаемого сигнала без явных физических формул. Они выявляют скрытые нелинейные зависимости, недоступные традиционным моделям, и адаптируются к конкретным сценариям БПЛА.

Входные данные

- Историческая телеметрия БПЛА: GPS (x,y,z), скорость/курс, RSSI/SNR/BER, timestamp (10^4 – 10^6 точек).
- Геоданные: DEM рельефа (SRTM/AW3D30), карты застройки (OSM), тип почвы/вегетации.
- Параметры среды: температура, влажность, давление (метео), загруженность спектра (спектральный анализ).
- Радио: частота, мощность TX, высота антенн, тип модуляции.

Преимущества:

- Высокая точность
- Адаптивность
- Динамика
- Реальное время

Недостатки:

- Черный ящик
- Ресурсы
- Большой объём данных

Примеры: LSTM (Long Short-Term Memory), XGBoost, Gaussian Processes (GP).

2.5. Сравнительный анализ типов моделей

Все модели предсказания уровня радиосигнала — эмпирические, физические, статистические и модели машинного обучения — могут применяться для обеспечения надёжной и безопасной связи БПЛА. Согласно данным, представленным в таблице 5, их сравнение позволяет выбрать наиболее экономически эффективный и оптимальный вариант, который не только гарантирует стабильную связь, но и снижает эксплуатационные затраты, минимизирует риски сбоев и адаптируется к изменяющимся условиям среды.

Таблица 5 – Сравнение типов моделей предсказания уровня сигнала

Критерий	Эмпирические модели	Физические (детерминированные) модели	Статистические модели	Модели машинного обучения (ML)
Основной принцип	Основаны на экспериментальных данных и упрощённых формулах	Основаны на физических законах распространения радиоволн	Основаны на вероятностных методах и статистических данных	Основаны на обучении алгоритмов на больших объёмах данных
Точность	Средняя	Высокая	Средняя	Очень высокая (при достаточных данных)
Скорость вычислений	Высокая	Низкая	Средняя	Низкая (после обучения)
Требования к данным	Минимальные	Высокие (детальные параметры среды)	Средние	Очень высокие (большие объёмы данных)
Универсальность	Ограничена условиями эксперимента	Высокая	Средняя	Очень высокая

Критерий	Эмпирические модели	Физические (детерминированные) модели	Статистические модели	Модели машинного обучения (ML)
Сложность реализации	Низкая	Высокая	Средняя	Высокая
Применимость для БПЛА	Подходит для простых сценариев	Подходит для сложных сценариев	Подходит для анализа больших данных	Подходит для динамических и сложных сценариев
Адаптивность к изменениям среды	Низкая	Средняя	Средняя	Высокая
Необходимость экспертных знаний	Минимальные	Высокие	Средние	Высокие

В рамках данного исследования была разработана программная модель предсказания уровня сигнала управления БПЛА на основе эмпирических моделей. Этот выбор обусловлен необходимостью обеспечить быстрое и надёжное предсказание в условиях ограниченных ресурсов, что актуально для большинства коммерческих и военных БПЛА. Несмотря на ограниченную точность в сложных условиях, модель демонстрирует достаточную эффективность для заданных сценариев и может быть легко масштабирована или дополнена более сложными алгоритмами в будущем.

В качестве основы для разработки программной модели были выбраны эмпирические модели "Окамура", "Окамура-Хата", "COST-231-Хата" и "Ли" поскольку они охватывают основные частотные диапазоны, используемые в

системах управления БПЛА. Эти модели позволяют учитывать разнообразные условия эксплуатации: от открытых пространств и сельской местности до плотной городской застройки, что обеспечивает универсальность и применимость разработанной модели для большинства современных коммерческих и военных беспилотных систем.

Для реализации программной модели необходимо привести теоретические основы расчёта затухания сигнала с использованием выбранных эмпирических моделей. Это включает в себя детальное описание формул, параметров и условий их применения: например, учёт частоты сигнала, высоты антенн, расстояния между передатчиком и приёмником, а также поправочных коэффициентов для различных типов местности. Кроме того, требуется разработать алгоритмы адаптации моделей под конкретные сценарии эксплуатации БПЛА, что позволит повысить точность предсказания уровня сигнала и обеспечить надёжную связь в заданных условиях.

2.6. Модель Окамуры

Модель Окамуры по предсказанию уровня сигнала в пределах соты основана на экспериментальных результатах, полученных при следующих условиях: высота повеса антенны БС над средним уровнем квазигладкой местности (трассы) 200 м, высота антенны МС 3м, расстояние между БС и МС r (1...100) км (длинные трассы), диапазон частот (100...3000) МГц. Трасса, на которой средняя высота неровностей не превышает 20 м, определена в модели Окамуры как «квазигладкая» [1].

По модели Окамуры сначала определяется УММС в антенне приемника (на входе приемника), находящегося на расстоянии 1км от БС, при распространении радиоволны над квазигладкой местностью:

$$P_M(r) = p_0(f, r) - a_M(f, r) + N_1(h_1, r) + N_2(h_2, f) \text{ где}$$

$a_M(f, r)$ – дополнительное ослабление сигнала в городе (медианное значение), определенное для квазигладкого городского района при базовых высотах антенн БС и МС; $N_1(h_1, r)$ – коэффициент «высота - усиление антенны БС», учитывающий, что высота антенны БС может отличаться от значения 200м;

$H_2(h_2, f)$ – коэффициент «высота-усиление антенны МС», учитывающий влияние реальной высоты антенны МС.

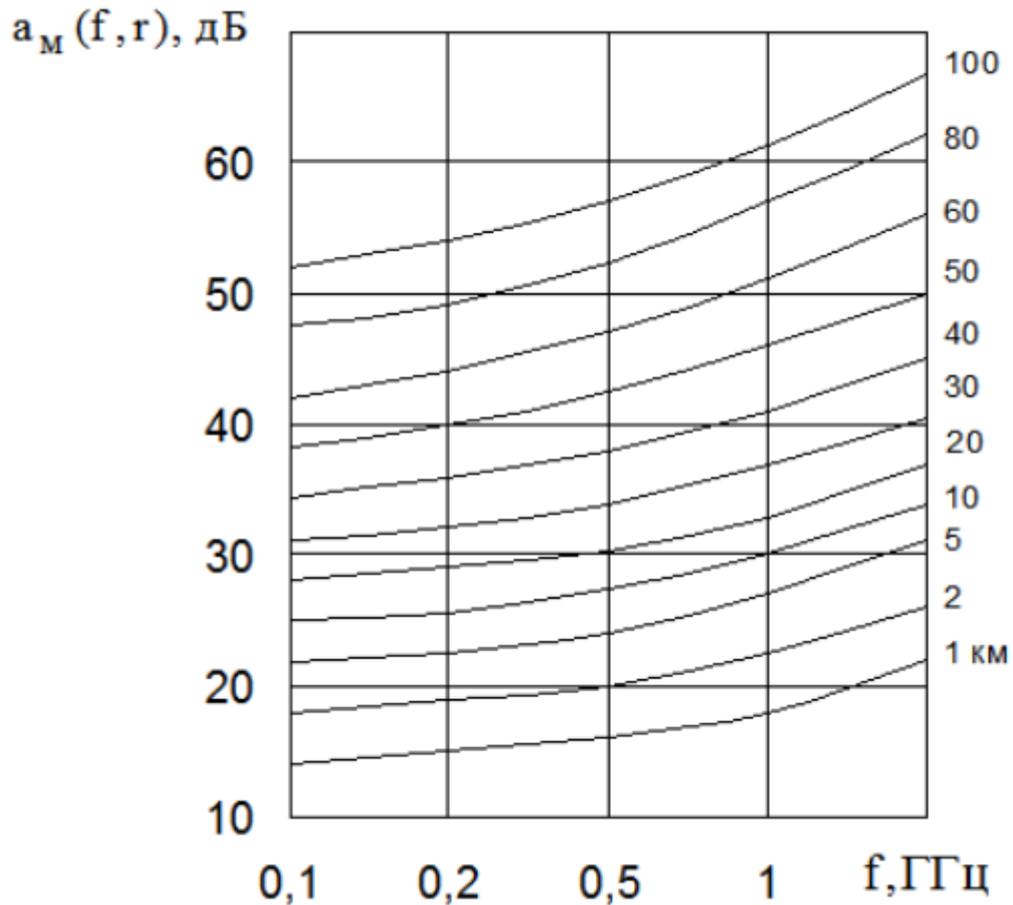


Рисунок 6 – Медианное ослабление сигнала на городских трассах протяженностью r

После расчета $P_{AM}(1 \text{ км}, f)$ рассчитывается УММС в антенне приемника для $r \geq 1 \text{ км}$:

$$P_{AM}(r, f) = P_{AM}(1 \text{ км}, f) = 10 \lg(r/1\text{км})^n + H_1(h_{BC}, r) + H_2(h_{MC}, f), \quad (9)$$

где n показатель затухания для квазигладкой городской застройки, который зависит от высоты антенны БС и протяженности трассы. Из приведенных на рисунке 6 зависимостей следует, что в условиях города показатель затухания резко возрастает при r 15-20 км);

$H_1(h_{BC}, r)$ коэффициент «высота-усиление антенны БС», учитывающий, что высота антенны БС может отличаться от значения 200 м , причем при $20\text{м} \leq h_{BC} \leq 1000 \text{ м}$:

$$H_1(h_{BC}, r) = 20 \lg (h_{BC}/ 200 \text{ м}), \text{ если } 1 \text{ км} \leq r \leq 10 \text{ км}, \quad (10)$$

$$N_1(h_{BC}, r) = (20 + (r \text{ км} - 10) / 3) \lg (h_{BC} / 200 \text{ м}), \text{ если } 10 \text{ км} \leq r \leq 100 \text{ км};$$

(11)

$N_2(h_{MC}, f)$ коэффициент «высота-усиление антенны МС», учитывающий, что высота антенны МС может отличаться от значения 3 м :

$$N_2(h_{MC}) = 10 \lg (h_{MC} / 3 \text{ м}), \text{ если } 1 \text{ м} \leq h_{MC} < 3 \text{ м},$$
 (12)

$$N_2(h_{MC}, f) = (20 + (f \text{ МГц} - 400) / 160) \lg(h_{MC}/3 \text{ м}), \text{ если } 3 \text{ м} \leq h_{MC} \leq 10 \text{ м},$$

(12)

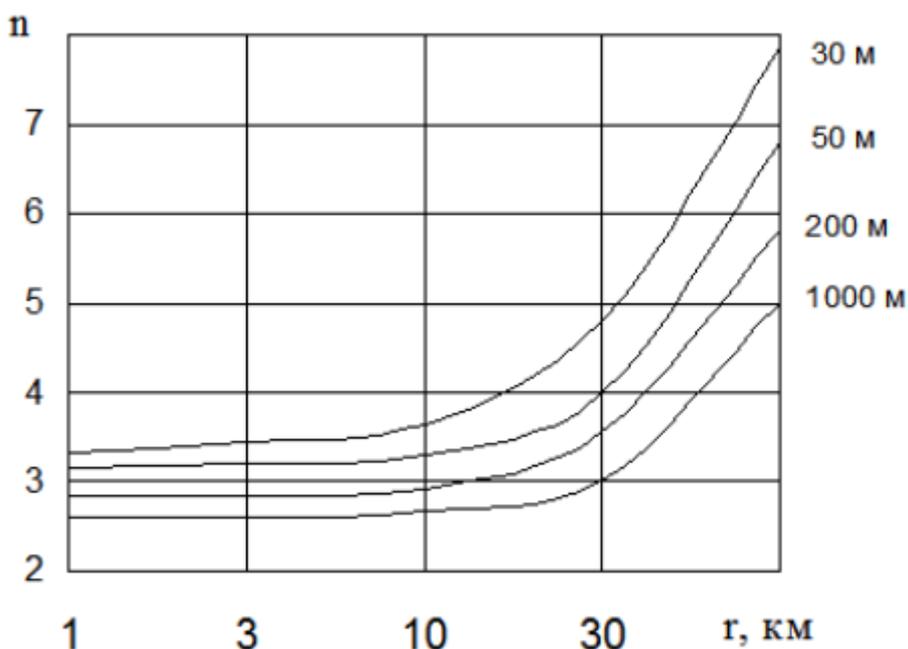


Рисунок 7 – Ориентировочные зависимости показателя затухания от протяженности трассы при различных высотах антенны БС для квазигладкого городского района

Формулы (8) - (13) аппроксимируют экспериментально измеренные Окамурой зависимости $N_1(h_{BC}, r)$ и $N_2(h_{MC}, f)$. На практике величина n определяется экспериментально.

Для местности, которая не относится к квазигладкой, модель Окамуры предусматривает введение поправочных коэффициентов в (9):

$$P_{MZ}(r, f) = P_M(r, f) + K_{Zоткр} + K_{Zнакл} + K_{Zводн} + K_{Zхолм},$$
 (14)

$K_{Zоткр}$ - поправочный коэффициент для пригородной зоны или для открытой трассы;

$K_{Zнакл}$ - поправочный коэффициент для трассы с наклоном;

$K_{Z_{\text{водн}}}$ - поправочный коэффициент для трассы земля - вода;

$K_{Z_{\text{холм}}}$ - поправочный коэффициент для холмистой (горной) местности.

В пригородной зоне потери сигнала при распространении меньше, чем в городе, поскольку в ней меньше строений и они ниже по высоте; еще меньше потери на открытой местности. Эти потери уменьшаются с ростом частоты и могут быть найдены из зависимостей рисунок 8.

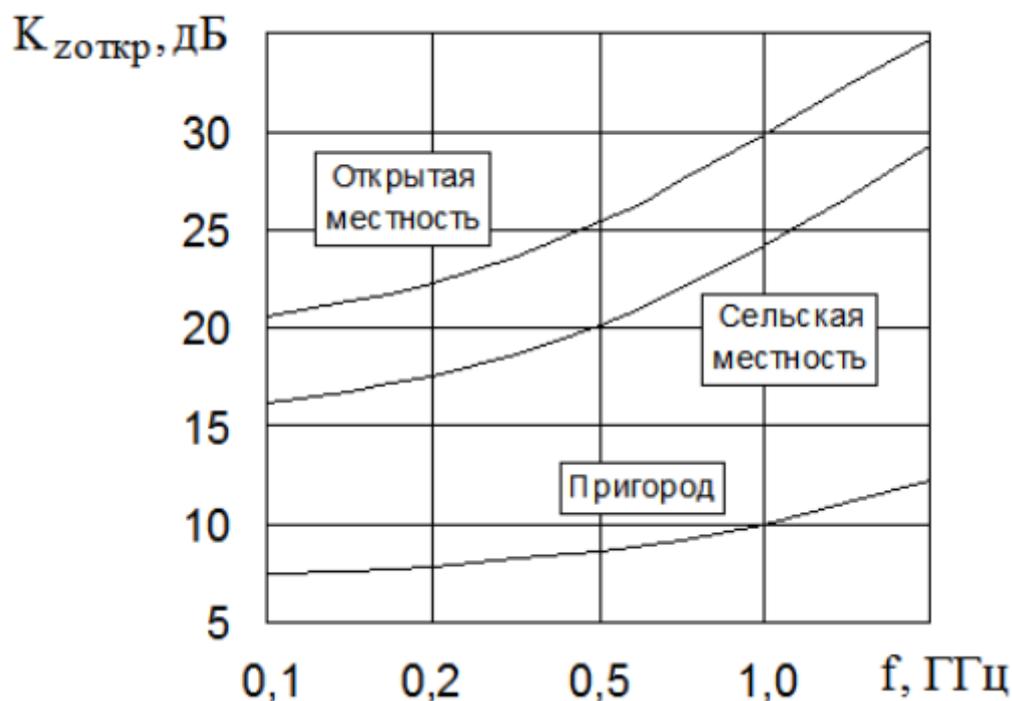


Рисунок 8 – Зависимости поправочных коэффициентов от частоты для различных трасс

Трассы с наклоном – это трассы с понижающимся или с повышающимся наклоном протяженностью 5 км и более. Для них определяется средний угол наклона $\phi_{\text{ср}}$, причем $\phi_{\text{ср}}$ – отрицательный, если МС находится на нижнем участке трассы, и $\phi_{\text{ср}}$ – положительный, если МС находится на верхнем участке трассы. Зависимости $K_{Z_{\text{накл}}}$ от $\phi_{\text{ср}}$ представлены на рисунке 9.

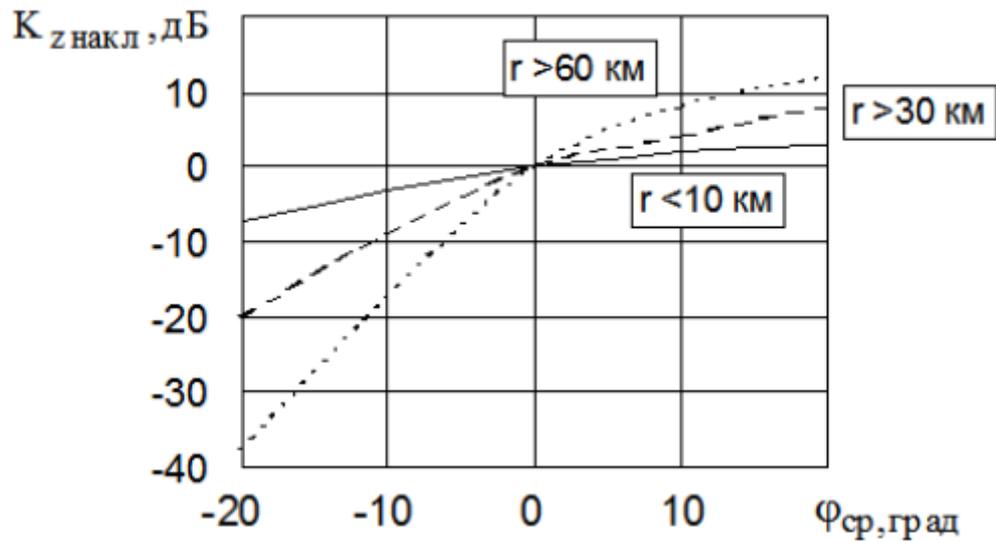


Рисунок 9 – Поправочные коэффициенты на трассах с наклоном

Ослабление сигнала уменьшается, если трасса распространения имеет водную поверхность (рисунок 10). Коэффициент $K_{Z_{\text{водн}}}$ зависит от отношения $b = r_{\text{в}} / r$, где

$r_{\text{в}}$ - протяженность трассы над водой;

r - общая протяженность трасс

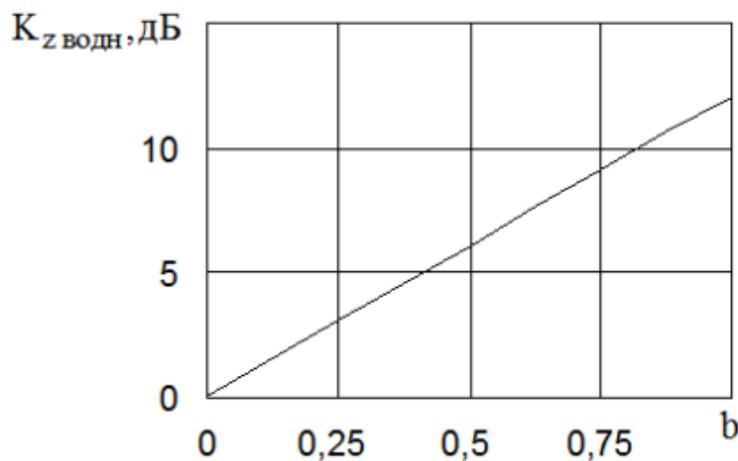


Рисунок 10 – Поправочный коэффициент для трассы с водной поверхностью

При расчете ослабления сигнала при распространении над холмистой (горной) местностью величина дополнительного ослабления (по сравнению с квазигладкой местностью) зависит от средней высоты неровностей

$$\Delta h = h(10\%) - h(90\%) \quad (15)$$

где h (10 %), (h 90 %) - значения высот местности на трассе протяженностью около 10 км, превышаемые в 10% и 90% точек профиля соответственно (рисунок 11).

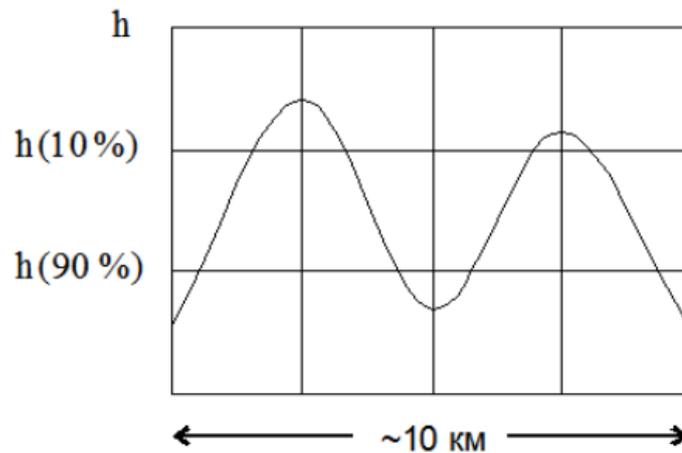


Рисунок 11 – Оценка холмистой (горной) поверхности

Зависимости $K_{Z_{\text{холм}}}$ от Δh представлены на рисунок 12.

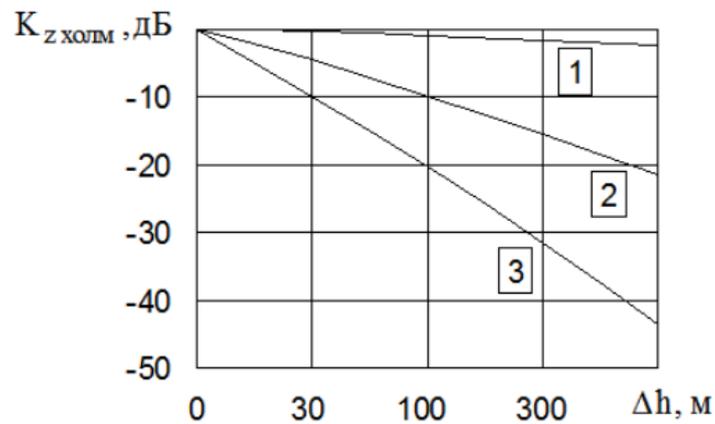


Рисунок 12 – Поправочный коэффициент для холмистой (горной) трассы.

Местонахождение МС: 1 – у вершины холма; 2 – промежуточное положение; 3 – у основания холма

2.7. Модель Окамура-Хата

Результаты экспериментальных измерений Окамуры положены в основу модели Хата. Эмпирические зависимости, используемые в модели Окамуры в виде графиков, в этой модели представлены в виде аппроксимирующих их формул. Согласно этой модели вместо (1.2) представим уровень УММС как

$$p_M(r) = p_{\Pi} + q_1 + q_2 - a_1 - a_2 - a_{MX}(f, r, h_1, h_2) \quad (1.9)$$

где $a_{MX}(f,r,h_1,h_2)$ - суммарное ослабление радиосигнала при распространении для модели Хата при статистическом учете параметров местности (a - выражено в децибелах, r – в километрах):

- для города

$$a_{MX}(f,r,h_1,h_2) = A + B \lg r; \quad (1.10)$$

- для пригородной зоны

$$a_{MX}(f,r,h_1,h_2) = A + B \lg r - C;$$

(1.11)

- для открытой местности

$$a_{MX}(f,r,h_1,h_2) = A + B \lg r - D;$$

(1.12)

Здесь аппроксимирующие коэффициенты:

$$A = A(f, h_1, h_2) = 69,55 + 26,16 \lg(f) - 13,82 \lg(h_1) - \alpha(h_2);$$

$$B = B(h_1) = [44,9 - 6,55 \lg(h_1)]$$

$$C = C(f) = 2[\lg(f/28)]^2 + 5,4;$$

$$D = D(f) = 4,78(\lg f)^2 - 19,33 \lg(f) + 40,94;$$

$\alpha(h_2)$ – параметр, учитывающий влияние высоты антенны МС.

Для крупных городов этот параметр слабо зависит от частоты, для средних и малых городов этот параметр зависит от частоты, однако используются две аппроксимирующие формулы:

$$\alpha(h_2) = 8,28[\lg(1,54h_2)]^2 - 1,1 \quad \text{при } f \geq 200 \text{ МГц};$$

$$\alpha(h_2) = 3,2[\lg(11,75h_2)]^2 - 4,97 \quad \text{при } f \geq 400 \text{ МГц};$$

для средних и малых городов этот параметр зависит от частоты;

$$\alpha(h_2) = (1,1 \lg f - 0,7)h_2 - (1,56 \lg f - 0,8)$$

В формулах для аппроксимирующих коэффициентов принято: f – частота излучения БС в МГц; r – расстояние между БС и МС в км; h_1 и h_2 – высоты установки антенны БС и МС. Модель Хата применяют при изменении параметров в пределах, указанных в таблице 5.

Таблица 5 – Пределы применения модели Хата

параметр	частота	высота антенны БС	высота антенны МС	протяженность трассы
обозначение	f , МГц	h_1 , м	h_2 , м	R
основная область	от 150 до 1500	от 30 до 200	от 1 до 10	от 1 до 20 км
расширенная область		от 1.5 до 400		от 2 до 80 км

Область применения модели Хата меньше области использования модели Окамуры. Аппроксимирующие выражения по модели Хата совпадают с результатами Окамуры с точностью до 1 дБ в пределах основной области и с меньшей точностью в пределах расширенной области.

Для предсказания уровня сигнала на трассах короче 1 км существуют другие модели.

2.8. Модель Ли

В моделях Ли местность классифицируют по двум признакам:

- по инфраструктуре, сформированной человеком (характер застройки): открытая территория, пригородная зона, городская застройка;
- по естественным свойствам (характер трассы): гладкая, холмистая, трасса над водной поверхностью, трасса через лиственные леса.

Модель «от зоны к зоне» создана на основании анализа результатов измерений уровня сигнала (локального среднего), опубликованных разными авторами для зон с различным характером застройки. В ее основе два следующих экспериментальных параметра модели:

p_1 - уровень сигнала в точке, отстоящей от БС на 1 миллю (или 1 км);

γ - наклон кривой потерь распространения. Численно равен ослаблению сигнала при увеличении длины трассы в 10 раз; единица измерения – дБ на декаду (дБ/дек).

Согласно этой модели, уровень мощности на входе приемника МС

$$P_c = p_1 + \alpha_1 - \gamma \lg R_{mi} + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 \quad (1.13)$$

где R_{mi} - протяженность трассы, выраженная в милях (миля = 1,6 км); p_1 и γ - параметры модели, определенные при типовых энергетических параметрах аппаратуры указанных в табл.5. $\alpha_1 \dots \alpha_5$ - поправочные коэффициенты; вводятся в случае, когда технические параметры отличаются от параметров по таблице 6.

Таблица 6 – Типовые параметры модели Ли

Параметры	стандартные значения	поправочные коэффициенты
Уровень мощности передатчика БС - $p_{БС}$	$p_{БС}^* = 40$ дБм	$a_1 = p_{БС} - 40$
Высота антенны БС - h_1	$h_1^* = 100$ фут (30м)	$a_2 = 20 \lg(h_1/h_1^*)$
Коэффициент усиления антенны БС - g_1	$g_1^* = 6$ дБ	$a_3 = g_1 - 6$
Высота антенны МС - h_2	$h_2^* = 10$ фут (3м)	$a_4 = 10 \lg(h_2/h_2^*)$
Коэффициент усиления антенны МС - g_2	$g_2^* = 0$ дБ	$a_5 = g_2$

Для определения параметров модели использованы результаты измерений мощности сигнала на трассах. Зависимости уровня мощности сигнала, измеренные для этих трасс показаны на рисунке 10.

Эти результаты получены при определенных стандартных параметрах, указанных в таблице 7.

Таблица 7 – Результаты модели Ли

№	трасса	p_1 , дБм	γ , дБ/де к	№	трасса	p_1 , дБм	γ , дБ/де к
1	открытая	-49	43,5	4	Токио	-84	30,5
2	типовая пригородная	-61,7	38,4	5	Нью Йорк Сити	-77	48
3	Филадельфия	-70	36,8	6	свободное пространство	-45	20

Подставив в (1.13) параметры модели Ли для трассы «типовая пригородная» и выражение для a_1 из табл.5. записывают уровень мощности сигнала на входе приемника МС:

$$P_c = 61.7 + (P_{\text{БС}} - 40) - 38.4 \lg R_{mi} + a_2 + a_3 + a_4 + a_5, \text{ дБм}, \quad (1.14)$$

Поправка при протяженности трассы (R) в километрах (1 миля = 1.6 км).: $Z_1 = 38.4 \lg(R/1.6) = 38.4 \lg R - 7.84$.

При стандартных параметрах (см. табл.5.) уровень мощности сигнала на расстоянии 1 км от БС (в дБм) $P_c = -61.7 + 7.84 = -53.86$. Подставив величины a_2 и a_4 в (1.14) находим $P_c = P_{\text{БС}} = -134.31 - 38.4 \lg R + 20 \lg(h_1) + 10 \lg(h_2) + g_1 + g_2$.

Окончательно в модели Ли для трассы «типовая пригородная» принят наклон $\gamma = 40$ дБ/дек (40 дБ на декаду) и указана контрольная точка $R = 10$ миль, в которой уровень мощности сигнала равен -100 дБм. Расчетная формула для модели Ли

$$P_c = P_{\text{БС}} = -132.7 - 40 \lg R + 20 \lg(h_1) + 10 \lg(h_2) + g_1 + g_2, \text{ дБм}, \quad (1.15)$$

где R выражено в км, а h_1 и h_2 - в м. Физический смысл слагаемых в (1.15) поясняется в таблице 8.

Таблица 8 – Пояснение к расчетной формуле

Слагаемое формулы	Физический смысл
$P_{\text{БС}} = -132.7 = P_c^*(1)$	уровень мощности сигнала на расстоянии 1 км от БС при стандартных условиях, дБм
$-\gamma \lg R$	учитывает влияние сформированной структуры

	($\gamma = 40$ дБ/декада для трассы «типовая пригородная»)
$+20 \lg h_1$	фактор «высота — усиление антенны БС», учитывающий влияние профиля трассы
$\varepsilon = 10 \lg h_2 + g_1 + g_2$	фактор, учитывающий отклонение технических параметров от стандартных указанных в табл.3.

Зависимость от длины трассы. Представляют (1.15) в виде

$$P_C(R) = k_i - 40 \lg R \quad (1.16)$$

где $k_i = P_C(1) = P_{БС} - 132.7 + 20 \lg(h_1) + 10 \lg(h_2) + g_1 + g_2$, дБм

$$(1.17)$$

- уровень мощности сигнала в точке приема на расстоянии 1 км от БС для трассы «типовая пригородная». Соответствующая мощность сигнала

$$P_C(1) = K_t = 10^{0,1k_i}; \text{ мВт.}$$

$$(1.18)$$

Мощность сигнала в точке приема на расстоянии R км от БС, с застройкой типа «типовая пригородная»

$$P_C(R) = K_t R^{-4}, \text{ мВт} \quad (1.19)$$

Аналогично (1.19) можно записать мощность сигнала в точке приема на расстоянии R км от БС, с застройкой любого типа:

$$P_M(R) = K_i R^{-n} \quad (1.20)$$

где K_i - мощность сигнала в точке приема на расстоянии 1 км от БС, для трассы с заданным типом застройки; $n = 0.1\gamma$ - показатель затухания, зависящий от типа застройки. Значение K_i и n можно найти на основании данных табл.6., а также (1.16).

При расчете реальных трасс следует сравнить рассматриваемую территорию с подходящей структурой из табл.6. Поскольку все пригородные зоны похожи, то для них используют (1.19). Для городов показатели затухания существенно отличаются. Так, например, для Токио $n=3$, а для центральной части Нью-Йорка $n=5$. В модели Ли указано, что в случае необходимости для

конкретных трасс могут быть проведены достаточно простые измерения уровня сигнала на расстоянии 1 миля и 10 миль от БС. В каждой точке должно быть выполнено по 5 - 7 измерений и их результаты усреднены. Локальные средние значения могут быть подставлены в (1.20).

Сопоставив (1.19) и 1.7), а также (1.20) и (1.6) отмечаем их совпадение.

Дополнительные факторы, которые могут влиять на значение уровня сигнала – это ориентация улиц и близость лесных массивов. При радиальном расположении городских улиц относительно БС возможно возникновение волноводного эффекта, и как следствие, усиление принимаемого сигнала. Принятого на МС сигналы, направления распространения которых параллельны направлениям улиц, имеют уровень мощности на 10...20дБ выше, чем сигналы, приходящие с других направлений. На частотах ниже 1 ГГц этот эффект значительно ослаблен. Если траектория радиосигнала пересекает лиственный лес, то нужно учитывать дополнительные потери из-за рассеяния его листвой. Эти потери могут добавляться в каждом конкретном случае. Установлено, что чем ближе БС лесного массива тем сильнее ослабление сигнала листвой. Поэтому следует избегать расположения БС вблизи лиственных массивов. Антенны БС должны быть подвешены выше верхушек деревьев.

2.9. Модель COST-231-Хата

Появление сотовых систем мобильной связи, работающих на частотах около 2 ГГц , стимулировало появление модели COST 231– Хата, которая применяется в диапазоне (1500...2000) МГц при протяженности трассы (1...20)км , высоте антенны БС (30...200) м , высоте антенны МС (1...10) м [6]:

$L_p=45,5-13,82\lg(h_{БС})+35,41\lg(f)-[1,1\lg(f)-0,7]h_{МС}+[44,9-6,55\lg(h_{БС})]\lg(r)$ – для центра столичного города;

$L_p=45,5-13,82\lg(h_{БС})+35,41\lg(f)-[1,1\lg(f)-0,7]h_{МС}+[44,9-6,55\lg(h_{БС})]\lg(r)$ – для среднего города и пригородного центра с умеренной плотностью посадки деревьев;

$L_p=9,56-13,82\lg(h_{БС})+53,73\lg(f)-[1,1\lg(f)-0,7]h_{МС}-4,78[1\lg(f)]^2+[44,9-6,55\lg(h_{БС})]\lg(r)$ – для сельской местности;

$L_p = 4,56 - 13,82 \lg(h_{BC}) + 53,73 \lg(f) - [1,1 \lg(f) - 0,7] h_{MC} - 4,78 [\lg(f)]^2 + [44,9 - 6,55 \lg(h_{BC})] \lg(r)$ – для открытой местности.

2.10. Выводы по второй главе

Модели предсказания уровня сигнала не являются самостоятельным решением, а работают в комплексе с другими методами обеспечения безопасности связи. Модели прогнозирования уровня радиосигнала являются ключевыми инструментами для обеспечения надежной и безопасной связи в системах управления БПЛА, потому что способны: предотвращать инциденты с потерей управления, защищать от помех и кибератак, минимизировать риски столкновений с различными объектами, подготавливать систему к динамическим условиям окружающей среды.

ГЛАВА 3. РАЗРАБОТКА ПРОГРАММНОЙ МОДЕЛИ ПРЕДСКАЗАНИЯ УРОВНЯ СИГНАЛА УПРАВЛЕНИЯ БПЛА

Конечная цель разработки программной модели предсказания уровня сигнала управления БПЛА заключается в создании надёжной, точной и адаптивной системы, способной прогнозировать качество связи между БПЛА и НСУ. Это позволит предотвращать потерю сигнала, оптимизировать маршруты полёта, повышать устойчивость к внешним помехам и атакам, а также обеспечивать безопасность и эффективность выполнения полётных заданий. В результате модель должна стать инструментом, который поможет операторам и автономным системам БПЛА принимать обоснованные решения для поддержания стабильной связи в различных условиях эксплуатации.

3.1. Анализ вариантов реализации программной модели

Существует множество вариантов реализации данного проекта. Рассмотрим основные из них:

1. Десктопная программа для анализа и сравнения моделей
2. Плагин для программ планирования полётных заданий
3. Встроенный аппаратный модуль на борту БПЛА
4. Облачная платформа для анализа и предсказания
5. Мобильное приложение для операторов БПЛА

3.1.1. Десктопная программа для анализа и сравнения моделей

Десктопная программа для анализа и сравнения моделей прогнозирования уровня сигнала — это автономное приложение, устанавливаемое на персональный компьютер, которое предназначено для загрузки, обработки и анализа данных, а также визуализации и интерпретации результатов. Такая программа позволяет пользователю выбирать точные модели для решения конкретных задач, тестировать гипотезы для дальнейшей интеграции в реальные системы, обеспечивая удобный интерфейс для взаимодействия и анализа.

Преимущества:

- Гибкость в выборе алгоритмов и моделей.
- Возможность тестирования и сравнения различных подходов.
- Удобство для исследовательских целей и анализа данных.

Недостатки:

- Требуется ручной запуск и анализа результатов.
- Не интегрирована в реальные системы управления БПЛА.

3.1.2. Плагин для программ планирования полётных заданий

Плагин для программ планирования полётных заданий — это программный модуль, который интегрируется в существующие специализированные приложения (например, Mission Planner, QGroundControl, UgCS) для расширения их функциональности путём добавления новых инструментов анализа, оптимизации или автоматизации. Модуль позволяет встраивать алгоритмы машинного обучения или физические модели непосредственно в интерфейс программы планирования, обеспечивая возможность автоматического учёта прогнозируемого уровня сигнала при построении маршрутов, оценке рисков потери связи и оптимизации параметров полёта. Плагин взаимодействует с основной программой через её API, используя её данные и интерфейс для отображения результатов, что делает его удобным и простым инструментом для операторов БПЛА.

Преимущества:

- Интеграция с существующими инструментами, которые уже используются операторами БПЛА.
- Возможность автоматически учитывать предсказания уровня сигнала при планировании маршрута.
- Удобство для пользователей, которые уже знакомы с интерфейсом программы.

Недостатки:

- Ограничения, связанные с особенностями архитектуры программ (например, сложность интеграции новых алгоритмов).
- Зависимость от обновлений основной программы.

3.1.3. Встроенный аппаратный модуль на борту БПЛА

Встроенный аппаратный модуль на борту БПЛА — это специализированное электронное устройство (микроконтроллер, микропроцессор или программируемая логическая матрица), физически интегрированное в бортовую систему БПЛА, предназначенное для автономного сбора, обработки и анализа данных в реальном времени. Такой модуль выполняет задачи предсказания уровня сигнала управления, оценивая текущие условия связи (например, расстояние до наземной станции, помехи, атмосферные условия) и оперативно корректируя параметры полёта (например, изменяя высоту, маршрут или частоту связи) для предотвращения потери сигнала. Он работает независимо от внешних систем, обеспечивая надёжность и устойчивость связи даже в условиях ограниченного доступа к наземной станции, и оптимизирован для работы с ограниченными вычислительными ресурсами и энергопотреблением.

Преимущества:

- Реальное время: Возможность предсказывать уровень сигнала непосредственно на борту БПЛА, что позволяет оперативно реагировать на изменения условий связи.
- Автономность: БПЛА может самостоятельно принимать решения (например, изменять маршрут или высоту полёта) для поддержания связи.
- Надёжность: Уменьшение зависимости от наземной станции управления.

Недостатки:

- Ограниченные вычислительные ресурсы на борту БПЛА.

- Сложность обновления алгоритмов и моделей.
- Потребность в оптимизации кода для работы на микроконтроллерах.

3.1.4. Облачная платформа для анализа и предсказания

Облачная платформа для анализа и предсказания уровня сигнала управления БПЛА — это распределённая вычислительная система, развёрнутая на удалённых серверах и предоставляющая доступ к мощным ресурсам обработки данных через интернет. Такая платформа предназначена для сбора, хранения, анализа и предсказания уровня сигнала связи между БПЛА и НСУ с использованием алгоритмов машинного обучения, статистических методов или физических моделей. Она обеспечивает масштабируемость, позволяя одновременно обрабатывать данные от множества БПЛА, а также гибкость за счёт возможности быстрого обновления алгоритмов и моделей без изменения аппаратной части. Облачная платформа позволяет операторам и системам управления получать актуальные прогнозы в реальном времени, оптимизировать маршруты полётов, предотвращать потерю связи и повышать общую надёжность управления БПЛА.

Преимущества:

- **Вычислительные мощности:** Возможность использования мощных серверов для сложных вычислений.
- **Масштабируемость:** Легко масштабировать систему для работы с большим количеством БПЛА.
- **Обновляемость:** Простота обновления моделей и алгоритмов.

Недостатки:

- Зависимость от качества связи с облаком.
- Задержки в передаче данных и получении результатов.

3.1.5. Мобильное приложение для операторов БПЛА

Мобильное приложение для операторов БПЛА — это программное обеспечение, устанавливаемое на мобильные устройства (смартфоны,

планшеты), предназначенное для управления, мониторинга и анализа работы беспилотных летательных аппаратов в полевых условиях. Такое приложение интегрирует функции планирования полётных заданий, отображения телеметрии в реальном времени, визуализации данных с датчиков, а также предсказания уровня сигнала управления с использованием встроенных алгоритмов машинного обучения или подключения к облачным сервисам. Оно обеспечивает операторам удобный и интуитивно понятный интерфейс для контроля состояния связи, принятия решений по корректировке маршрутов и параметров полёта, а также получения уведомлений о потенциальных рисках потери сигнала. Мобильное приложение позволяет работать в условиях ограниченной инфраструктуры, обеспечивая мобильность, доступность и оперативность управления БПЛА.

Преимущества:

- Удобство и доступность для операторов.
- Возможность работы в полевых условиях.
- Интеграция с другими функциями управления БПЛА.

Недостатки:

- Ограниченные вычислительные ресурсы мобильных устройств.
- Зависимость от операционной системы и аппаратной платформы.

Таблица 9 Сравнительная характеристика вариантов реализации проекта

Вариант реализации	Основное Преимущества	Основной Недостаток	Применение
Десктопная программа	Гибкость, возможность сравнения моделей.	Не интегрирована в реальные системы	Исследовательские задачи, анализ данных.

Вариант реализации	Основное Преимущество	Основной Недостаток	Применение
Плагин	Интеграция с существующими инструментами	Ограничения архитектуры программы	Практическое использование для планирования маршрутов.
Аппаратный модуль на борту БПЛА	Работа в реальном времени	Ограниченные вычислительные ресурсы	Автономные полёты, предотвращение потери связи.
Облачная платформа	Возможность использования мощных серверов для сложных вычислений	Зависимость от качества связи с облаком	Управление группой БПЛА, мониторинг в реальном времени.
Мобильное приложение	Удобство и доступность для операторов	Ограниченные вычислительные ресурсы	Управление БПЛА в полевых условиях.

В дипломной работе был определен вариант реализации программной модели предсказания уровня сигнала управления БПЛА в виде десктопного приложения. На основании анализа рассмотренных вариантов, представленных в таблице 9.

В работе [1] была разработана программа для расчёта уровня сигнала в системе подвижной радиосвязи, которая стала основой для создания текущей программы предсказания уровня сигнала управления БПЛА. Новая программа включает в себя расширенный функционал для анализа и сравнения различных моделей.

3.2. Выбор технологии реализации

Для эффективного управления БПЛА программное обеспечение должно предоставлять операторам удобный графический интерфейс, выполнять сложные вычисления уровня сигнала, а также обеспечивать гибкую визуализацию данных — всё это требует использования языка программирования с развитыми инструментами для научных расчётов, быстрой разработки интерфейсов и кроссплатформенной поддержки, что делает Python оптимальным выбором для реализации данного решения.

Имеющиеся недостатки в рамках поставленной задачи несущественны, вследствие чего и была выбрана данная технология

3.3. Разработка алгоритма предсказания уровня сигнала

Для решения задачи предсказания уровня сигнала управления БПЛА был разработан алгоритм, представленный в виде блок-схемы. Алгоритм включает последовательность этапов: от ввода параметров до вывода графика зависимости уровня сигнала от расстояния для каждой модели, а также формирования отчёта с результатами точности моделей. Блок-схема наглядно иллюстрирует логику работы алгоритма.

Алгоритм работы программы представлен на рисунке 13.

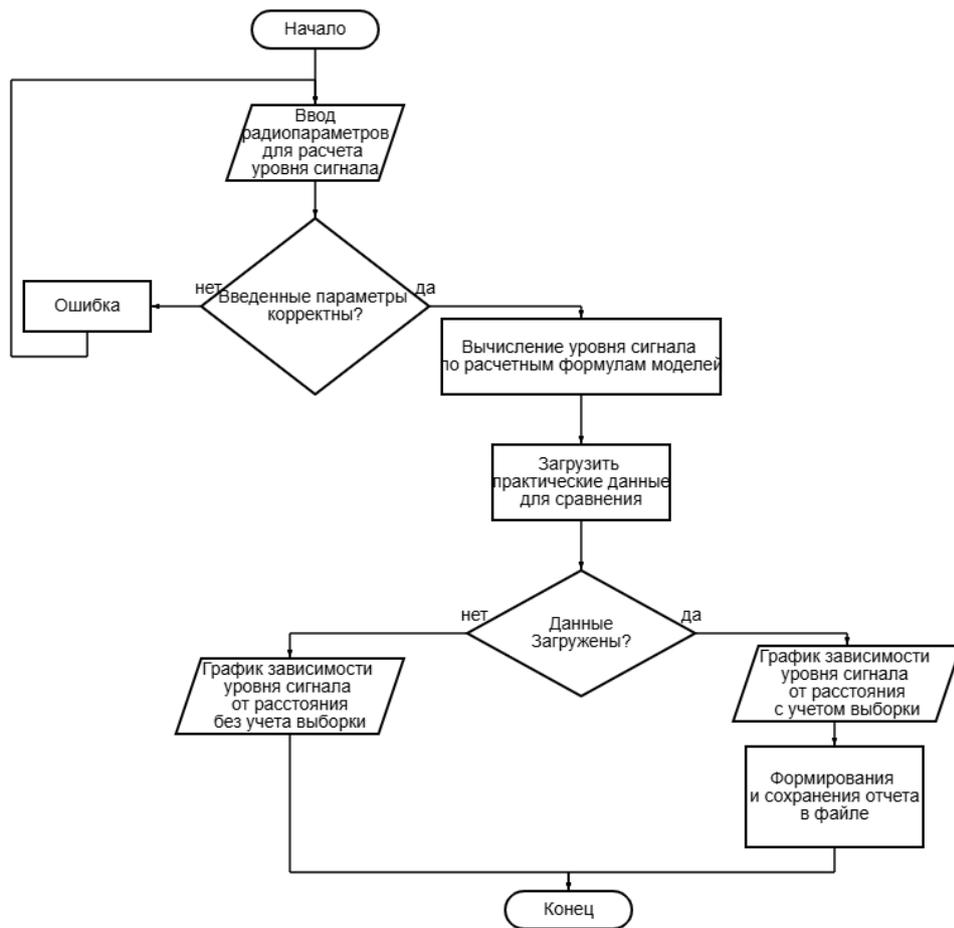


Рисунок 13 – Блок схема алгоритма

3.4. Описание функционала программы

Для обеспечения простоты и удобства интерфейс программы реализован единым окном. Представлен на рисунке 14.

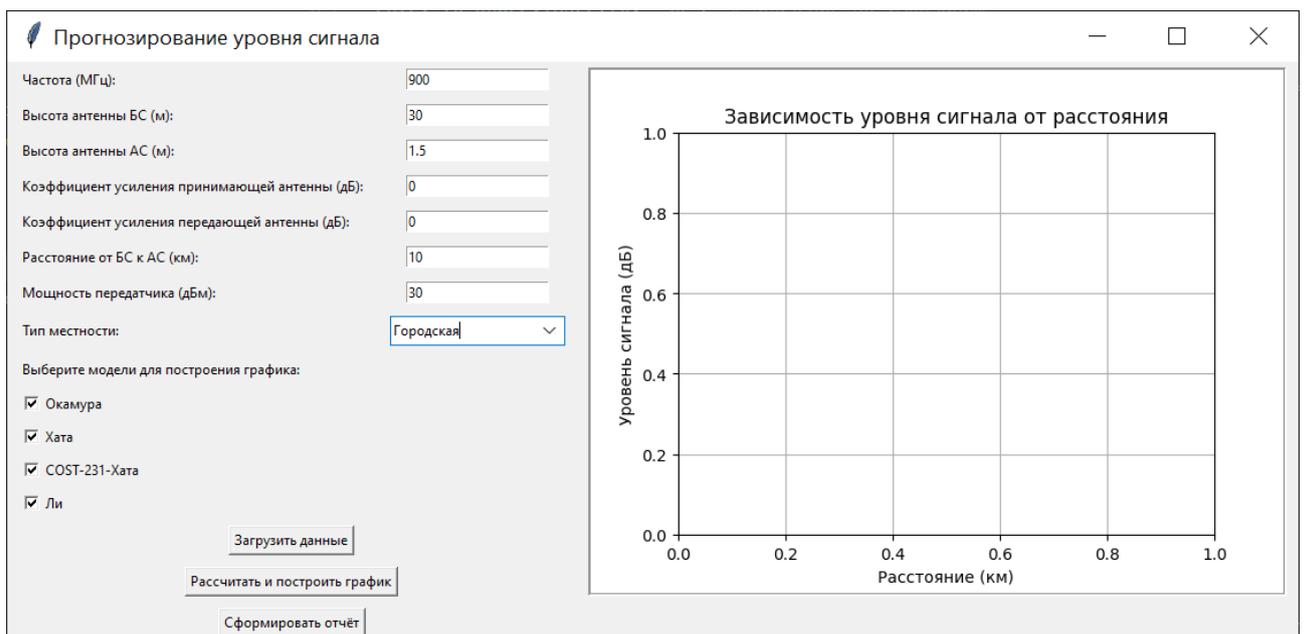


Рисунок 14 – программа "Прогнозирование уровня сигнала"

В главе 2 приведены параметры, необходимые для расчёта по эмпирическим моделям (рисунок 15).

Частота (МГц):	<input type="text" value="900"/>
Высота антенны БС (м):	<input type="text" value="30"/>
Высота антенны АС (м):	<input type="text" value="1.5"/>
Коэффициент усиления принимающей антенны (дБ):	<input type="text" value="0"/>
Коэффициент усиления передающей антенны (дБ):	<input type="text" value="0"/>
Расстояние от БС к АС (км):	<input type="text" value="10"/>
Мощность передатчика (дБм):	<input type="text" value="30"/>
Тип местности:	<input type="text" value="Городская"/>

Рисунок 15 – Компоненты ввода параметров для расчета уровня сигнала

Для корректной работы программы оператор должен вводить точные и достоверные значения. Неправильный ввод данных может привести к ошибкам в расчётах. В случае некорректного заполнения система отобразит окно с сообщением об ошибке (рисунок 16).

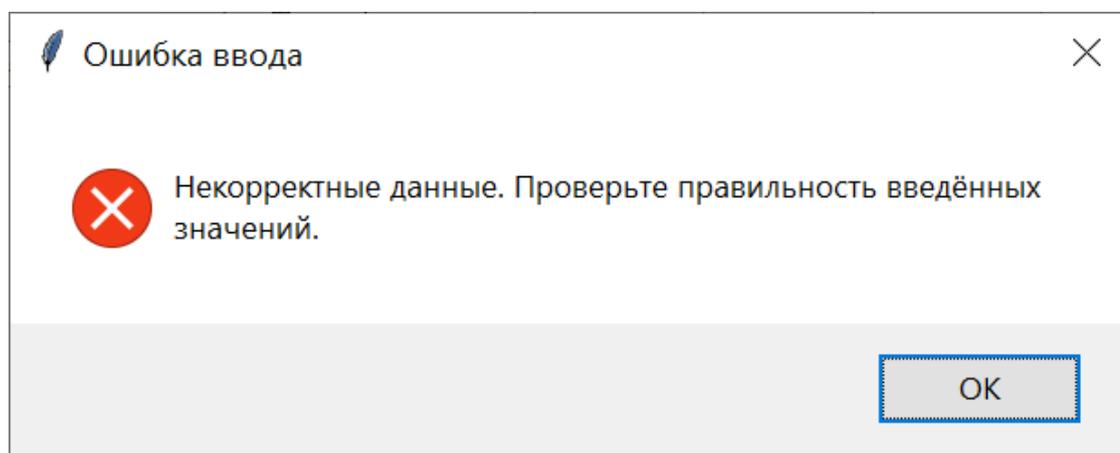


Рисунок 16 – Ошибка ввода

Выбор моделей осуществляется соответствующими флажками (рисунок 17).

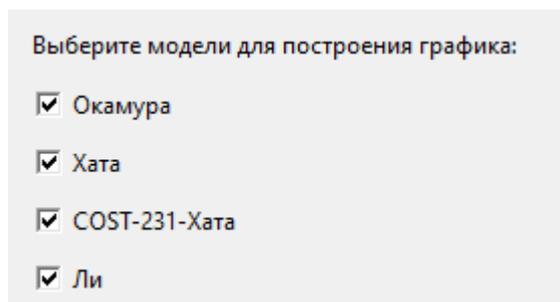


Рисунок 17 – Выбор моделей

На рисунке 18 представлены основные элементы, используемые для анализа моделей. С их помощью осуществляется загрузка достоверных данных из файла с расширением CSV, необходимых для сравнительного анализа, вычисление уровня сигнала, построение графиков, а также сохранение отчёта в формате DOCX с результатами работы программы.

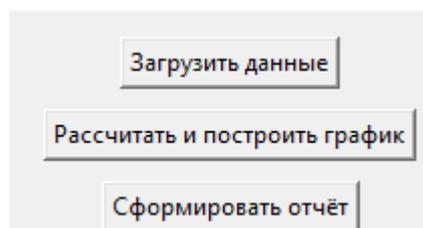


Рисунок 18 – Кнопки основного функционала программы

3.5. Тестирование модели

В рамках исследования была проведена экспериментальная валидация разработанных программных моделей предсказания уровня сигнала управления БПЛА. Тестирование осуществлялось с использованием практических данных, полученных из [4]. Данные включали в себя реальные измерения уровня сигнала, полученные в практических условиях эксплуатации, а также ключевые параметры, влияющие на качество связи.

В Таблице 10 представлены практические данные измерений уровня сигнала, полученные в ходе экспериментов. Эти данные использовались для сравнения с предсказанными значениями.

Таблица 10. Практические параметры

Расстояние до точки, км	RSSI, дБм
0.1	-87
1	-92
2	-110
3	-104
4	-108
5	-115
6	-125
7	-113
8	-118
9	-120
10	-113
11	-118
12	-123
13	-130
14	-126
15	-135
16	-137

Расстояние до точки, км	RSSI, дБм
17	-125
18	-115
19	-118
20	-124
21	-132
22	-139
23	-128
24	-129
25	-125
26	-137
27	-124
28	-119
29	-123

В Таблице 11 приведены исходные параметры, использовавшиеся в расчётах.

Таблица 11 - Исходные параметры

Параметр	Значение
Частота (МГц)	868
Высота антенны БС (м)	30
Высота антенны МС (м)	1,5
Коэффициент усиления принимающей антенны	0
Коэффициент усиления передающей антенны	0
Тип местности	Городская
Мощность передатчика (дБм)	15
Расстояние между передатчиком и приемником (км)	30

3.6. Анализ результатов работы программы.

На основании результатов, представленных на рисунке 19, можно сделать следующие выводы об адекватности используемых моделей:

- Все теоретические модели демонстрируют экспоненциальное затухание уровня сигнала с увеличением расстояния, что соответствует физическим законам распространения радиоволн.
- Модели Ли и Окамура показывают наиболее близки к практическим значениям, что представляет сложность определить визуально наилучшую модель.
- Модели Хата и COST-231-Хата показывают наибольшее затухание сигнала, что может быть обусловлено их упрощёнными предположениями о рельефе местности.

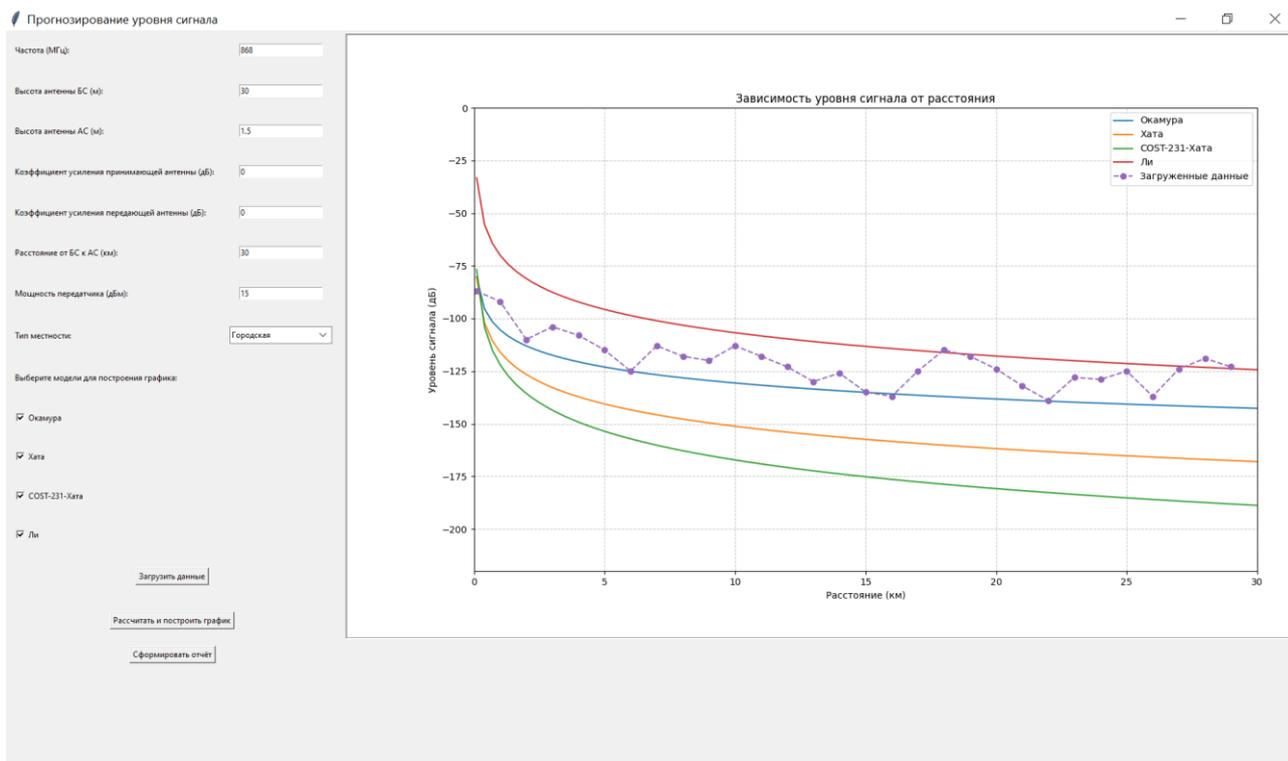


Рисунок 19 – График зависимости уровня сигнала от расстояния с учетом практических данных

Для повышения точности оценки адекватности разработанных моделей целесообразно сформировать отчёт, включающий исходные параметры расчётов, значения среднеквадратичного отклонения (RMSE), а также метрика точности, полученные в результате сравнения теоретических предсказаний с экспериментальными данными.

На рисунке 20 представлены результаты тестового эксперимента, оформленные в виде отчёта с расширением DOCX. Анализ данных показал, что модель Окамура демонстрирует наилучшие характеристики для прогнозирования уровня сигнала в полевых условиях.

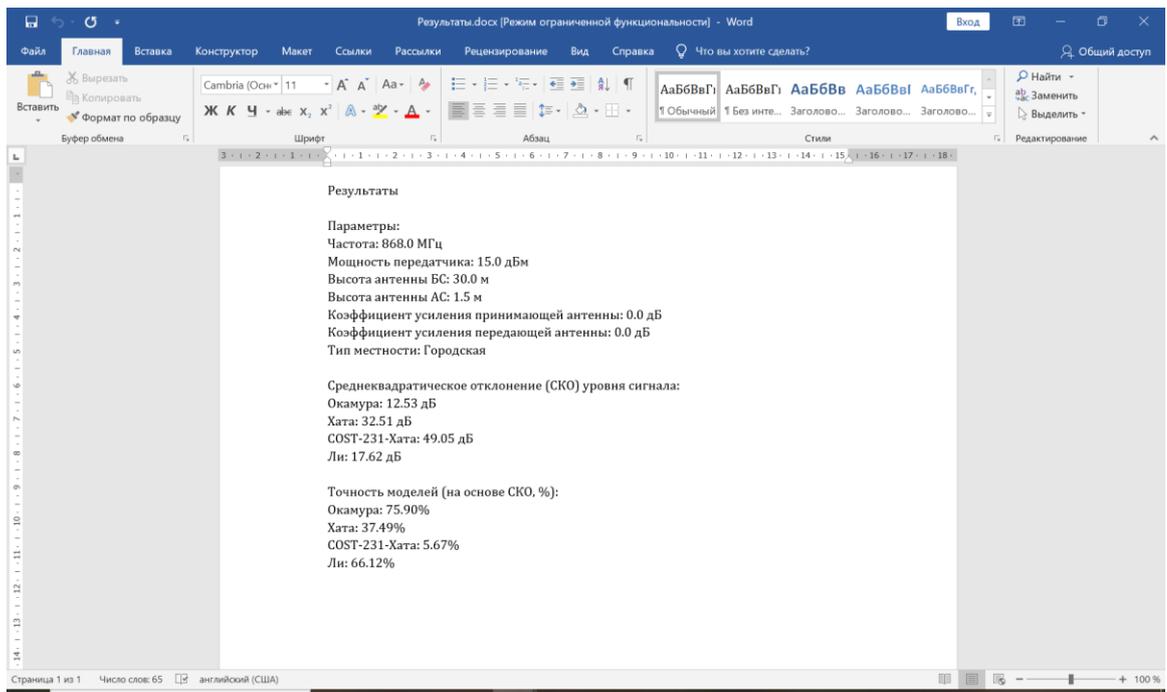


Рисунок 20 – Сформированный отчёт

Для проведения расчётов с использованием исходных параметров возможно применение любой из рассматриваемых моделей с целью оценки потенциальных потерь связи (рисунок 21). Однако возникает вопрос об обоснованности выбора модели, обеспечивающей наибольшую точность результатов, при отсутствии экспериментальных данных для валидации.

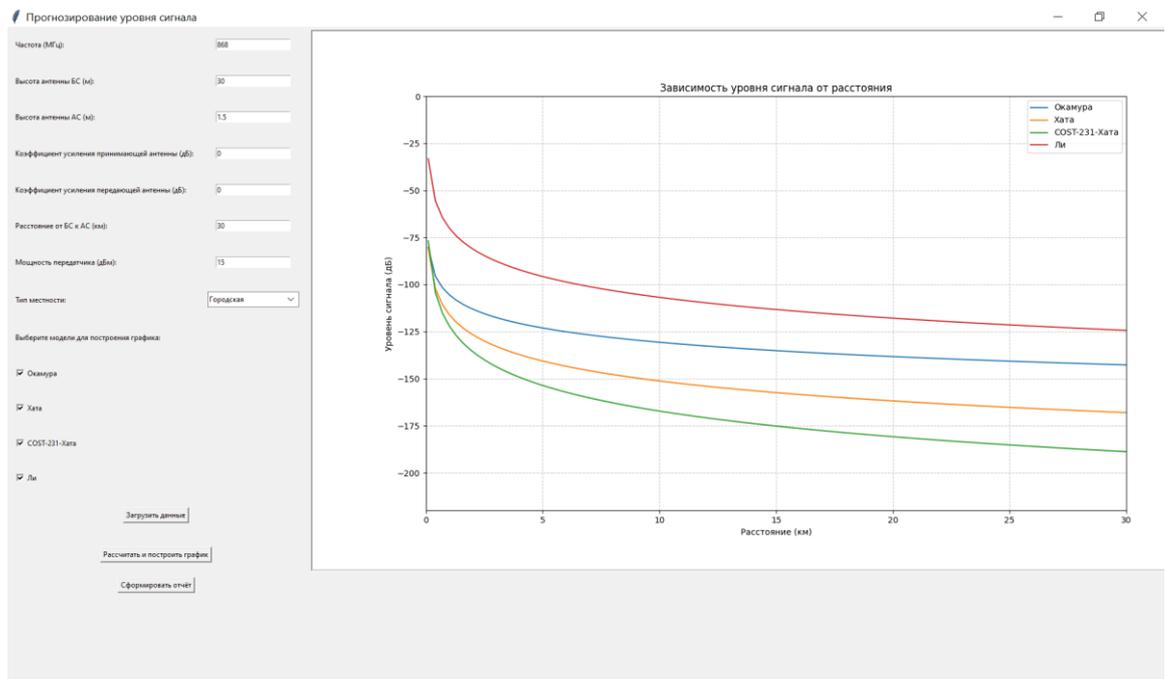


Рисунок 21 – График зависимости уровня сигнала от расстояния без учета практических данных

Выбор оптимальной модели зависит от стратегии применения, доступных вычислительных и временных ресурсов, а также от условий эксплуатации, таких как тип местности (городская застройка, сельская местность, открытые пространства), наличие помех и требований к надёжности связи. В каждом конкретном случае необходимо учитывать специфику среды распространения сигнала и ограничения, накладываемые условиями задачи.

3.7. Выводы по третьей главе

В ходе исследования был разработан, теоретически обоснован и экспериментально протестирован прототип программной модели (приложение А), предназначенной для прогнозирования уровня сигнала управления БПЛА с высокой степенью точности.

Практическая значимость разработанной программы заключается в её способности оптимизировать маршруты полётов БПЛА, что минимизирует риск потери связи и повышает надёжность выполнения поставленных задач. Кроме того, результаты исследования открывают перспективы для создания полностью автономных систем управления, способных адаптироваться к динамически изменяющимся условиям эксплуатации.

Экспериментальные данные и анализ результатов подтверждают эффективность и применимость разработанных алгоритмов для практического использования в системах управления БПЛА. Внедрение данной модели способствует повышению безопасности и экономической целесообразности применения БПЛА в различных отраслях, включая мониторинг, сельское хозяйство, экологические исследования и поисково-спасательные операции.

ЗАКЛЮЧЕНИЕ

В ходе выполнения дипломной работы было проведено комплексное исследование, направленное на разработку программной модели предсказания уровня сигнала управления БПЛА. Объектом исследования выступили системы связи и управления БПЛА, а предметом — программная модель безопасного распространения сигнала управления БПЛА.

Основной целью исследования являлась разработка программной модели, способной прогнозировать уровень сигнала управления БПЛА с высокой точностью, что позволяет повысить надёжность и безопасность систем управления. Для достижения поставленной цели были решены следующие задачи:

1. Проведён анализ современных проблем безопасности связи в системах управления БПЛА. Установлено, что традиционные методы защиты недостаточны для обеспечения полноценной безопасности в условиях динамически изменяющейся среды. Для решения этой проблемы необходим комплексный подход, включающий использование инструментов анализа и планирования, таких как модели предсказания уровня сигнала.

2. Исследованы существующие модели предсказания уровня сигнала, такие как модели Окамура, Хата, COST-231-Хата и Ли. Показано, что модели прогнозирования уровня радиосигнала являются ключевыми инструментами для обеспечения надёжной и безопасной связи в системах управления БПЛА. Они позволяют предотвращать инциденты с потерей управления, защищать от помех и кибератак, минимизировать риски столкновений с объектами и адаптировать систему к динамическим условиям окружающей среды.

3. Обоснован выбор программной среды для разработки модели предсказания уровня сигнала управления БПЛА. Использование языка программирования Python и библиотек Pandas, NumPy, Scikit-learn и Matplotlib обусловлено их простотой, богатой экосистемой для анализа данных, а также возможностью создания интерактивного графического интерфейса для визуализации результатов.

4. Разработана, теоретически обоснована и экспериментально протестирована программная модель предсказания уровня сигнала управления БПЛА. Модель позволяет загружать реальные данные, проводить их предобработку, обучать и тестировать различные модели машинного обучения, визуализировать результаты и сравнивать их с экспериментальными данными, а также формировать отчёты о точности предсказаний.

5. Проведена оценка практической значимости разработанной модели. Её применение позволяет оптимизировать маршруты полётов БПЛА, минимизируя риск потери связи, повышать надёжность систем управления за счёт адаптивного прогнозирования уровня сигнала, а также создавать полностью автономные системы управления, способные адаптироваться к изменяющимся условиям эксплуатации. Внедрение данной модели способствует повышению безопасности, эффективности и экономической целесообразности использования БПЛА в различных отраслях, таких как мониторинг, сельское хозяйство, экологические исследования и поисково-спасательные операции.

Таким образом, в результате проведённого исследования была разработана программная модель предсказания уровня сигнала управления БПЛА, которая позволяет повысить надёжность и безопасность систем управления. Полученные результаты подтверждают эффективность и применимость разработанных алгоритмов для практического использования в системах управления БПЛА.

Дальнейшее развитие модели может включать интеграцию с системами искусственного интеллекта для адаптивного прогнозирования уровня сигнала в реальном времени, разработку гибридных моделей, сочетающих теоретические подходы с методами машинного обучения, а также внедрение в коммерческие и государственные проекты, связанные с применением БПЛА. Данная работа вносит значимый вклад в развитие систем связи и управления БПЛА, открывая новые возможности для повышения безопасности и эффективности их применения.

СПИСОК ЛИТЕРАТУРЫ

1. Чернецова Е. А., Белов А.А. Программа расчета уровня сигнала в системе подвижной радиосвязи // Информационные технологии и системы: управление, экономика, транспорт, право. – 2025. – № 4(52). – С. 114-120
2. Кузьмин А.П. Савельев М.Ф, Актуальные проблемы информационной безопасности программного обеспечения и каналов связи коммерческих беспилотных авиационных систем Вестник Российского нового университета 2023-Выпуск №3 С 157-169
3. Коннов, А. Д. Разработка метода обнаружения атак на беспилотный летательный аппарат на основе анализа сетевого трафика / А. Д. Коннов, Р. Р. Галимов // Современная наука: актуальные проблемы, достижения и инновации: Материалы Международной научно-практической конференции, Чистополь, 29 мая 2020 года / ЧУДПО «Научно-исследовательский и образовательный центр». - Казань: ООО ПК «Астор и Я», 2020. С. 33–41.
4. Славнов, В. К. Устройство выявления, подавления каналов управления и телеметрии сверхмалых БЛА / В. К. Славнов, О. М. Барсуков, Н. А. Корчагин // Актуальные проблемы деятельности подразделений УИС: Сборник материалов Всероссийской научно-практической конференции, Воронеж, 25 октября 2018 года / Ответственный за выпуск Д. Г. Зыбин. - Воронеж: Издательско-полиграфический центр «Научная книга», 2018. - С. 134–137.
5. Долгий, Е. Ю. Разработка схемы защищённого канала дальнего радиуса действия для наземной станции управления беспилотного летательного аппарата / Е. Ю. Долгий, К. В. Шошина, Р. А. Алешко // Молодой учёный. - 2015. - № 13.1 (93.1). - С. 10–12.
6. Авдонин, И. А. Организация защиты данных, передаваемых между беспилотным летательным аппаратом и наземной станцией управления, на основе шифра Вернама / И. А. Авдонин, М. Б. Будько, В. А. Грозов // Научно-технический вестник информационных технологий, механики и оптики. - 2016. - Т. 16. - № 5. - С. 850–855.

7. Андреев Р.А., Прасолов А.А., Федоров А.С. Исследование дальности связи технологии LoRa в условиях мегаполиса // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т, 2021. – Т. 3. – С. 21-27.
8. Recommendation ITU-R P.525-2 «Calculation of free-space attenuation» // The International Telecommunication Union (ITU). URL: <https://www.itu.int/md/R15-SG03-C-0009> (дата обращения: 24.04.2024).
9. Коршунов Н.А., Котельников Р.В. Борьба с лесными пожарами: проблема информационного обеспечения авиасредствами и ее решение // Пожарная безопасность. – 2008. - №1. – С.125-129
10. Гуров В. А. Разработка и исследование алгоритма перемещения беспилотных летательных аппаратов в составе роя по заранее заданным маршрутам //Шаг в науку. – 2024. – №. 4. – С. 41-46
11. Душин С. В., Шаврин С. С., Алешин В. С., Фархадов М. П. Тенденции и перспективы развития беспроводной подводной связи // DSPA: Вопросы применения цифровой обработки сигналов. 2020. Т. 10. № 2. С. 11–18. EDN: ISOJOA

ПРИЛОЖЕНИЕ А

Исходный код программы “Прогнозирования уровня сигнала”

```
import tkinter as tk
from tkinter import ttk, messagebox, filedialog
import matplotlib.pyplot as plt
import numpy as np
import pandas as pd
from matplotlib.backends.backend_tkagg import FigureCanvasTkAgg
from docx import Document

# Глобальная переменная для хранения загруженных данных
loaded_data = None

def validate_inputs():
    try:
        frequency = float(entry_frequency.get())
        bs_antenna_height = float(entry_bs_height.get())
        ms_antenna_height = float(entry_ms_height.get())
        rx_gain = float(entry_rx_gain.get())
        tx_gain = float(entry_tx_gain.get())
        distance = float(entry_distance.get())

        if (
            frequency <= 0
            or bs_antenna_height <= 0
            or ms_antenna_height <= 0
            or distance <= 0
        ):
            raise ValueError
```

```

    return True
except ValueError:
    messagebox.showerror(
        "Ошибка ввода",
        "Некорректные данные. Проверьте правильность введённых значений.",
    )
    return False

def load_data():
    global loaded_data
    file_path = filedialog.askopenfilename(filetypes=[("CSV files", "*.csv")])
    if file_path:
        try:
            # Попробуем прочитать файл с разными разделителями
            try:
                loaded_data = pd.read_csv(file_path, delimiter=";")
            except:
                try:
                    loaded_data = pd.read_csv(file_path, delimiter=",")
                except Exception as e:
                    messagebox.showerror("Ошибка", f"Ошибка при загрузке данных:
{e}")
            return

        # Покажем информацию о загруженных данных
        messagebox.showinfo(
            "Информация о данных",
            f"Количество столбцов: {loaded_data.shape[1]}\n"

```

```

        f"Количество строк: {loaded_data.shape[0]}\n"
        f"Заголовки столбцов: {list(loaded_data.columns)}",
    )

    if loaded_data.shape[1] < 2:
        raise ValueError(
            "В файле должно быть как минимум два столбца: расстояние и
уровень сигнала."
        )

        messagebox.showinfo("Успех", "Данные успешно загружены!")
    except Exception as e:
        messagebox.showerror("Ошибка", f"Ошибка при загрузке данных: {e}")

def calculate_signal_level():
    if not validate_inputs():
        return

    # Получение значений из полей ввода
    frequency = float(entry_frequency.get())
    bs_antenna_height = float(entry_bs_height.get())
    ms_antenna_height = float(entry_ms_height.get())
    rx_gain = float(entry_rx_gain.get())
    tx_gain = float(entry_tx_gain.get())
    distance = float(entry_distance.get())
    terrain_type = combo_terrain.get()

    # Получение выбранных моделей
    selected_models = []

```

```

if okumura_var.get():
    selected_models.append("Окамура")
if hata_var.get():
    selected_models.append("Хата")
if cost_hata_var.get():
    selected_models.append("COST-231-Хата")
if lee_var.get():
    selected_models.append("Ли")

# Построение графика зависимости уровня сигнала от расстояния
plot_signal_graph(
    frequency,
    bs_antenna_height,
    ms_antenna_height,
    rx_gain,
    tx_gain,
    distance,
    selected_models,
    terrain_type,
)

```

```

# Расчёт среднеарифметического диапазона значений уровня сигнала
загружаемых данных

```

```

avg_loaded_signal = None
if loaded_data is not None:
    try:
        if loaded_data.shape[1] >= 2:
            avg_loaded_signal = np.mean(loaded_data.iloc[:, 1])
    except Exception as e:

```

```

messagebox.showerror(
    "Ошибка", f"Ошибка при обработке загруженных данных: {e}"
)

```

```

def okumura_model(
    frequency, bs_antenna_height, ms_antenna_height, distance, terrain_type
):
    f_MHz = frequency
    h_bs = bs_antenna_height
    h_ms = ms_antenna_height
    R_km = distance

    if terrain_type == "Городская":
        if f_MHz >= 400:
            alpha_hms = 3.2 * (np.log10(11.75 * h_ms)) ** 2 - 4.97
        else:
            alpha_hms = 8.29 * (np.log10(1.54 * h_ms)) ** 2 - 1.1
    else:
        alpha_hms = (1.1 * np.log10(f_MHz) - 0.7) * h_ms - (
            1.56 * np.log10(f_MHz) - 0.8
        )

    A = 59 + 26.16 * np.log10(f_MHz) - 13.82 * np.log10(h_bs) - alpha_hms
    B = 34.9 - 6.55 * np.log10(h_bs)

    if terrain_type == "Пригородная":
        C = 2 * (np.log10(f_MHz / 28)) ** 2 + 5.4
        a_MH = A + B * np.log10(R_km) - C

```

```

elif terrain_type == "Открытая":
    D = 4.78 * (np.log10(f_MHz)) ** 2 - 18.33 * np.log10(f_MHz) + 40.94
    a_MH = A + B * np.log10(R_km) - D
else: # Городская
    a_MH = A + B * np.log10(R_km)

P_M = 10 # Примерное значение уровня мощности передатчика
P_R = P_M - a_MH

return P_R

```

```

def hata_model_COST_231(
    frequency, bs_antenna_height, ms_antenna_height, distance, terrain_type
):
    f_MHz = frequency
    h_bs = bs_antenna_height
    h_ms = ms_antenna_height
    R_km = distance

    if terrain_type == "Городская":
        if f_MHz >= 400:
            alpha_hms = 3.2 * (np.log10(11.75 * h_ms)) ** 2 - 4.97
        else:
            alpha_hms = 8.29 * (np.log10(1.54 * h_ms)) ** 2 - 1.1
    else:
        alpha_hms = (1.1 * np.log10(f_MHz) - 0.7) * h_ms - (
            1.56 * np.log10(f_MHz) - 0.8
        )

```

$A = 75.55 + 26.16 * \text{np.log10}(f_MHz) - 13.82 * \text{np.log10}(h_bs) - \text{alpha_hms}$

$B = 54.9 - 6.55 * \text{np.log10}(h_bs)$

if terrain_type == "Пригородная":

$C = 2 * (\text{np.log10}(f_MHz / 28)) ** 2 + 5.4$

$a_MH = A + B * \text{np.log10}(R_km) - C$

elif terrain_type == "Открытая":

$D = 4.78 * (\text{np.log10}(f_MHz)) ** 2 - 18.33 * \text{np.log10}(f_MHz) + 40.94$

$a_MH = A + B * \text{np.log10}(R_km) - D$

else: # Городская

$a_MH = A + B * \text{np.log10}(R_km)$

$P_M = 10$ # Примерное значение уровня мощности передатчика

$P_R = P_M - a_MH$

return P_R

def hata_model(frequency, bs_antenna_height, ms_antenna_height, distance, terrain_type):

$f_MHz = frequency$

$h_bs = bs_antenna_height$

$h_ms = ms_antenna_height$

$R_km = distance$

if terrain_type == "Городская":

if $f_MHz \geq 400$:

$\text{alpha_hms} = 3.2 * (\text{np.log10}(11.75 * h_ms)) ** 2 - 4.97$

else:

$\text{alpha_hms} = 8.29 * (\text{np.log10}(1.54 * h_ms)) ** 2 - 1.1$

else:

```
alpha_hms = (1.1 * np.log10(f_MHz) - 0.7) * h_ms - (  
    1.56 * np.log10(f_MHz) - 0.8  
)
```

```
A = 69.55 + 26.16 * np.log10(f_MHz) - 13.82 * np.log10(h_bs) - alpha_hms
```

```
B = 44.9 - 6.55 * np.log10(h_bs)
```

```
if terrain_type == "Пригородная":
```

```
    C = 2 * (np.log10(f_MHz / 28)) ** 2 + 5.4
```

```
    a_MH = A + B * np.log10(R_km) - C
```

```
elif terrain_type == "Открытая":
```

```
    D = 4.78 * (np.log10(f_MHz)) ** 2 - 18.33 * np.log10(f_MHz) + 40.94
```

```
    a_MH = A + B * np.log10(R_km) - D
```

```
else: # Городская
```

```
    a_MH = A + B * np.log10(R_km)
```

```
P_M = 10 # Примерное значение уровня мощности передатчика
```

```
P_R = P_M - a_MH
```

```
return P_R
```

```
def lee_model(frequency, bs_antenna_height, ms_antenna_height, distance,  
terrain_type):
```

```
    if terrain_type == "Городская":
```

```
        p1 = -70
```

```
        gamma = 36.8
```

```
    elif terrain_type == "Пригородная":
```

```
        p1 = -61.7
```

```

    gamma = 38.4
elif terrain_type == "Открытая":
    p1 = -49
    gamma = 43.5
else: # Холмистая
    p1 = -60
    gamma = 40

P_C = p1 - gamma * np.log10(distance)

return P_C

# Функция построения графика

def plot_signal_graph(
    frequency,
    bs_antenna_height,
    ms_antenna_height,
    rx_gain,
    tx_gain,
    max_distance,
    selected_models,
    terrain_type,
):
    # Очистка предыдущего графика
    for widget in graph_frame.wininfo_children():
        widget.destroy()

    if not selected_models:

```

```

empty_label = tk.Label(
    graph_frame, text="Выберите хотя бы одну модель для построения
графика."
)
empty_label.pack(pady=200)
return

# Создание данных для графика
distances = np.linspace(0.1, max_distance, 100)
signal_levels = {}

# Расчёт уровня сигнала для каждой модели
for model in selected_models:
    if model == "Окамура":
        signal_levels[model] = [
            okumura_model(
                frequency, bs_antenna_height, ms_antenna_height, d, terrain_type
            )
            for d in distances
        ]
    elif model == "Хата":
        signal_levels[model] = [
            hata_model(
                frequency, bs_antenna_height, ms_antenna_height, d, terrain_type
            )
            for d in distances
        ]
    elif model == "COST-231-Хата":
        signal_levels[model] = [
            hata_model_COST_231(

```

```

        frequency, bs_antenna_height, ms_antenna_height, d, terrain_type
    )
    for d in distances
]
elif model == "Ли":
    signal_levels[model] = [
        lee_model(
            frequency, bs_antenna_height, ms_antenna_height, d, terrain_type
        )
        for d in distances
    ]

# Создание графика
fig, ax = plt.subplots(figsize=(15, 9))

# Установка фиксированных пределов для осей
ax.set_xlim(0, max_distance)
ax.set_ylim(-220, 0) # Примерные пределы для уровня сигнала в дБ

# Построение графиков для каждой модели
for model in selected_models:
    ax.plot(distances, signal_levels[model], label=model)

# Отображение загруженных данных, если они есть
if loaded_data is not None:
    try:
        if loaded_data.shape[1] >= 2:
            ax.plot(
                loaded_data.iloc[:, 0],
                loaded_data.iloc[:, 1],

```

```

        label="Загруженные данные",
        linestyle="--",
        marker="o",
    )
except Exception as e:
    messagebox.showerror(
        "Ошибка", f"Ошибка при отображении загруженных данных: {e}"
    )

# Добавление легенды
ax.legend(loc="upper right")

# Добавление сетки
ax.grid(True, linestyle="--", alpha=0.7)

# Подписи осей
ax.set_xlabel("Расстояние (км)")
ax.set_ylabel("Уровень сигнала (дБ)")
ax.set_title("Зависимость уровня сигнала от расстояния")

# Отображение графика в окне tkinter
canvas = FigureCanvasTkAgg(fig, master=graph_frame)
canvas.draw()
canvas.get_tk_widget().pack(side=tk.TOP, fill=tk.BOTH, expand=True)

def update_graph_axes():
    # Очистка предыдущего графика
    for widget in graph_frame.winfo_children():
        widget.destroy()

```

```

# Создание пустого графика с осями
fig, ax = plt.subplots(figsize=(6, 4))
ax.set_xlabel("Расстояние (км)")
ax.set_ylabel("Уровень сигнала (дБ)")
ax.set_title("Зависимость уровня сигнала от расстояния")
ax.grid(True)

# Отображение пустого графика в окне tkinter
canvas = FigureCanvasTkAgg(fig, master=graph_frame)
canvas.draw()
canvas.get_tk_widget().pack(side=tk.TOP, fill=tk.BOTH, expand=True)

def calculate_rmse(model_signal, loaded_signal):
    """Рассчитывает среднеквадратическое отклонение (RMSE) между двумя
    массивами."""
    if len(model_signal) != len(loaded_signal):
        raise ValueError("Длины массивов не совпадают.")
    return np.sqrt(np.mean((np.array(model_signal) - np.array(loaded_signal)) ** 2))

def calculate_accuracy_from_rmse(rmse, loaded_signal):
    """Рассчитывает точность в процентах на основе RMSE и диапазона
    данных."""
    max_signal = np.max(loaded_signal)
    min_signal = np.min(loaded_signal)
    signal_range = max_signal - min_signal

    # Избегаем деления на ноль

```

```

if signal_range == 0:
    return 100.0 # Если все значения одинаковы, точность 100%

# Точность в процентах
accuracy = (1 - (rmse / signal_range)) * 100
return max(0, min(100, accuracy)) # Ограничиваем от 0% до 100%

def generate_report():
    if not validate_inputs():
        return

    # Получение значений из полей ввода
    frequency = float(entry_frequency.get())
    bs_antenna_height = float(entry_bs_height.get())
    ms_antenna_height = float(entry_ms_height.get())
    rx_gain = float(entry_rx_gain.get())
    tx_gain = float(entry_tx_gain.get())
    distance = float(entry_distance.get())
    terrain_type = combo_terrain.get()

    # Получение выбранных моделей
    selected_models = []
    if okumura_var.get():
        selected_models.append("Окамура")
    if hata_var.get():
        selected_models.append("Хата")
    if cost_hata_var.get():
        selected_models.append("COST-231-Хата")
    if lee_var.get():

```

```

selected_models.append("Ли")

if not selected_models:
    messagebox.showerror("Ошибка", "Выберите хотя бы одну модель для
отчёта.")
    return

if loaded_data is None or loaded_data.shape[1] < 2:
    messagebox.showerror("Ошибка", "Загрузите данные для расчёта
точности.")
    return

# Извлечение расстояний и уровней сигнала из загруженных данных
try:
    loaded_distances = loaded_data.iloc[:, 0].values
    loaded_signal = loaded_data.iloc[:, 1].values
except Exception as e:
    messagebox.showerror("Ошибка", f"Ошибка при извлечении данных: {e}")
    return

# Расчёт RMSE и точности для каждой модели
rmse_results = {}
accuracy_results = {}
for model in selected_models:
    model_signal = []
    for d in loaded_distances:
        if model == "Окамура":
            model_signal.append(okumura_model(frequency, bs_antenna_height,
ms_antenna_height, d, terrain_type))
        elif model == "Хата":

```

```

        model_signal.append(hata_model(frequency, bs_antenna_height,
ms_antenna_height, d, terrain_type))
    elif model == "COST-231-Хата":
        model_signal.append(hata_model_COST_231(frequency,
bs_antenna_height, ms_antenna_height, d, terrain_type))
    elif model == "Ли":
        model_signal.append(lee_model(frequency, bs_antenna_height,
ms_antenna_height, d, terrain_type))

    rmse_results[model] = calculate_rmse(model_signal, loaded_signal)
    accuracy_results[model] = calculate_accuracy_from_rmse(rmse_results[model],
loaded_signal)

    tx_power = float(entry_tx_power.get())

# Формирование текста отчёта
report_text = "Результаты\n\n"
report_text += f"Параметры:\n"
report_text += f"Частота: {frequency} МГц\n"
report_text += f"Мощность передатчика: {tx_power} дБм\n"
report_text += f"Высота антенны БС: {bs_antenna_height} м\n"
report_text += f"Высота антенны АС: {ms_antenna_height} м\n"
report_text += f"Коэффициент усиления принимающей антенны: {rx_gain}
дБ\n"
report_text += f"Коэффициент усиления передающей антенны: {tx_gain} дБ\n"
report_text += f"Тип местности: {terrain_type}\n\n"

report_text += "Среднеквадратическое отклонение (СКО) уровня сигнала:\n"
for model in rmse_results:
    report_text += f"{model}: {rmse_results[model]:.2f} дБ\n"

report_text += "\nТочность моделей (на основе СКО, %):\n"

```

```

for model in accuracy_results:
    report_text += f"{model}: {accuracy_results[model]:.2f}%\n"

# Сохранение отчёта в DOCX
try:
    doc = Document()
    doc.add_paragraph(report_text)
    doc.save("Результаты.docx")
    messagebox.showinfo("Отчёт", "Отчёт успешно сформирован и сохранён в
файл 'Результаты.docx'.")
except Exception as e:
    messagebox.showerror("Ошибка", f"Ошибка при сохранении отчёта: {e}")

# Создание главного окна
root = tk.Tk()
root.title("Прогнозирование уровня сигнала")

# Поля ввода
tk.Label(root, text="Частота (МГц):").grid(row=0, column=0, padx=10, pady=5,
sticky="w")
entry_frequency = tk.Entry(root)
entry_frequency.grid(row=0, column=1, padx=10, pady=5)
entry_frequency.insert(0, "900")

tk.Label(root, text="Высота антенны БС (м):").grid(
    row=1, column=0, padx=10, pady=5, sticky="w"
)
entry_bs_height = tk.Entry(root)

```

```
entry_bs_height.grid(row=1, column=1, padx=10, pady=5)
entry_bs_height.insert(0, "30")
```

```
tk.Label(root, text="Высота антенны АС (м):").grid(
    row=2, column=0, padx=10, pady=5, sticky="w"
)
```

```
entry_ms_height = tk.Entry(root)
entry_ms_height.grid(row=2, column=1, padx=10, pady=5)
entry_ms_height.insert(0, "1.5")
```

```
tk.Label(root, text="Коэффициент усиления принимающей антенны (дБ):").grid(
    row=3, column=0, padx=10, pady=5, sticky="w"
)
```

```
entry_rx_gain = tk.Entry(root)
entry_rx_gain.grid(row=3, column=1, padx=10, pady=5)
entry_rx_gain.insert(0, "0")
```

```
tk.Label(root, text="Коэффициент усиления передающей антенны (дБ):").grid(
    row=4, column=0, padx=10, pady=5, sticky="w"
)
```

```
entry_tx_gain = tk.Entry(root)
entry_tx_gain.grid(row=4, column=1, padx=10, pady=5)
entry_tx_gain.insert(0, "6")
```

```
tk.Label(root, text="Расстояние от БС к АС (км):").grid(
    row=5, column=0, padx=10, pady=5, sticky="w"
)
```

```
entry_distance = tk.Entry(root)
entry_distance.grid(row=5, column=1, padx=10, pady=5)
entry_distance.insert(0, "10")
```

```

tk.Label(root, text="Мощность передатчика (дБм):").grid(row=6, column=0,
padx=10, pady=5, sticky="w")
entry_tx_power = tk.Entry(root)
entry_tx_power.grid(row=6, column=1, padx=10, pady=5)
entry_tx_power.insert(0, "30") # Значение по умолчанию

# Выпадающий список для типа местности
tk.Label(root, text="Тип местности:").grid(row=7, column=0, padx=10, pady=5,
sticky="w")
terrain_types = ["Городская", "Пригородная", "Открытая", "Холмистая",
"Горная"]
combo_terrain = ttk.Combobox(root, values=terrain_types)
combo_terrain.grid(row=7, column=1, padx=10, pady=5)
combo_terrain.set("Городская")

# Чекбоксы для выбора моделей
tk.Label(root, text="Выберите модели для построения графика:").grid(
    row=8, column=0, padx=10, pady=5, sticky="w"
)

okumura_var = tk.BooleanVar(value=True)
okumura_check = tk.Checkbutton(root, text="Окамура", variable=okumura_var)
okumura_check.grid(row=9, column=0, padx=10, pady=2, sticky="w")

hata_var = tk.BooleanVar(value=True)
hata_check = tk.Checkbutton(root, text="Хата", variable=hata_var)
hata_check.grid(row=10, column=0, padx=10, pady=2, sticky="w")

cost_hata_var = tk.BooleanVar(value=True)

```

```

cost_hata_check = tk.Checkbutton(root, text="COST-231-Хата",
variable=cost_hata_var)
cost_hata_check.grid(row=11, column=0, padx=10, pady=2, sticky="w")

lee_var = tk.BooleanVar(value=True)
lee_check = tk.Checkbutton(root, text="Ли", variable=lee_var)
lee_check.grid(row=12, column=0, padx=10, pady=2, sticky="w")

# Кнопка загрузки данных
load_data_button = tk.Button(root, text="Загрузить данные", command=load_data)
load_data_button.grid(row=13, column=0, columnspan=2, pady=5)

# Кнопка для расчета
calculate_button = tk.Button(
    root, text="Рассчитать и построить график", command=calculate_signal_level
)
calculate_button.grid(row=14, column=0, columnspan=2, pady=5)

# Кнопка для формирования отчёта
generate_report_button = tk.Button(
    root, text="Сформировать отчёт", command=generate_report
)
generate_report_button.grid(row=15, column=0, columnspan=2, pady=5)

# Фрейм для графика (справа)
graph_frame = tk.Frame(
    root, width=500, height=400, bg="#f0f0f0", relief=tk.GROOVE, borderwidth=3
)
graph_frame.grid(row=0, column=2, rowspan=15, padx=10, pady=5, sticky="nsew")
graph_frame.grid_propagate(False)

```

```
# Инициализация пустого графика с осями  
update_graph_axes()
```

```
# Запуск главного цикла  
root.mainloop()
```