

**Проект «Фрактал»:
децентрализованная сеть
обнаружения и поражения
беспилотных летательных
аппаратов (БПЛА)**

Лэй Энстазия

Лэй Энстазия
Проект «Фрактал»:
децентрализованная
сеть обнаружения и
поражения беспилотных
летательных аппаратов (БПЛА)

<https://litres.ru/74418638>

SelfPub; 2026

Аннотация

Беспилотники изменили правила войны. Дешёвые, автономные и почти незаметные, они делают традиционные системы ПВО беспомощными. Проект «Фрактал» — это новый подход к противодроновой обороне. Вместо дорогих радаров и ракет — децентрализованная самоорганизующаяся сеть из сотен дешёвых сенсорных узлов. Каждый узел оснащён нейронным процессором, который анализирует звук, радиолокационные сигналы и радиоизлучение в реальном времени, отличая дрон от птицы или облака. Сеть не имеет единого центра — она живуча и самовосстанавливается при любых потерях. Мобильные огневые группы (МОГ) замыкают полный цикл «обнаружение — решение — поражение» без участия человека. Экономика проекта в

десятки раз эффективнее классических систем. Книга подробно описывает архитектуру, сенсорную фузию, алгоритмы, тактику и перспективы развития. Это не просто техническое решение — это философия обороны будущего, где победа достигается интеллектом, а не стоимостью.

Содержание

Введение	5
Глава 1. Беспилотная революция 2020х	16
Глава 2. Ахиллесова пята классических систем	22
Глава 3. «Молчаливые» дроны — самый сложный сценарий	30
Глава 4. Почему одного радара недостаточно	38
Глава 5. Акустический слух — микрофонные решётки	44
Глава 6. Радиочастотный детектор — «перехватчик» радиоголосов	53
Глава 7. Тепловизор — зрение в темноте	65
Глава 8. Сенсорная фузия на практике	74
Глава 9. От облака к периферии — почему задержка недопустима	82
Глава 10. Нейронный процессор (NPU) как основа каждого узла	89
Глава 11. Локальное принятие решений	99
Конец ознакомительного фрагмента.	101

Лэй Энстазия Проект «Фрактал»: децентрализованная сеть обнаружения и поражения беспилотных летательных аппаратов (БПЛА)

Введение

Новая реальность воздушного пространства

Они не издают звука, который можно было бы услышать за километры. Они не оставляют теплового следа, который нельзя было бы спутать с птицей. Они не отражают радиоволны так, как отражал бы металлический бомбардировщик. Они просто есть — маленькие, быстрые, почти незаметные — и они меняют всё.

Беспилотные летательные аппараты стали не просто новой категорией вооружения. Они стали новой реальностью воздушного пространства — реальностью, к которой традиционные системы противовоздушной обороны оказались не

готовы. И проблема здесь не в техническом несовершенстве. Проблема глубже: она лежит в самой философии защиты, которую эти системы воплощают.

Мы стоим на пороге нового этапа в истории противовоздушной обороны. Угрозы изменились — и средства защиты должны измениться вместе с ними. Эта книга — о том, как один проект отвечает на этот вызов.

Три фундаментальных разрыва

Чтобы понять, почему традиционные системы ПВО терпят поражение в войне дронов, нужно увидеть три структурных разрыва, которые делают их уязвимыми.

Первый разрыв — экономический. Стоимость перехвата одной воздушной цели с помощью традиционных средств может в десятки, а то и в сотни раз превышать стоимость самого средства нападения. Зенитная ракета для комплекса Patriot оценивается в 3–6 миллионов долларов. А дрон, который она сбивает, может стоить от нескольких сотен до нескольких десятков тысяч долларов. Это не просто дорого. Это экономически неустойчиво. Когда защитник вынужден тратить ресурс, который стоит в 30, 100 или 150 раз дороже цели, атакующий выигрывает войну на истощение ещё до того, как нанесён первый урон.

Второй разрыв — структурный. Традиционные системы ПВО построены по централизованному принципу: один дорогой радар на возвышенности, один командный центр, одна точка принятия решений. Информация стекается в один

пункт, а решения исходят из одного источника. Это создаёт единую точку отказа: повредите командный центр или нарушьте связь с ним — и система перестаёт работать. Иерархия создаёт задержки — а в мире, где дрон пролетает километр за десять секунд, каждая секунда задержки может стать фатальной.

Третий разрыв — сенсорный. Современные автономные дроны способны действовать без радиосигнала. Они наводятся на цель по встроенной оптике и заранее загруженным базам данных. Они не излучают — они не «говорят». А это значит, что радиочастотные детекторы, которые традиционно используются для идентификации и пеленгации, становятся бесполезными. Традиционная система, лишённая одного из своих ключевых сенсоров, теряет способность классифицировать цель. Оператору приходится выбирать между риском ложной тревоги и риском пропущенной угрозы. И в этой дилемме система проигрывает.

Именно эти три разрыва — экономический, структурный и сенсорный — делают традиционную ПВО уязвимой перед новой угрозой. Именно эти три принципа должны быть пересмотрены.

Новая философия: три столпа проекта «Фрактал»

Проект «Фрактал» — это ответ на структурный вызов. Он предлагает не модернизацию старых систем, а смену парадигмы. Вместо централизации — децентрализация. Вместо дороговизны — массовость. Вместо иерархии — самоорга-

низация.

Массовость. Один дорогой радар не может увидеть сотню дронов одновременно. Одна зенитная ракета не может сбить рой. Оборона должна стать такой же массовой, как и атака. Это означает множество дешёвых сенсоров вместо одного дорогого. Это означает сеть, а не точку. Это означает, что стоимость узла обнаружения должна быть сопоставима со стоимостью атакующего дрона, чтобы защитник мог развернуть систему в масштабе, адекватном угрозе.

Децентрализация. Вместо единого командного центра — самоорганизующаяся mesh-сеть, где каждый узел является и приёмником, и передатчиком, и маршрутизатором. Вместо иерархии «командир отдаёт приказ — подчинённый выполняет» — фрактальная структура, где один и тот же принцип организации повторяется на любом масштабе: от отдельного датчика до стратегического уровня. Если один узел выходит из строя, остальные автоматически перенастраивают маршруты. Сеть самовосстанавливается, как живой организм.

Интеллект на границе. Вместо отправки всех данных в облако или на мощный сервер — обработка непосредственно на месте съёма данных. Нейронные процессоры на каждом узле анализируют спектрограммы звука, радарные сигналы и радиочастотные профили в реальном времени. Они принимают решения за миллисекунды, без участия человека и без задержек на передачу данных. Они отличают шум винтов дрона от шума автомобильного двигателя. Они распознают

микродоплеровский профиль вращающегося пропеллера — и отличают его от машущего крыла птицы. Они делают это с минимальным энергопотреблением — так, что каждый узел может работать автономно часами или даже сутками.

От теории к практике: архитектура системы

Проект «Фрактал» — это не просто концепция. Это детально проработанная архитектура, которая охватывает все уровни противодроновой обороны: от сенсоров до средств поражения, от отдельного узла до стратегического командования.

В основе системы лежит сенсорная фузия — слияние данных от четырёх типов датчиков:

- Радар миллиметрового диапазона обеспечивает дальнейшее обнаружение, точное измерение координат и скорости, а также микродоплеровский анализ для первичной классификации.

- Акустическая решётка из MEMS-микрофонов в тетраэдрической конфигурации обеспечивает трёхмерную пеленгацию и точную классификацию по спектральному портрету винтов.

- Пассивный RF-детектор перехватывает сигналы управления и телеметрии, идентифицируя тип дрона и его «почерк».

- Тепловизор (устанавливаемый только на командных узлах) обеспечивает финальную верификацию цели в сложных погодных условиях и в тёмное время суток.

Каждый из этих сенсоров по отдельности уязвим. Но вместе они образуют систему, которая перекрывает слабые места друг друга. Именно этот принцип — сенсорная фузия — превращает разрозненные датчики в единый «организм», способный видеть там, где радары слепы; слышать там, где акустика бессильна; и понимать там, где алгоритмы прошлого поколения сдаются.

Обработка данных происходит на нейронных процессорах (NPU), установленных на каждом узле. NPU анализирует не «сырые» сигналы, а спектрограммы — визуальные представления сигналов в частотно-временной плоскости. Это позволяет снизить вычислительную нагрузку в десятки раз и работать с минимальным энергопотреблением. Каждый узел самостоятельно решает, что именно он видит и слышит, и передаёт в сеть не терабайты «сырых» данных, а сжатые треки — координаты, тип, уровень доверия.

Протокол трек-верификации обеспечивает коллективное подтверждение целей. Когда один узел обнаруживает потенциальный объект, он запрашивает подтверждение у соседей. Только когда три узла независимо подтверждают одну и ту же цель в одном секторе, она считается реальной. Этот механизм отсекает ложные тревоги — птиц, облака, метеоявления — с эффективностью, недостижимой для любой одиночной системы.

Гетерогенная архитектура распределяет ресурсы оптимально: дешёвые сенсорные узлы («бойцы») обеспечивают

массовое покрытие, а один дорогой командный узел (МОГ — мобильная огневая группа) с тепловизором и средствами поражения обеспечивает верификацию и принятие решений. Один командир на десять бойцов — это не компромисс, а экономическая эффективность, позволяющая развернуть систему в десятки раз дешевле традиционных аналогов.

Фрактальная иерархия делает систему масштабируемой до любого размера. Один и тот же паттерн повторяется на всех уровнях: «Боец» «Командир» (МОГ) «Команда» (стратегический штаб). Каждый уровень является «бойцом» для вышестоящего и «командиром» для нижестоящего. Информация движется снизу вверх — от сырых треков к верифицированным тактическим данным и стратегической картине. Команды движутся сверху вниз — целеуказания, приоритеты, обновлённые модели для NPU.

Mesh-сеть объединяет все узлы в единую самоорганизующуюся систему. Каждый узел является одновременно и приёмником, и маршрутизатором. Если один узел выходит из строя, сеть автоматически перенастраивает маршруты за миллисекунды. Протоколы самоорганизации (AODV, NeoMesh) обеспечивают непрерывную работу даже при частичных потерях.

Мобильные огневые группы на базе пикапов или броневых автомобилей замыкают на себе полный цикл «обнаружение — решение — поражение». Они автономны, не зависят от внешних сетей и способны действовать даже при полной по-

тере связи со штабом. Их подвижность позволяет выдвигаться на маршруты пролёта дронов, создавая мобильные заслоны там, где стационарные средства бессильны.

Почему эта книга — не просто техническое описание

Эта книга — не просто сборник технических спецификаций и алгоритмов. Это попытка показать, как рождается новая парадигма обороны. Парадигма, где победа достигается не мощностью, а умом; не ценой, а архитектурой; не централизацией, а распределением.

Мы живём в эпоху, когда новая парадигма войны — комбинация роботизации, ИИ-автономии и межсетевой интеграции — размывает традиционные преимущества крупных держав. Её главный вызов — низкая стоимость. И ответом на этот вызов может быть только симметричный по своей философии подход: дешёвый, умный, децентрализованный.

Проект «Фрактал» — это именно такой ответ. Он не пытается «догнать» угрозу, создавая всё более дорогие и сложные системы. Он меняет саму логику обороны. Вместо крепости — сеть. Вместо генерала — коллективный разум. Вместо одного всевидящего ока — тысячи глаз, которые видят больше, чем одно око, потому что они видят с разных точек и думают вместе.

О структуре книги

Книга построена так, чтобы провести читателя через все уровни системы — от философии до практической реализа-

ции.

Часть I (главы 1–3) раскрывает проблему: эволюцию беспилотных угроз, уязвимости традиционных систем и появление «молчаливых» дронов как самого сложного сценария.

Часть II (главы 4–8) посвящена сенсорной фузии — четырём «чувствам» системы: радару, акустике, RF-детектору и тепловизору, а также тому, как их объединение создаёт целостную картину воздушной обстановки.

Часть III (главы 9–11) рассказывает об «интеллекте на границе» — нейронных процессорах, локальном принятии решений и том, почему обработка на месте, а не в облаке, является единственным способом выжить в войне дронов.

Часть IV (главы 12–14) описывает децентрализованную самоорганизующуюся сеть: mesh-протоколы, трек-верификацию и гетерогенную архитектуру.

Часть V (главы 15–17) посвящена мобильным огневым группам — центрам боевого управления и поражения, их тактической автономности и эстафете перехвата.

Часть VI (главы 18–21) раскрывает фрактальную самоорганизацию — систему «матрешку», где один паттерн повторяется на всех уровнях, а самовосстановление делает сеть практически неуничтожимой.

Часть VII (главы 22–29) погружается в аппаратную архитектуру: от MCU и NPU до радаров, микрофонов, RF-детекторов, тепловизоров, mesh-радио и энергетических решений.

Часть VIII (главы 30–32) переходит к тактике применения — развёртыванию на объекте, отработке типовых угроз и взаимодействию с другими средствами ПВО.

Часть IX (главы 33–35) рассматривает экономику, масштабирование и внедрение — сравнение стоимости с традиционными решениями, этапы развёртывания и цикл постоянного обновления моделей.

Часть X (главы 36–38) заглядывает в будущее: федеративное обучение, прогнозирование маршрутов роёв, интеграция с РЭБ и роботизация поражения.

Заключение подводит философский итог: победа в войне дронов — это победа интеллекта, децентрализации и экономической эффективности.

Приложения содержат технические спецификации, глоссарий, примеры расчётов и ссылки на открытые стандарты.

Для кого эта книга

Эта книга адресована широкому кругу читателей: военным специалистам, инженерам, разработчикам систем ПВО, исследователям в области искусственного интеллекта и сенсорных систем, а также всем, кто интересуется будущим войны и технологий.

Она написана так, чтобы быть понятной как для профессионалов, так и для читателей без глубокой технической подготовки. Математические формулы и инженерные детали вынесены в отдельные разделы, а основное повествование сосредоточено на логике, архитектуре и философии систе-

мы.

Вместо предисловия

Мы живём в эпоху, когда угрозы радикально изменились. Традиционные системы ПВО, созданные для войны, которой больше нет, не могут защитить нас от роёв дешёвых, автономных, малозаметных дронов. Нам нужна новая парадигма.

Проект «Фрактал» предлагает эту парадигму. Это не просто система обнаружения и поражения. Это философия обороны, где интеллект распределён, стоимость минимальна, а живучесть заложена в самой архитектуре. Это подход, где побеждает не тот, у кого больше ракет, а тот, у кого быстрее и точнее работают «глаза» и «уши».

Эта книга — приглашение к диалогу о том, как должна выглядеть оборона будущего. Она не претендует на истину в последней инстанции, но предлагает одно из возможных решений — решение, основанное на логике, физике и экономике.

Добро пожаловать в мир проекта «Фрактал».

Глава 1. Беспилотная революция 2020х

От разведывательных БПЛА к роям-камикадзе

В начале 2020х годов беспилотные летательные аппараты прочно ассоциировались с наблюдением. Они зависали над полем боя, передавали видео, корректировали огонь, но сами оставались уязвимыми и сравнительно дорогими инструментами. Их ценность измерялась качеством оптики и дальностью радиоканала. Потеря такого аппарата была ощутимой — не столько из-за стоимости, сколько из-за потери разведывательных возможностей.

Этот образ рухнул в течение нескольких лет. Технологический рывок в миниатюризации моторов, аккумуляторов, навигационных чипов и вычислительных модулей сделал возможным то, о чём раньше говорили лишь футурологи: беспилотник превратился из глаза в меч. И, что важнее, в расходный меч.

К середине десятилетия дроны перестали быть штучным товаром. Их производство встало на конвейер, а стоимость одного боеспособного аппарата упала до уровня, сопоставимого с ценой дорогого смартфона. Это изменило саму экономику вооружённого противостояния. Если раньше потеря средства поражения требовала значительных ресурсов, то

теперь противник мог позволить себе отправлять в небо десятки и сотни аппаратов за один вылет, не считая их однократными.

Ключевой прорыв произошёл в области автономности. Первые ударные дроны ещё требовали оператора — человека, который вёл аппарат по видеоканалу и в финальный момент наводил на цель. Но уже к 2025 году широкое распространение получили системы, способные распознавать объекты по встроенным базам данных, самостоятельно выбирать траекторию полёта и атаковать без участия внешнего управления. Это стало возможным благодаря внедрению нейросетевых ускорителей непосредственно на борту — чипов, которые выполняли модели машинного зрения с минимальным энергопотреблением.

Автономный дрон — это принципиально иная угроза. Он не нуждается в радиоканале, его невозможно заглушить средствами радиоэлектронной борьбы. Он не передаёт телеметрию, его нельзя запеленговать. Он просто следует по заранее рассчитанному маршруту, ориентируясь на показания инерциальной навигационной системы, а на финальном отрезке — на изображение с камеры, сопоставляемое с эталоном. Такой аппарат становится «глухим» к внешним помехам и крайне сложным для обнаружения традиционными средствами.

Параллельно с автономией развивалась концепция роевого взаимодействия. Если одиночный дрон — это игла, то рой

— это град. Десятки аппаратов, запущенные с разных точек, могут координировать свои действия через локальную сеть, обмениваться данными о целях, перераспределять задачи и атаковать с нескольких направлений одновременно. Это не просто увеличение количества — это появление нового качества: система, где отдельные элементы взаимозаменяемы, а общая эффективность выше суммы частей. Рой не имеет «головы», которую можно отрубить; он продолжает действовать, пока в нём остаётся хотя бы несколько активных единиц.

Переход от разведывательных БПЛА к роям-камикадзе — это не просто техническая эволюция. Это изменение самой логики воздушного противостояния. Защита больше не может строиться на отражении единичных, дорогих угроз. Она должна быть готова к одновременному приёму множества дешёвых, малозаметных и интеллектуальных целей, каждая из которых сама по себе не представляет большой ценности, но в совокупности способна перегрузить и разрушить любую централизованную систему обороны.

Тактика массовых налётов и автономных групп

Массовый налёт — это не просто сумма отдельных вылетов. Это тщательно спланированная операция, использующая слабости классической ПВО: ограниченное количество пусковых установок, конечный запас дорогих ракет, время реакции, необходимое для захвата и сопровождения цели. Когда в небе одновременно появляются двадцать, пятьдесят

или сто малых аппаратов, система переходит в режим перегрузки. Она вынуждена выбирать приоритеты — и неизбежно пропускает часть целей.

Тактика строится на принципе «роя-отвлекавателя»: часть дронов выполняет функцию ложных целей, привлекая огонь, в то время как основные ударные группы проходят через образовавшиеся бреши. Учитывая, что различие между ложным и боевым дроном может быть минимальным — часто их конструкция идентична, а различаются лишь полезная нагрузка и программа полёта — система ПВО не может эффективно разделять цели без глубокого анализа.

Другой ключевой элемент — эшелонирование высот и направлений. Аппараты, летящие на предельно малой высоте (менее 10 метров), скрываются от радаров за местными предметами. Те, что идут выше, создают ложные отметки. Одни приближаются с фронтальной стороны, другие заходят с тыла, третьи — фланговыми маршрутами. Рой не имеет единого вектора; он растекается как жидкость, заполняя все доступные подходы.

Особую сложность представляют автономные группы, которые не обмениваются сигналами между собой и не имеют командира. Каждый дрон действует по заранее заложенному алгоритму, но при этом все они следуют единому тактическому замыслу. Такой рой невозможно подавить точечным ударом по узлу связи или пункту управления — их просто нет. Каждый аппарат самодостаточен, и уничтожение поло-

вины группы почти не влияет на боеспособность остальных.

Массовые налёты стали возможны не только из-за удешевления самих дронов, но и благодаря развитию логистики запуска. Стартовые платформы могут быть размещены на транспортных средствах, в контейнерах, на подвижных шасси. Запуск может производиться из любого места, где есть достаточно ровная поверхность. Это делает невозможным заранее определить направление главного удара и сосредоточить там средства обороны.

В таких условиях традиционные системы ПВО, ориентированные на перехват крупных высокоскоростных целей, оказываются беспомощными. Их радары не видят рои на малых высотах, их вычислители не справляются с сотнями одновременно сопровождаемых объектов, а стоимость каждого перехвата делает экономически нецелесообразной защиту от массовых налётов.

Именно здесь возникает главный вызов, на который отвечает проект «Фрактал». Если противник перешёл к тактике дешёвых, автономных, многочисленных атак, то защита должна быть столь же дешёвой, автономной и многочисленной. Она не может зависеть от одного дорогостоящего радара или одного командного центра. Она должна быть распределённой, самоорганизующейся и интеллектуальной на каждом уровне. Она должна видеть то, чего не видят большие радары, слышать то, что не слышат станции РЭБ, и принимать решения быстрее, чем человек может осознать проис-

ходящее.

Беспилотная революция 2020х годов не оставляет выбора: игнорировать её значит обречь себя на неизбежные потери. Проект «Фрактал» предлагает не модернизацию существующих средств, а смену парадигмы — переход от централизованных, дорогих и уязвимых систем к децентрализованным, дешёвым и живучим сетям, где каждый узел одновременно является и чувствительным органом, и мыслящим элементом, способным действовать как часть единого целого и как самостоятельная боевая единица.

Глава 2. Ахиллесова пята классических систем

Радары дальнего действия и их «слепые зоны» у земли

Классические системы противовоздушной обороны рождались в иную эпоху — для перехвата крупных летательных аппаратов, движущихся на большой высоте по предсказуемым траекториям. Их радары — мощные, дорогие, стационарные — были спроектированы для одной задачи: видеть далеко и видеть крупное.

Новый класс угроз — малые беспилотные аппараты — нарушает это уравнение почти по всем статьям.

Современные дроны изготавливаются из композитных и радиопрозрачных материалов, которые плохо отражают радиоволны. Их эффективная поверхность рассеяния на порядки меньше, чем у пилотируемого самолёта. Но главная проблема заключается даже не в этом.

Дроны летят низко — у самой земли, между зданиями, над гребнями холмов, в складках рельефа. В таких условиях радиолокационный луч сталкивается с непреодолимыми препятствиями: здания экранируют сигнал, деревья рассеивают его, холмы создают мёртвые зоны. Радар, который уверенно видит цель на горизонте, слепнет там, где цель пря-

чется за ближайшим поворотом.

Это явление известно как «ближняя слепая зона» — участок пространства в непосредственной близости от радара, который остаётся вне поля его зрения. Для наземных радиолокационных станций эта зона может простирается на несколько километров. Именно в этом радиусе дроны наносят наиболее опасные удары.

Техническая природа этой слепоты двойственна. Во-первых, низколетящие цели оказываются в зоне «земных помех» — отражений сигнала от поверхности, растительности, искусственных сооружений. Радар не может отличить движущийся объект от фона, на котором он находится. Во-вторых, традиционные системы фильтрации, настроенные на отбрасывание «мусора» — птиц, облаков, атмосферных явлений, — часто отбрасывают и дроны как ложные цели.

Специалисты отмечают, что наземные радары, сколь бы совершенными они ни были, имеют фундаментальные ограничения в обнаружении малых дронов в лесистой местности, прибрежных районах и горной местности. Строения, стены и металлические конструкции создают дополнительные препятствия для радиоволн. В результате воздушное пространство над защищаемым объектом остаётся открытым для атак, которые классические системы просто не замечают до последнего момента.

Ирония заключается в том, что чем мощнее и дороже радар, тем более уязвимой становится вся система. Высокоцен-

ная радиолокационная инфраструктура сама является привлекательной целью. Её уничтожение или вывод из строя создаёт операционные «дыры», которые невозможно быстро восполнить.

Высокая стоимость одного перехвата

Допустим, радар всё-таки обнаружил дрон. Что дальше? Традиционное решение — выпустить по нему зенитную ракету. И здесь вступает в силу фундаментальное противоречие, которое можно назвать асимметрией стоимости.

Цифры, известные из открытых источников, рисуют красноречивую картину. Один перехватчик класса «земля-воздух» средней дальности стоит от нескольких сотен тысяч до нескольких миллионов долларов. При этом цель, которую предстоит поразить, — малый беспилотный аппарат — обходится противнику в сумму, на несколько порядков меньшую.

Соотношение затрат может превышать 100:1. В некоторых сценариях перехватчик оказывается дороже цели в сотни раз.

Эта асимметрия создаёт парадоксальную ситуацию: обороняющаяся сторона вынуждена расходовать свои самые дорогие ресурсы для уничтожения самых дешёвых средств противника. Каждый успешный перехват — это тактическая победа, но стратегическое истощение. Запасы перехватчиков ограничены, их производство требует времени и ресурсов. Противник, действующий асимметрично, может просто

«переиграть» оборону в экономической плоскости.

Эта проблема носит не ситуативный, а системный характер. Как отмечают эксперты в области противодроновой обороны, «сбивать дроны стоимостью в десятки тысяч евро ракетами за несколько миллионов — это критическая асимметрия стоимости». Система управления должна принимать решение: запускать дорогой перехватчик или прибегать к более экономичным контрмерам.

Однако в условиях быстротечной атаки времени на принятие такого решения практически нет. Классическая архитектура ПВО часто не оставляет выбора: либо перехват дорогой ракетой, либо пропуск цели.

Уязвимость централизованного управления: единая точка отказа

Традиционная архитектура ПВО построена по иерархическому принципу: множество датчиков собирают данные, которые стекаются в единый командный центр, где принимаются решения. Это похоже на мозг, к которому тянутся нервы со всего тела.

У этой конструкции есть фатальная уязвимость: единая точка отказа. Современные системы ПВО настолько сильно зависят от центральных командных пунктов, радаров и пусковых установок, что нейтрализация одного-единственного элемента может создать операционную «дыру», которая приведёт к пропущенным перехватам, задержкам с оповещением и, в конечном счёте, к поражению защищаемых объектов.

Исследователи в области противовоздушной обороны указывают, что современные силы ПВО «слишком сильно зависят от единых точек отказа, особенно от сенсоров и командных узлов управления». Противнику достаточно нейтрализовать несколько командных пунктов или радаров.

Централизация также порождает проблемы с задержками и зависимостью от каналов связи. Полная централизация концентрирует задержки передачи данных и увеличивает риск отказа каналов связи. В условиях применения средств радиоэлектронной борьбы связь с центром может быть нарушена — и тогда вся система слепнет.

Анализ показывает, что системы ПВО, построенные на принципе количественного насыщения радиолокационными средствами, часто оказываются фрагментированными, чрезмерно централизованными и критически зависимыми от внешней инфраструктуры. При нарушении работы этой инфраструктуры значительная часть средств ПВО может стать небоеспособной или неинтегрированной.

Иерархическая архитектура, столь эффективная в условиях предсказуемой угрозы, оказывается хрупкой перед лицом асимметричных действий. Она создаёт иллюзию контроля, но цена этого контроля — уязвимость, заложенная в самой структуре.

Почему одиночный дорогой сенсор проигрывает множеству дешёвых дронов

Мы подошли к главному противоречию. Классическая си-

стема ПВО строится вокруг небольшого числа очень дорогих сенсоров. Их мало, они статичны, и каждый из них — критический элемент, потеря которого может парализовать всю оборону.

Противник использует прямо противоположную стратегию: множество дешёвых, расходных аппаратов. Эта асимметрия создаёт несколько эффектов, которые делают классические системы уязвимыми.

Первое — насыщение. Даже если дорогой радар видит все цели в рое, система перехвата физически не может обработать их все одновременно. Количество пусковых установок и ракет ограничено. Противник может просто «забить» оборону количеством.

Второе — экономическое истощение. Как мы видели выше, стоимость перехвата одного дешёвого дрона дорогой ракетой делает такую оборону экономически несостоятельной. Противник может позволить себе терять десятки аппаратов; обороняющаяся сторона не может позволить себе сбивать их все.

Третье — уязвимость самого сенсора. Одиночный дорогой радар сам является ценной целью. Его стоимость — многие миллионы. Противник может направить один дешёвый аппарат на уничтожение этого радара. Это одна из самых эффективных инвестиций в военной истории: дешёвые беспилотные аппараты успешно поражают дорогие радиолокационные системы.

Традиционные радары были спроектированы для обнаружения пилотируемых самолётов и ракет, поэтому они отфильтровывают маленькие, медленные, низколетящие объекты как «шум». Этот методологический разрыв — между тем, что система умеет видеть, и тем, что ей нужно видеть, — и есть суть проблемы.

К философии проекта «Фрактал»

Из этих трёх уязвимостей — слепоты у земли, экономической асимметрии и централизации — вырастает необходимость принципиально иной архитектуры.

Проект «Фрактал» предлагает не просто модернизацию существующих систем, а смену парадигмы. Вместо одного дорогого прожектора в тёмном поле — сотня маленьких огоньков, каждый из которых видит немного, но вместе они формируют полную картину. Вместо иерархического «мозга», к которому стекаются нервы, — децентрализованная сеть, где решение принимается коллективно, на месте, без задержек и без единой точки отказа.

Эта философия строится на нескольких ключевых принципах.

Множественность вместо единственности. В сети «Фрактал» нет незаменимых узлов. Потеря любого элемента не нарушает работу системы — остальные автоматически перенастраиваются. Это не просто устойчивость к потерям, а принципиальная неуничтожимость: чтобы парализовать сеть, нужно вывести из строя каждый её узел одновременно.

Распределённый интеллект вместо централизованного. Каждый узел сети оснащён нейронным процессором, способным принимать самостоятельные решения. Данные не отправляются в центр для обработки — они анализируются на месте, в режиме реального времени. Это устраняет задержки и зависимость от каналов связи.

Гетерогенность вместо единообразия. В сети есть «бойцы» — простые и дешёвые сенсорные узлы, и «командиры» — мобильные огневые группы, оснащённые тепловизорами и средствами поражения. Такое распределение ресурсов позволяет покрыть большую территорию при ограниченном бюджете.

Сенсорная фузия вместо одиночного датчика. Четыре типа датчиков — радар, акустика, RF-детектор и тепловизор — работают в единой связке, компенсируя слабости друг друга. Радар видит далеко, но не знает, что именно он видит. Акустика классифицирует тип, но работает на коротких дистанциях. RF-детектор идентифицирует «свой-чужой», но бессилен против молчащих аппаратов. Тепловизор подтверждает цель в сложных условиях, но дорог. Вместе они образуют систему, которая перекрывает все сценарии.

Классические ПВО создавались для войны, которой больше нет. Они дороги, централизованы и слепы на низких высотах. Новые угрозы требуют иного подхода — дешёвого, умного, распределённого. Именно такой подход реализует проект «Фрактал».

Глава 3. «Молчаливые» дроны — самый сложный сценарий

Они летят бесшумно, низко и почти незаметно. Они могут нести взрывчатку, вести разведку или просто нарушать работу аэропортов. Но главная их опасность — в другом. Современные автономные дроны, наводящиеся на цель по встроенной оптике и базе данных, вообще не излучают радиочастотных сигналов. Их невозможно «запеленговать» по радиопередаче. Они просто летят по расчётной траектории, бесшумно приближаясь к объекту.

Этот класс угроз получил в профессиональной среде устойчивое название — «тёмные дроны» (Dark Drones). Их появление стало одним из самых значительных сдвигов в современной войне дронов и поставило перед системами противовоздушной обороны задачи, к которым традиционные подходы оказались не готовы.

Анатомия «молчаливого» дрона: как он видит и куда летит

Чтобы понять, почему «молчаливый» дрон так трудно обнаружить, нужно заглянуть внутрь его навигационной системы. В отличие от обычного БПЛА, который постоянно обменивается данными с пультом управления или спутниками, автономный дрон полагается исключительно на борто-

вые средства.

Визуальная одометрия — ключевая технология, лежащая в основе таких систем. Бортовая камера непрерывно сканирует поверхность земли, а нейросетевой модуль в реальном времени обрабатывает видеопоток и сопоставляет изображение с предварительно загруженной цифровой картой местности — спутниковыми снимками или аэрофотосъёмкой. Этот метод позволяет беспилотнику определять своё местоположение с точностью до метров, не используя ни GPS, ни радиосигналы, ни связь с оператором.

Российские инженеры, например, уже завершили разработку такой системы, названной «марсианской» — по аналогии с вертолётom NASA Ingenuity, который использовал аналогичный принцип на Марсе, где GPS просто не существует. Немецкий стартап SE3 Labs пошёл ещё дальше: их система позволяет дронам ориентироваться в совершенно незнакомой местности без спутниковой навигации, используя только бортовую камеру и инерциальные датчики.

Пассивность — второе ключевое свойство «молчаливых» дронов. Они не излучают ничего. Никаких радиосигналов, никаких запросов к спутникам, никаких телеметрических пакетов. Система OSIRIS, разработанная Delian Alliance, специально проектировалась так, чтобы обеспечить «абсолютную малозаметность и защиту от датчиков обнаружения» именно за счёт отсутствия радиочастотной сигнатуры. А технология NOCTA от ASIO, достигшая девятого уров-

ня технологической готовности (TRL-9), работает исключительно в пассивном режиме, без внешних сигналов и связи, непрерывно вычисляя абсолютное положение дрона.

И наконец, помехоустойчивость. Поскольку «молчаливый» дрон не зависит от спутниковых сигналов и радиоканалов, он практически неуязвим для средств радиоэлектронной борьбы. Его невозможно «ослепить» глушилкой или подменить ему GPS-координаты. В условиях, когда традиционные средства РЭБ превращают небо в зону радиомолчания, такой дрон продолжает выполнять задачу так, как будто ничего не происходит.

Бесполезность RF-пеленгации: почему «тишина» — это оружие

Традиционные системы обнаружения дронов в значительной степени полагаются на радиочастотный анализ. RF-датчики сканируют эфир в поисках сигналов управления, телеметрии или видеотрансляции. Этот подход работал до тех пор, пока дроны были «говорливыми».

Но сегодня ситуация радикально изменилась. Как отмечается в аналитических материалах, «по мере эволюции дронов их радиоканалы становились зашифрованными, более трудными для обнаружения или вовсе устранились. Некоторые автономные дроны теперь работают без какого-либо радиочастотного излучения, что делает традиционные методы обнаружения неэффективными».

RF-датчик в такой ситуации становится бесполезным —

он «слышит» тишину. И это не просто техническая деталь. Это фундаментальный сдвиг в балансе сил.

Представьте себе: дрон, который не излучает ничего, пролетает над охраняемым объектом. RF-детекторы молчат. Средства радиоэлектронной борьбы не могут его подавить — ему нечего подавлять. Операторы системы ПВО не видят его на своих экранах, потому что системы предупреждения настроены на поиск радиосигналов. «Дрон, навигирующий автономно с использованием бортовых камер и датчиков, может вообще не излучать обнаруживаемого сигнала. Это тот пробел, который RF-детекция и системы постановки помех не могут закрыть самостоятельно».

Этот пробел становится ещё более опасным в условиях массированного применения. Рой «молчаливых» дронов, каждый из которых невидим для радиочастотных систем обнаружения, может приблизиться к объекту практически незамеченным. Именно поэтому эксперты говорят о «тёмных дронах» как об угрозе национальной безопасности и критической инфраструктуре.

Задачи, которые ставит перед системой «молчаливый» противник

Появление «молчаливых» дронов требует пересмотра самих принципов построения систем противовоздушной обороны. Вот ключевые задачи, которые этот класс угроз ставит перед любой защитной системой.

Задача 1. Обнаружение без радиочастотной подпи-

си

RF-пеленгация больше не является надёжным методом обнаружения. Система должна полагаться на другие физические принципы.

В арсенале остаются:

- Радары — но они должны быть достаточно чувствительными, чтобы обнаруживать малоразмерные цели с низкой эффективной поверхностью рассеяния (композитные материалы делают дроны почти невидимыми для радаров).

- Акустические датчики — они улавливают звук винтов, но только на коротких дистанциях и при условии отсутствия сильного фонового шума.

- Оптические и тепловизионные системы — они видят дрон, но только в пределах прямой видимости и при благоприятных погодных условиях.

Ни один из этих методов по отдельности не даёт полноценного решения. Только сенсорная фузия — объединение данных от разных типов датчиков — способна создать целостную картину воздушной обстановки.

Задача 2. Классификация без радиосигнатуры

Обычный RF-датчик не только обнаруживает дрон, но и идентифицирует его тип по характеристикам сигнала управления. «Молчаливый» дрон этой информации не даёт.

Как отличить автономный дрон-камикадзе от гражданского квадрокоптера, который случайно залетел в запретную зону? Как понять, что этот «молчаливый» объект несёт

взрывчатку, а не просто выполняет съёмку?

Ответ — в микродоплеровском анализе. Вращающиеся винты дрона создают характерные микроскопические изменения частоты отражённого радарного сигнала. Эти изменения позволяют отличить дрон от птицы, а один тип дрона — от другого. Нейросетевые алгоритмы, обученные на тысячах часов записей, способны сделать это за миллисекунды — но только если система вообще «видит» объект.

Задача 3. Противодействие в условиях, когда «нечем глушить»

Традиционная тактика борьбы с дронами включает радиоэлектронное подавление — глушение каналов управления и навигации. Против «молчаливого» дрона этот метод не работает. Его нельзя «отключить» удалённо, потому что ему не нужна связь.

Это означает, что единственный способ нейтрализации — физическое поражение: пулемётный огонь, зенитная ракета, дрон-перехватчик или лазерное оружие. Но для этого нужно точно знать, где находится цель, с какой скоростью и по какой траектории она движется. Ошибка в координатах — и средство поражения пролетает мимо, а дрон достигает цели.

Задача 4. Своевременность в условиях сокращённого времени реакции

«Молчаливые» дроны часто летят низко — чтобы оставаться вне зоны обнаружения радаров. Они могут появиться из-за складок местности, зданий или деревьев буквально за

секунды до подлёта к цели.

Традиционная цепочка «обнаружение идентификация принятие решения поражение» в таком сценарии просто не успевает сработать. Нужна система, которая автоматизирует каждый этап и сокращает задержки до миллисекунд. Нужна система, которая не ждёт, пока оператор посмотрит на экран, а действует самостоятельно.

Почему традиционные системы проигрывают

Именно здесь классические системы дают сбой. Построенные по принципу «один дорогой радар, одна камера, один центр управления», они оказываются беспомощными перед «молчаливым» противником.

Радар может «не заметить» маленький дрон из композитных материалов. RF-датчик «слышит» тишину. Акустика тонет в шуме города или ветра. Тепловизор видит только в пределах прямой видимости.

Каждый датчик по отдельности имеет слабые места. Но вместе они образуют систему, которая перекрывает недостатки друг друга.

Именно эту задачу решает проект «Фрактал». Он не пытается найти «серебряную пулю» против «молчаливых» дронов. Вместо этого он строит распределённую сенсорную сеть, где радары, акустические датчики и тепловизоры работают как единый организм. Где нейросети на каждом узле анализируют спектрограммы и микродоплеровские профили в реальном времени. Где решение о тревоге принима-

ется коллективно — несколькими узлами одновременно, по принципу консенсуса. «Молчаливый» дрон может обмануть один датчик. Но он не может обмануть сеть.

«Молчаливые» дроны — это не гипотетическая угроза будущего. Это реальность 2026 года. Технологии визуальной одометрии, пассивной навигации и автономного целеуказания уже существуют и активно внедряются. Они делают традиционные RF-методы обнаружения бесполезными и ставят перед системами ПВО задачи, которые невозможно решить в рамках централизованной архитектуры.

Ответом на этот вызов может быть только децентрализованная, гетерогенная, интеллектуальная сеть — где каждый узел видит по-своему, но вместе они формируют единый, точный образ воздушного пространства. Именно такую сеть и предлагает проект «Фрактал».

Глава 4. Почему одного радара недостаточно

В предыдущих главах мы говорили о том, как радикально изменилась природа воздушных угроз к 2026 году и почему традиционные системы ПВО оказались к ним не готовы. Теперь настало время разобрать главный инструмент, на который полагается большинство существующих систем обнаружения, — радар. И ответить на вопрос: почему в новой реальности одного радара недостаточно?

Радар как «дальномер»: дальность, скорость, координаты

Радар — это, по сути, «дальномер» с функцией измерения скорости. Он излучает радиоволны, принимает отражённый сигнал и на основе времени задержки и доплеровского сдвига частоты определяет три ключевых параметра цели: дальность (расстояние до объекта), азимут (направление) и радиальную скорость (приближается или удаляется). Именно за эти качества радар остаётся основой практически всех систем воздушного наблюдения.

У радара есть неоспоримые преимущества. Он работает на больших дистанциях, в любую погоду и в любое время суток — в отличие от оптических и тепловизионных систем, которые «слепнут» в тумане, дожде или темноте. Он обеспе-

чивает точное измерение координат и скорости, что критически важно для наведения средств поражения. В этом смысле радар — незаменимый инструмент.

Однако именно здесь кроется первая и самая опасная иллюзия: радар даёт нам координаты, но не даёт смысла. Он показывает, где находится объект и как быстро он движется, но не отвечает на вопрос, что это за объект. А в условиях войны дронов это вопрос жизни и смерти.

Ограничение первое: малые размеры и низкая эффективная поверхность рассеяния

Современные БПЛА — это не крупные самолёты с металлическими корпусами, хорошо отражающими радиоволны. Это лёгкие конструкции из композитов, пластика и углепластика. Их эффективная поверхность рассеяния (RCS) ничтожна — сопоставима с RCS крупной птицы.

Радар, настроенный на обнаружение традиционных воздушных целей, просто «не видит» такие объекты. Чтобы заметить маленький дрон, порог обнаружения приходится снижать. Но это ведёт к другой проблеме — лавине ложных срабатываний. Система начинает «видеть» всё, что хоть немного отражает радиоволны: птиц, облака, деревья, автомобили на ближайшей дороге.

Как отмечают исследователи, радарные системы демонстрируют отличные результаты в оценке дальности и скорости, но проблемы с небольшими БПЛА, обладающими низкой радиолокационной заметностью, и в условиях сильных

помех. Иными словами, радар отлично измеряет дальность и скорость — но только когда цель вообще удаётся обнаружить.

Ограничение второе: невозможность классификации

Предположим, радар всё-таки зафиксировал объект. Координаты есть, скорость есть. Но что это? Дрон? Птица? Лист, сорванный ветром? Облако?

Радар сам по себе не даёт ответа. Его сигнал — это просто отражённая электромагнитная волна. По ней можно определить размер, скорость и траекторию, но не природу объекта. А птицы и малые дроны демонстрируют схожие радиолокационные поперечные сечения и динамику полета. Они летают на одних и тех же высотах, с сопоставимыми скоростями, и радар их просто путает.

Особенно остро эта проблема стоит на низких высотах, где и действуют большинство угроз. Как указывается в одном из исследований, полеты на малых высотах вызывают помехи из-за перекрывающихся азимутов радиолокационного слежения, а городская застройка и рельеф создают многолучевые помехи, которые ещё больше запутывают картину.

Попытки решить проблему классификации с помощью микроплеровского анализа — то есть анализа тончайших изменений частоты отражённого сигнала, вызванных вращением винтов или взмахами крыльев, — дают ограниченный результат. Существующие системы на основе микродо-

плеровского анализа достигают точности всего 70–85%, это приводит к неприемлемо высокому уровню ложных срабатываний, что ставит под угрозу надежность работы. Даже самые современные алгоритмы, обещающие точность до 97,5%, работают в идеальных лабораторных условиях. В реальной боевой обстановке, с фоновыми шумами, помехами и меняющимися погодными условиями, результаты оказываются куда скромнее.

Ограничение третье: ложные цели — птицы, облака и не только

Проблема ложных целей — это не абстрактная теоретическая сложность. Это прямая угроза боеспособности системы.

Представьте: система ПВО получает сотни ложных тревог в час. Каждая из них требует проверки, отвлекает операторов, загружает вычислительные мощности. В критический момент, когда настоящий дрон действительно приближается к объекту, система может просто «захлебнуться» информационным шумом и не заметить угрозу.

Ложные тревоги, вызванные отражениями от птиц, «могут привести к перегрузке вычислительных устройств РЛС или даже бессмысленному расходованию боеприпасов на уничтожение не представляющих опасности объектов». Спектрограммы, создаваемые вращением винтов дрона, часто очень похожи на спектрограммы, получаемые при движении крыльев птиц. Причём ошибки возможны в обе сто-

роны: движение крыльев птицы может быть принято за вращение винтов (ложная тревога), а вращение винтов — за движение крыльев (пропуск цели).

Облака, атмосферные неоднородности, детали ландшафта — всё это создаёт отражения, которые радар с низким порогом обнаружения интерпретирует как цели. В одном из экспериментов матрица ошибок классификации показывала, что образцы облаков и деревьев регулярно ошибочно классифицируются как дроны.

Что это значит для защиты от дронов?

Один радар — это как прожектор в тёмном поле. Он показывает, что в поле что-то есть, но не говорит, кто это. Враг, друг, птица, облако? Решение принимает человек или автоматика — и цена ошибки может быть катастрофической.

Именно поэтому современные исследования сходятся во мнении: одномодальные подходы — радар, акустика, зрение или радиочастотная съёмка — недостаточны для надёжного обнаружения БПЛА в различных условиях. Ни один сенсор по отдельности не обеспечивает надёжного обнаружения дронов.

Радар даёт дальность, скорость и координаты — но не даёт классификации. Акустика даёт классификацию по звуку винтов — но работает на коротких дистанциях и страдает от фонового шума. RF-датчик идентифицирует дрон по его радиосигналу — но бесполезен против автономных аппаратов, которые «молчат». Тепловизор подтверждает цель — но до-

рог и требует прямой видимости.

Каждый из этих сенсоров по отдельности уязвим. Но вместе они образуют систему, которая перекрывает слабые места друг друга. Радар видит далеко — акустика уточняет, что именно он видит. RF-датчик идентифицирует «свой-чужой» — тепловизор подтверждает цель в сложных условиях.

Именно этот принцип — сенсорная фузия — лежит в основе нашего проекта. Не потому, что радар плох. А потому, что одного радара — как и любого одного сенсора — в новой реальности уже недостаточно. Угрозы изменились. Должны измениться и средства их обнаружения.

Глава 5. Акустический слух — микрофонные решётки

Звук — это, пожалуй, самое недооценённое чувство в системах противовоздушной обороны. Радары ищут отражённый сигнал, тепловизоры ловят инфракрасное излучение, RF-датчики охотятся за радиоволнами. Но ни один из них не работает в пассивном режиме так же эффективно, как обычный человеческий слух, который без всяких приборов способен определить направление на пролетающий самолёт за несколько километров.

Акустическое обнаружение дронов использует тот же природный принцип. Каждый беспилотный летательный аппарат — это источник характерного акустического излучения, создаваемого вращающимися винтами и работающими двигателями. Это излучение несёт в себе уникальную информацию: не только сам факт присутствия дрона, но и его тип, примерные размеры, а в некоторых случаях даже техническое состояние. Задача системы — услышать этот звук, понять, кому он принадлежит, и определить, откуда он исходит.

Принцип трёхмерной пеленгации

Человеческое ухо определяет направление на источник звука благодаря тому, что звук приходит к левому и правому

уху с разной задержкой и разной громкостью. Мозг анализирует эти микроскопические различия и строит пространственную картину. Микрофонная решётка работает по тому же принципу, но с гораздо большей точностью и в трёх измерениях.

В нашей системе на каждом узле используется тетраэдрическая решётка из четырёх MEMS-микрофонов. Почему именно тетраэдр — четырёхгранник с микрофонами в каждой вершине? Плоские решётки, где все микрофоны лежат в одной плоскости, страдают фундаментальным ограничением: они не могут однозначно определить угол места (высоту) источника звука. Для них все направления «вверх» и «вниз» относительно плоскости выглядят одинаково. Тетраэдрическая конфигурация решает эту проблему: три измерения пространства требуют как минимум четырёх точек, не лежащих в одной плоскости. Четыре микрофона, расположенных в вершинах правильного тетраэдра, дают ровно столько независимых парных разностей, сколько нужно для однозначного определения азимута и угла места источника звука.

Как это работает на физическом уровне.

Когда звуковая волна от дрона достигает микрофонной решётки, она приходит к каждому из четырёх микрофонов в разное время — с задержками, зависящими от расстояния между микрофонами и направления на источник. Эти задержки составляют микросекунды, но современные MEMS-

микрофоны с частотой дискретизации 44,1 кГц и выше способны их зафиксировать.

Алгоритм пеленгации использует метод TDOA (Time Difference of Arrival) — разности времени прихода сигнала. Для каждой пары микрофонов вычисляется взаимно-корреляционная функция, пик которой соответствует временной задержке между ними. Имея шесть независимых парных задержек (для четырёх микрофонов), система решает систему уравнений и определяет направление на источник в трёхмерном пространстве.

Для повышения точности в сложных акустических условиях — при отражениях от зданий, земли и других объектов — могут применяться более сложные алгоритмы, включая байесовские фильтры и модели гауссовых смесей, которые эффективно подавляют многолучевую интерференцию.

Современные полевые испытания показывают, что такие системы способны определять направление на квадрокоптер с точностью до $\pm 1^\circ$ по азимуту и углу места на дистанции до 200 метров. Для более крупных аппаратов с фиксированным крылом точность сохраняется на дистанциях до 400 метров.

Спектральный портрет дрона

Обнаружить звук — это только полдела. Гораздо важнее понять, что именно издаёт этот звук. Шум автомобильного двигателя, лай собаки, работа строительной техники, крики птиц — городской акустический ландшафт полон звуков, которые могут быть ошибочно приняты за дрон. И здесь на по-

мощь приходит спектральный анализ — способность системы «видеть» звук так, как его не видит человеческое ухо.

Как устроен акустический сигнал дрона.

Звук, издаваемый например мультироторным дроном, имеет сложную структуру.

Её можно разделить на две основные составляющие:

1. Дискретные (гармонические) составляющие — это тональные компоненты на частотах, кратных частоте вращения винтов. Для четырёхлопастного винта основная частота шума вращения равна частоте вращения, умноженной на число лопастей. Первые пять гармоник этой частоты дают наиболее заметный вклад в общий акустический портрет. Именно эти гармоники создают тот самый характерный «жужжащий» звук, по которому мы безошибочно узнаём дрон.

2. Широкополосная составляющая — это аэродинамический шум, создаваемый турбулентностью воздушного потока вокруг лопастей, а также шум от электродвигателей (аэродинамический, магнитный и механический). Этот компонент занимает широкий диапазон частот и создаёт «шумовую подушку», на фоне которой выделяются дискретные гармоники.

Каждый тип дрона имеет свой уникальный спектральный портрет.

Он зависит от множества факторов:

- Числа лопастей и винтов — четырёхлопастные винты

дают иной спектр, чем двухлопастные; квадрокоптеры с четырьмя винтами создают сложную интерференционную картину.

- Частоты вращения — разные режимы полёта (зависание, набор высоты, скоростной полёт) меняют спектр.

- Типа двигателей — бесколлекторные электродвигатели имеют свой характер шума.

- Конструктивных особенностей — даже дефекты лопастей влияют на спектральный портрет.

Именно эта уникальность делает возможным классификацию дрона по звуку. Нейросеть на NPU, получая Mel-спектрограмму — визуальное представление звукового сигнала в частотно-временной плоскости — сравнивает её с эталонными спектральными портретами, хранящимися в памяти. Современные системы на основе свёрточных нейросетей, обученные на миллионах аудиосэмплов, достигают точности идентификации типа дрона не менее 95%.

Mel-спектрограмма: почему именно она.

Человеческий слух воспринимает частоты нелинейно — мы лучше различаем низкие частоты, чем высокие. Mel-шкала была разработана именно для того, чтобы отражать это восприятие. Mel-спектрограмма — это представление звука, где частотная ось масштабирована по Mel-шкале, что делает её идеальной для задач распознавания: нейросеть «слышит» звук так же, как его слышит человек, но с гораздо большей детализацией.

В нашей системе NPU на каждом узле строит Mel-спектрограмму размером 128×128 точек прямо на месте съёма данных и пропускает её через лёгкую свёрточную нейросеть. Результат — не просто «да/нет», а вероятность принадлежности к определённому типу дрона с указанием уровня доверия.

Дистанция и влияние фоновых помех

Акустическое обнаружение имеет одно фундаментальное ограничение: звук затухает с расстоянием. И это затухание подчиняется суровым законам физики, которые нельзя обойти никакими алгоритмами.

Дальность обнаружения: от чего она зависит.

Ожидаемая дальность акустического обнаружения определяется соотношением сигнал-шум между акустической мощностью винтов дрона и уровнем фонового шума окружающей среды. Это соотношение масштабируется пропорционально квадратному корню из отношения сигнал/шум. Проще говоря, чтобы удвоить дальность обнаружения, мощность звука дрона должна вырасти в четыре раза, либо уровень фонового шума должен упасть в четыре раза.

В реальных условиях цифры выглядят так:

- В тихой обстановке (фоновый шум около 0 дБ, что практически недостижимо в полевых условиях) дальность обнаружения может достигать 1 км.
- В спокойной городской среде система надёжно обнаруживает малые квадрокоптеры на 200 метрах.

- Крупные дроны с двигателями внутреннего сгорания обнаруживаются на 4–5 км.

- FPV-дроны — самые маленькие и тихие — распознаются на дистанции от 300 до 500 метров.

Эти цифры объясняют, почему акустика в нашей системе не работает в одиночку. На дистанциях свыше 200–500 метров звук дрона может быть слишком слабым для надёжного обнаружения, особенно на фоне городского шума. Но именно здесь в дело вступает радар, который видит объект на километры вперёд. Акустика же выполняет свою роль на «финишной прямой» — когда дрон уже приблизился к охраняемому объекту и требует точной классификации и пеленгации.

Главный враг — фоновый шум.

Уровень фонового шума — это второй по значимости параметр, влияющий на дальность обнаружения (после мощности самого дрона). И здесь система сталкивается с серьёзными вызовами:

- Городской шум — транспорт, стройки, промышленные объекты создают мощный акустический фон, маскирующий сигнал дрона.

- Погодные условия — дождь, ветер, снег создают собственный шум, который может перекрыть звук винтов.

- Акустические помехи — отражения от зданий, земли, деревьев создают многолучевость, искажающую сигнал.

Для борьбы с этими помехами в системе используются

несколько уровней защиты:

1. Пространственная фильтрация — тетраэдрическая решётка позволяет сформировать диаграмму направленности, подавляющую звуки, приходящие с других направлений.

2. Спектральная фильтрация — нейросеть обучена отличать спектральный портрет дрона от шумов города даже при низком соотношении сигнал-шум.

3. Верификация по сети — если один узел «слышит» подозрительный сигнал, но не уверен, он запрашивает подтверждение у соседей. Если три узла в разных точках зафиксировали один и тот же спектральный профиль в одном направлении — ложная тревога практически исключена.

Критерий слышимости.

Существует эмпирическое правило: беспилотный летательный аппарат становится акустически обнаруживаемым, когда его уровень шума превышает природный фон на 3 дБА. Это означает, что даже небольшое превышение фона уже даёт системе шанс на обнаружение — при условии, что нейросеть правильно «узнает» спектральный портрет.

Именно поэтому в нашей системе акустический датчик — это не просто «микрофон», а полноценный вычислительный модуль. MEMS-микрофоны с частотой дискретизации 44,1 кГц и динамическим диапазоном не менее 80 дБ собирают данные. MCU буферизует аудиопоток и передаёт его на NPU. NPU строит Mel-спектрограмму, прогоняет её через нейросеть и за миллисекунды выдаёт вердикт: есть дрон или

нет, и если есть — какой именно.

Акустическое обнаружение не заменит радар. Но оно даёт системе то, чего не даёт ни один радар: способность опознать дрон по «голосу», точно определить его тип и подтвердить, что в небе — не птица, не облако и не ложная цель. В сочетании с радаром, RF-детектором и тепловизором акустика превращается из слабого звена в один из столпов сенсорной фузии — «слух» системы, который слышит то, чего не видят остальные.

Глава 6. Радиочастотный детектор — «перехватчик» радиоголосов

В предыдущей главе мы говорили об акустическом «слуше» системы — способности слышать дрон по звуку его винтов. Но у каждого дрона есть ещё один «голос», который он не всегда может скрыть, — это его радиоизлучение. Большинство беспилотных аппаратов управляются по радиоканалу, передают телеметрию и видеосигнал. И этот радиоголос — ценнейший источник информации для системы обнаружения.

Радиочастотный (RF) датчик в нашей сети выполняет роль пассивного перехватчика. Он ничего не излучает, не демаскирует себя, не создаёт помех. Он просто слушает эфир — и когда дрон «говорит», RF-датчик слышит его, идентифицирует и определяет направление. Это делает RF-обнаружение одним из самых надёжных и информативных методов пассивной разведки в арсенале противодроновой обороны.

Пассивное сканирование: как перехватчик слышит эфир

Современные дроны используют для связи несколько основных частотных диапазонов. Выбор конкретной частоты зависит от задач аппарата, его размера и требуемой дальности управления. Наш RF-датчик перекрывает все ключенные

диапазоны, в которых работают подавляющее большинство гражданских и многих военных БПЛА.

433 МГц — это «дальнобойный» диапазон. Сигналы на этой частоте обладают отличной проникающей способностью, огибают препятствия и сохраняют мощность на дистанциях до нескольких километров. Здесь работают многие системы дальнего управления, телеметрии и некоторые типы радиомаяков. Однако пропускная способность этого диапазона невелика, поэтому для передачи видео он практически не используется.

900 МГц (в России — 868–915 МГц) — ещё один «дальний» диапазон, который активно применяется в системах управления коммерческими и промышленными дронами. Он обеспечивает хороший компромисс между дальностью и скоростью передачи данных. Многие производители выбирают именно этот диапазон для своих аппаратов средней дальности.

2.4 ГГц — это, без преувеличения, «сердце» радиоуправления дронами. Именно здесь работают подавляющее большинство пультов управления, систем телеметрии и некоторые видеопередатчики. Но у этого диапазона есть один серьёзный недостаток: он переполнен. Wi-Fi, Bluetooth, микроволновые печи и тысячи других устройств создают мощный фоновый шум, в котором сигнал дрона может затеряться. Задача RF-датчика — не просто обнаружить наличие сигнала в этом хаосе, а выделить из него именно тот, который

принадлежит дрону.

5.8 ГГц — основной диапазон для передачи видеосигнала с дрона. Здесь и FPV-каналы, и системы высокоскоростной передачи данных. Этот диапазон обладает высокой пропускной способностью, но его сигналы хуже проникают сквозь препятствия и быстрее затухают с расстоянием.

Современные коммерческие RF-детекторы перекрывают диапазон от 70 МГц до 6 ГГц, что позволяет обнаруживать сигналы управления практически всех существующих типов дронов. Наш датчик построен по тому же принципу: он постоянно сканирует эти диапазоны, фиксируя любые сигналы, превышающие порог чувствительности.

Как организовано сканирование.

RF-датчик может быть реализован двумя способами. Первый — на основе широкополосного SDR-приёмника (Software Defined Radio), который оцифровывает весь диапазон сразу и передаёт данные на NPU для анализа. Второй — на основе специализированного чипа-детектора с перестройкой частоты, который последовательно «просматривает» узкие участки спектра.

В нашей системе используется гибридный подход: широкополосный приёмник с быстрым переключением между ключевыми диапазонами. Это позволяет одновременно отслеживать активность на всех критичных частотах. При обнаружении сигнала выше порога формируется спектрограмма «частота–время» — визуальное представление того, как

меняется спектр сигнала во времени. Именно эта спектрограмма отправляется на NPU для идентификации.

Чувствительность приёмника должна быть не хуже -100 дБм — это уровень, достаточный для обнаружения даже слабых сигналов с дронов, находящихся на значительном удалении. Скорость сканирования выбирается такой, чтобы гарантированно захватывать кратковременные пакеты данных, включая быстрые Frequency Hopping Spread Spectrum (FHSS) сигналы, которые постоянно меняют частоту.

Идентификация типа управления и телеметрии

Обнаружить радиосигнал — это только первый шаг. Гораздо важнее понять, кому принадлежит этот сигнал и что он означает. Здесь на помощь приходит распознавание RF-«отпечатков» — уникальных характеристик сигналов, по которым можно идентифицировать не только тип дрона, но даже конкретную модель или производителя.

Какие сигналы излучает дрон.

У большинства коммерческих и многих военных БПЛА есть три основных типа радиосигналов:

1. Сигнал управления (uplink) — идёт от пульта оператора к дрону. Содержит команды на изменение скорости, направления, высоты и других параметров полёта. Обычно это короткие пакеты данных, передаваемые с высокой частотой.
2. Сигнал телеметрии (downlink) — передаётся от дрона к оператору. Содержит информацию о координатах, высоте, скорости, заряде батареи, статусе двигателей и других пара-

метрах.

3. Видеосигнал — передаёт изображение с бортовой камеры. Это самый «тяжёлый» тип сигнала, требующий высокой пропускной способности. Часто передаётся на отдельной частоте (например, 5.8 ГГц).

Каждый из этих сигналов имеет свои характерные особенности: тип модуляции, структуру пакетов, частоту следования, шаблонных перескоков (для FHSS). Современные системы RF-идентификации используют паттерн-распознавание — методы, которые выделяют повторяющиеся структуры в передачах дрона и позволяют отличить управляющие команды от телеметрии и видеосигнала.

Как нейросеть на NPU идентифицирует дрон.

На каждом узле нашей сети NPU получает спектрограмму RF-сигнала и анализирует её с помощью лёгкой свёрточной нейросети. Нейросеть обучена распознавать:

- Тип модуляции — например, FHSS (Frequency Hopping Spread Spectrum) для многих современных пультов или OFDM для видеосигналов.

- Протокол — DJI OcuSync, ExpressLRS, Crossfire, ELRS и другие.

- Производителя — по уникальным «почеркам» сигналов, которые отличаются у разных брендов.

- Конкретную модель — при достаточной базе данных.

RF-идентификация настолько точна, что некоторые системы способны различать до 17 различных моделей дро-

нов по их RF-сигнатурам. В условиях плотного эфира, где 2.4 ГГц переполнен Wi-Fi и Bluetooth-сигналами, нейросеть способна выделить именно дронный сигнал по его уникальным спектральным и временным характеристикам.

Важно понимать: RF-датчик не просто даёт ответ «дрон/не дрон». Он предоставляет полный профиль — тип управления, протокол, производителя, модель и, что критически важно, уровень доверия к этому определению. Эта информация передаётся в сеть вместе с треком и используется для принятия решений — как тактических, так и стратегических.

Проблема «молчащих» дронов — и как сеть компенсирует это

У RF-обнаружения есть один фатальный недостаток: оно работает только тогда, когда дрон излучает. Если дрон «молчит» — если он не передаёт ни управляющих сигналов, ни телеметрии, ни видео — RF-датчик становится бесполезным.

Именно такие аппараты называют «тёмными» дронами (dark drones) или RF-silent дронами. Они не излучают радиочастотных сигналов или электронных подписей, что делает их чрезвычайно сложными для традиционных систем обнаружения. Эти угрозы уже широко применяются в современных конфликтах, и представляют собой одну из самых сложных задач в сфере противодействия БПЛА.

Откуда берутся «молчащие» дроны.

Существует несколько сценариев, при которых дрон не излучает радиосигналов.

Первый и самый очевидный — полностью автономный полёт. Дрон получает задание до старта, загружает карту маршрута и выполняет его, ориентируясь исключительно на встроенные датчики — камеры, инерциальные системы, иногда — на спутниковую навигацию. Радиосвязь с оператором не используется. Такие аппараты практически невозможно обнаружить средствами радиоэлектронной разведки.

Второй сценарий — режим радиомолчания, когда оператор намеренно отключает все передатчики на борту, чтобы скрыть дрон от систем RF-обнаружения. Дрон может лететь по заранее заданному маршруту, а связь восстанавливается только в критический момент — например, для подтверждения цели.

Третий — использование оптоволоконной линии связи вместо радиоканала. В этом случае сигнал управления и телеметрии передаются по оптоволоконному кабелю, который разматывается с дрона в полёте. Такой дрон не излучает вообще ничего, оставаясь невидимым для любых RF-детекторов.

Четвёртый сценарий — электромагнитная тишина как тактический приём. Группа дронов может выполнять полёт в режиме полного радиомолчания, обмениваясь данными только между собой по узконаправленным каналам или вообще без обмена, действуя по заранее согласованному алго-

ритму.

Почему это проблема для традиционных систем.

Большинство существующих C-UAS (Counter-Unmanned Aircraft Systems) решений полагаются на RF-обнаружение как на основной или один из основных методов идентификации угроз. Когда дрон перестаёт излучать, эти системы «слепнут». Они могут зафиксировать объект радаром, но не могут его классифицировать — понять, что это именно дрон, а не птица или облако. А без классификации невозможно принять решение о противодействии.

Именно здесь архитектура нашей сети проявляет свои ключевые преимущества.

Как сеть компенсирует «молчание» дрона.

В проекте «Фрактал» RF-датчик — это один из четырёх, но не единственный. Когда дрон «молчит», его всё равно можно обнаружить другими способами:

- Радар видит движущийся объект, определяет его координаты и скорость. Даже если дрон не излучает, он отражает радиоволны.

- Акустика слышит звук винтов. Даже самый тихий дрон создаёт акустический шум, который можно зафиксировать на определённой дистанции.

- Тепловизор (на командном узле) видит тепловой след от моторов и электроники.

Но главное — это протокол трек-верификации. Когда один узел обнаруживает объект по радару, но RF-датчик

молчит (а значит, нет уверенности в классификации), он не объявляет тревогу в одиночку. Вместо этого он отправляет запрос соседям: «Я вижу объект в секторе таком-то. У вас есть акустическое или RF-подтверждение?»

Если три соседних узла в тот же момент зафиксировали акустический сигнал в том же направлении — цель считается реально существующей, даже если RF-каналы молчат. Если один из соседних узлов «услышал» RF-сигнал — классификация становится точной. Если ни один RF-датчик не слышит ничего, а акустика не даёт уверенного результата — система может запросить подтверждение у командного узла с тепловизором, который наведёт оптику в указанную точку.

Таким образом, RF-датчик в нашей системе — это не «всё или ничего». Это один из голосов в хоре. Когда он молчит, другие голоса продолжают звучать. И именно коллективное решение сети позволяет отличить «молчащий» дрон от ложной цели.

Исследования показывают, что для полного подавления всех каналов обнаружения «тёмному» дрону нужно одновременно избегать радиолокационного отражения (что практически невозможно для аппарата с винтами), акустического излучения (что требует практически бесшумных двигателей) и теплового следа (что невозможно без специального охлаждения). В ближайшие годы появление дронов, невидимых одновременно для всех четырёх типов сенсоров, маловероятно.

RF-детектор как элемент сетевой разведки

Помимо прямой задачи обнаружения, RF-датчик выполняет ещё одну важную функцию — сбор разведывательной информации о противнике.

Когда система фиксирует RF-сигнал от дрона, она не просто отмечает его присутствие.

Она запоминает:

- Тип сигнала и протокол — это позволяет понять, какое оборудование использует противник.
- Модель дрона — даёт представление о его возможностях (дальность, полезная нагрузка, автономность).
- Паттерны поведения — например, характерные интервалы между пакетами телеметрии могут указывать на определённые тактические приёмы.

Эта информация агрегируется на уровне «Команды» и может использоваться для стратегического анализа: выявления новых типов угроз, прогнозирования маршрутов, адаптации правил ведения огня.

Более того, собранные RF-данные позволяют обновлять модели NPU по всей сети. Если вышестоящий штаб выявил новый тип дрона с неизвестным ранее RF-профилем, его «цифровой портрет» может быть рассчитан и распространён по всем узлам через спутниковый канал. В следующий раз, когда этот дрон появится в зоне действия сети, его идентифицируют мгновенно.

Электромагнитная совместимость: когда радар и

RF-датчик мешают друг другу

В завершение — важное техническое замечание. В нашей системе на одном узле одновременно работают радар (который излучает) и RF-датчик (который принимает). Это создаёт потенциальный конфликт: мощный импульс радара может перегрузить входные цепи RF-приёмника и вывести его из строя или, как минимум, сделать его «слепым» на время работы радара.

Для решения этой проблемы в архитектуре предусмотрены два механизма:

1. Физическое разнесение — антенны радара и RF-датчика размещаются на максимально возможном расстоянии друг от друга и экранируются.
2. Временная синхронизация — в момент излучения радарного импульса RF-вход блокируется аттенюатором (ослабителем сигнала), защищая малошумящий усилитель (LNA) от перегрузки. Это делается аппаратно, по сигналу от MCU, с задержкой в микросекунды.

Такое решение позволяет радару и RF-датчику работать практически одновременно, не мешая друг другу, и обеспечивает непрерывное покрытие всеми четырьмя сенсорными каналами.

RF-детектор — это «радиослух» системы, её способность слышать то, что не видят радар и тепловизор. Он даёт точную идентификацию, определяет тип управления и модель дрона, собирает разведывательную информацию. Но он не

самодостаточен. Именно в комбинации с другими сенсорами — радаром, акустикой, тепловизором — и в рамках децентрализованной сети с протоколом трек-верификации RF-обнаружение превращается из уязвимого звена в один из столпов системы, способной видеть даже «молчащие» угрозы.

Глава 7. Тепловизор — зрение в темноте

Среди всех четырёх типов сенсоров, составляющих сенсорную фузию проекта «Фрактал», тепловизор занимает особое место. Радар видит далеко, но не знает, что именно он видит. Акустика слышит «голос» дрона, но глуха на дистанции. RF-датчик перехватывает радиосигналы, но бессилен против «молчаливых» аппаратов. Тепловизор же — единственный сенсор, который в равной степени эффективен и днём, и ночью, в тумане и в дыму, против движущихся и зависших целей. Он не просто дополняет другие датчики — он становится тем самым «арбитром», который в спорных ситуациях выносит окончательный вердикт: есть угроза или нет.

Неохлаждаемый микроболометр — тихая революция

Чтобы понять, почему тепловизор стал доступным для массового применения в системах противодроновой обороны, нужно разобраться в том, как работают тепловизионные датчики вообще. Исторически сложилось так, что высокочувствительные тепловизоры требовали криогенного охлаждения — детектор нужно было охлаждать до температур жидкого азота (около 196 °С), чтобы минимизировать соб-

ственный тепловой шум и добиться максимальной чувствительности. Такие системы дают впечатляющие результаты: чувствительность до 5–10 мК (милликельвинов), способность различать мельчайшие перепады температур. Но цена этого преимущества — сложность, вес, энергопотребление и стоимость. Охлаждаемый тепловизор — это не просто камера, это целая инфраструктура: криогенный двигатель, трубки, хладагент, регулярное обслуживание. Такой прибор может стоить в 5–20 раз дороже неохлаждаемого аналога. Один охлаждаемый тепловизор для систем безопасности обходится примерно в \$20 000, тогда как неохлаждаемый — около \$500.

Неохлаждаемый микроболометр работает по совершенно иному принципу. Вместо того чтобы регистрировать отдельные фотоны инфракрасного излучения (как это делают охлаждаемые детекторы), микроболометр измеряет изменение температуры термоизолированной мембраны, которая нагревается под действием падающего инфракрасного излучения. Каждый пиксель матрицы — это микроскопический «термометр», который меняет своё электрическое сопротивление в зависимости от температуры. Такие детекторы работают при комнатной температуре и не требуют никакого охлаждения.

У этой технологии есть свои ограничения: чувствительность неохлаждаемых микроболометров ниже, чем у охлаждаемых систем (типичные значения — около 40 мК против

5–10 мК). Однако для задач обнаружения дронов этой чувствительности более чем достаточно: тепловой след от работающих моторов и электроники дрона значительно превышает порог обнаружения.

Что даёт неохлаждаемый микроболометр системе «Фрактал»:

- Малый вес и компактность. Отсутствие криогенного оборудования позволяет встраивать тепловизор в мобильный узел без ущерба для его подвижности.

- Низкое энергопотребление. В то время как охлаждаемые системы потребляют десятки ватт только на поддержание температуры, неохлаждаемый микроболометр укладывается в 1 Вт в активном режиме, что критично для автономной работы узла от аккумулятора.

- Надёжность и отсутствие обслуживания. Нет движущихся частей, нет хладагента, нет регулярных замен фильтров и компрессоров.

- Мгновенная готовность. Охлаждаемому детектору требуется время, чтобы достичь рабочей температуры. Микроболометр готов к работе сразу после включения.

- Стоимость. Это, пожалуй, самый важный фактор. Современные тепловизоры на основе неохлаждаемых микроболометров с разрешением 640×512 пикселей и частотой 60 Гц становятся доступными для массового применения. Стоимость качественного тепловизора, способного обнаружить дрон самолетного типа на дистанции до 8 км, оценивается в

\$7 000–8 000 (примерно 600–700 тыс. рублей) — и эта цена продолжает снижаться по мере развития технологий.

В системе «Фрактал» используется тепловизор с разрешением не менее 640×512 пикселей, частотой кадров 60 Гц и чувствительностью не хуже 20 мК — характеристики, которые полностью обеспечивают все задачи по обнаружению и верификации дронов.

Подтверждение цели в тумане, ночью и при маскировке

Оптические камеры, работающие в видимом диапазоне, — это глаза системы. Но у этих глаз есть серьёзные ограничения: они слепнут в темноте, беспомощны в тумане и легко обманываются маскировкой. Тепловизор решает все эти проблемы.

Ночь — не помеха.

Инфракрасное излучение, которое регистрирует тепловизор, исходит от самих объектов — от их нагретых элементов. Дрон в полёте — это не просто механическая конструкция. Его двигатели нагреваются, электроника выделяет тепло, аккумуляторы работают в активном режиме. Всё это создаёт устойчивый тепловой контраст на фоне окружающей среды, особенно ночью, когда земля и воздух остывают. Именно поэтому тепловизоры стали основным инструментом ночной охоты на дроны — они видят то, что скрыто от человеческого глаза и любой оптической камеры.

Туман и дым — преодолимы.

В отличие от видимого света, длинноволновое инфракрасное излучение (диапазон 8–14 мкм) гораздо лучше проникает через взвешенные в воздухе частицы — капли воды, дым, пыль. Тепловизор «пробивает» лёгкую дымку и туман, обеспечивая детализацию, недоступную для обычной камеры. Комплексы на основе тепловизионных камер способны работать 24 часа в сутки — в полной темноте, в плотном тумане, в дыму и даже во время снегопада.

Маскировка — не гарантия безопасности.

Противник может попытаться скрыть дрон от тепловизора, используя теплоизоляционные материалы или специальные «плащи-невидимки», снижающие тепловую сигнатуру. Однако практика показывает, что дешёвые маскировочные решения часто дают обратный эффект: плохо продуманные теплоизоляционные покрытия создают на теле дрона холодные пятна, которые на фоне более тёплого окружения выглядят даже более контрастно, чем сам дрон без маскировки. В любом случае, даже если тепловая сигнатура дрона ослаблена, система «Фрактал» не полагается на один только тепловизор — он выступает в роли верификатора, а не первичного детектора. Если радар и акустика уже зафиксировали объект в определённой точке, тепловизор знает, куда смотреть, и может сфокусироваться на конкретном секторе, что многократно повышает вероятность обнаружения даже слабого теплового сигнала.

Как работает верификация на практике.

Когда узел-боец обнаруживает цель по радару и акустике, но не может её однозначно классифицировать (например, потому что RF-датчик «молчит», а акустический сигнал слаб), он отправляет запрос командному узлу (МОГ). Командный узел, получив координаты трека, за доли секунды наводит тепловизор в указанную точку. Тепловизор с частотой 60 кадров в секунду захватывает изображение, нейросеть на NPU командира анализирует тепловой портрет цели и выдаёт вердикт: это дрон, птица или ложная цель. Вся операция занимает миллисекунды — быстрее, чем дрон успеет изменить траекторию.

Почему тепловизор устанавливается только на командных узлах — экономическая логика

Самое дорогое, что есть в системе «Фрактал», — это тепловизор. И именно здесь архитектура проекта демонстрирует свою экономическую эффективность. В отличие от традиционных систем ПВО, где каждый пост охраны оснащается полным набором датчиков, включая дорогие тепловизоры, проект «Фрактал» предлагает гетерогенную модель: один командный узел с тепловизором на группу из 10–15 «бойцов», у которых тепловизора нет.

Почему это работает.

В логике обнаружения дронов тепловизор решает задачу верификации, а не первичного обнаружения. Первичное обнаружение обеспечивают радары и акустические датчики, которые установлены на каждом «бойце» и стоят на поряд-

ки дешевле. Если каждый «боец» будет оснащён тепловизором, стоимость системы вырастет в 10–15 раз без пропорционального роста эффективности, потому что:

1. Тепловизор не нужен постоянно. В большинстве сценариев радар и акустика дают достаточно информации для принятия решения. Тепловизор требуется только в сложных случаях — для подтверждения типа цели или для работы в экстремальных погодных условиях.

2. Один тепловизор покрывает зону всех «бойцов». Поскольку «бойцы» развёрнуты в пределах радиуса прямой видимости (до 1–2 км друг от друга), один командный узел с тепловизором может по запросу «заглянуть» в любой сектор, который видит любой из «бойцов».

3. Командный узел — мобильный. МОГ не привязана к одной точке. Она может перемещаться, оптимизируя зону покрытия тепловизора в зависимости от текущей угрозы.

Цифры, которые говорят сами за себя.

- Тепловизор с характеристиками, необходимыми для обнаружения дронов на дистанции до 8 км, стоит \$7 000–8 000.

- Для сети из 10 узлов (1 «командир» + 9 «бойцов») стоимость тепловизионной части составляет \$7 000–8 000.

- Если бы каждый из 10 узлов был оснащён тепловизором, стоимость выросла бы до \$70 000–80 000 только за счёт тепловизоров.

Экономия — в 10 раз без потери функциональности.

Что даёт эта экономия.

Сэкономленные средства могут быть направлены на:

- Увеличение количества «бойцов». Вместо 10 узлов с тепловизорами можно развернуть 100 узлов с радарами и акустикой, кратно увеличив плотность сенсорного покрытия.

- Усиление средств поражения. Интеграция более эффективных систем перехвата на МОГ.

- Резервирование. Возможность иметь несколько МОГ в пределах одной сети, каждая со своим тепловизором, для повышения живучести.

Но есть и нюанс.

Фрактальная архитектура проекта предусматривает, что роль «командира» не является статичной. Если командный узел выходит из строя, его функции — включая тепловизионную верификацию — может взять на себя любой другой узел, на котором установлен тепловизор. В идеальной конфигурации система может иметь несколько МОГ с тепловизорами, распределённых по территории, что создаёт избыточность и ещё больше повышает надёжность. Но даже в этом случае количество тепловизоров в сети остаётся на порядок меньше, чем количество узлов-бойцов.

Итог экономической логики.

Тепловизор — это не роскошь, а стратегический ресурс. В системе «Фрактал» он размещается там, где приносит максимальную пользу, — на мобильной огневой группе, кото-

рая выступает центром принятия решений. «Бойцы» обеспечивают массовость и плотность покрытия, «Командир» — точность и верификацию. Один дорогой тепловизор на десять дешёвых сенсорных узлов — это не компромисс, а оптимальное распределение ресурсов, которое делает систему «Фрактал» одновременно и эффективной, и доступной для массового развёртывания.

Глава 8. Сенсорная фузия на практике

Каждый из четырёх датчиков системы «Фрактал» по отдельности — это инструмент с принципиальными ограничениями. Радар может «ослепнуть» из-за отражений от земли или не различить дрон и птицу. Акустика «глохнет» на ветру и при городском шуме. RF-датчик беспомощен против автономных дронов, которые вообще не излучают радиосигналов. Тепловизор даёт кристально чистую картинку, но стоит дорого и потому устанавливается только на командных узлах.

Современные угрозы устроены хитрее: автономные дроны, наводящиеся на цель по встроенной оптике и базе данных, вообще не излучают радиочастотных сигналов. Но именно в этом и заключается парадокс: ни один дрон не является полностью «тёмным». Он всегда издаёт звук, всегда отражает радиоволны и всегда выделяет тепло. Вопрос лишь в том, как собрать эти разрозненные «отпечатки» в единую картину.

Ответ — сенсорная фузия. Не просто параллельное использование разных датчиков, а их глубокая интеграция на уровне данных, решений и, что особенно важно, на уровне всей сети.

Четыре датчика — четыре роли в одном оркестре

Сенсорная фузия в системе «Фрактал» строится не как простая сумма показаний, а как иерархический процесс, где каждый датчик выполняет свою уникальную функцию на разных этапах обнаружения и верификации.

Радар — «дальномер» и «первый свидетель». Радар миллиметрового диапазона (около 60 ГГц) обеспечивает первичное обнаружение движущихся объектов на дистанции до нескольких километров. Он даёт координаты, скорость и направление движения. Но радар не знает, что именно он видит: дрон, птицу или просто облако. Его главная задача — заметить, что в воздухе что-то есть.

Более того, радар способен на большее. Анализируя микроплеровский профиль — тончайшие изменения частоты отражённого сигнала, вызванные вращением винтов дрона, — нейросеть на NPU может отличить дрон от птицы ещё до того, как в дело вступят другие датчики. Вращающийся винт создаёт характерные модуляции сигнала, которых нет у машущего крыла. Исследования показывают, что классификация на основе микроплеровских сигнатур может достигать точности от 96% до 100%. Но даже эта высокая точность не абсолютна — и здесь на сцену выходят остальные чувства системы.

Акустика — «классификатор по голосу». Когда радар зафиксировал объект, акустический датчик включается в работу. Микрофонная решётка улавливает звук винтов, NPU

строит Mel-спектрограмму и сравнивает её с базой известных акустических портретов. Современные системы на основе свёрточных нейросетей способны различать десятки типов дронов с точностью более 97%. Акустика не просто подтверждает, что объект — это дрон. Она говорит, какой именно дрон: модель, размер, а иногда даже режим полёта.

Но у акустики есть ограничение по дальности: в реальных условиях она надёжно работает на дистанции 300–500 метров. На больших расстояниях звук затухает или маскируется фоновым шумом. Поэтому акустика — это датчик «финишной прямой», который вступает в игру, когда дрон уже приближается к охраняемому объекту, при ограниченной сети.

RF-датчик — «идентификатор свой-чужой». Радиочастотный детектор сканирует эфир в поисках сигналов управления и телеметрии в диапазонах 433 МГц, 900 МГц, 2,4 ГГц и 5,8 ГГц. Если дрон управляется по радиоканалу или передаёт телеметрию, RF-датчик не просто обнаруживает его — он может определить, модель и даже местоположение пилота.

Но ключевая функция RF-датчика в нашей системе — идентификация «свой-чужой». Дружественные дроны, оснащённые радиолокационным опознавателем, автоматически маркируются системой на высоте до 5 км и расстоянии до 100 км от запросчика. Это позволяет сети мгновенно отличать свои аппараты от вражеских и не тратить ресурсы на ложные тревоги.

Однако если дрон летит в полностью автономном режиме, без радиосвязи, RF-датчик «слепнет». Именно для этого сценария и нужны остальные три датчика.

Тепловизор — «арбитр» и «последнее слово». Тепловизор устанавливается только на командных узлах (МОГ) — он слишком дорог для массового развёртывания. Но его роль в системе уникальна: он обеспечивает верификацию высшего уровня. Когда «боец» обнаруживает цель, но не может её однозначно классифицировать (например, из-за того, что RF-датчик молчит, а акустика не уверена из-за шума), он отправляет запрос «командиру». Тот за доли секунды наводит тепловизор в указанную точку и подтверждает или опровергает угрозу.

Тепловизор видит тепловой след от моторов и электроники — и делает это в условиях, где другие датчики бессильны: ночью, в тумане, при плохой видимости. Это «судья», который выносит окончательный вердикт.

От разрозненных сигналов к единой картине: пошаговый сценарий

Представим, как эта четвёрка работает вместе в реальной боевой обстановке.

Шаг 1. Радар замечает движение. На расстоянии 1,5 км от охраняемого объекта радар одного из узлов-бойцов фиксирует движущуюся точку. NPU на узле анализирует микродоплеровский профиль и определяет, что это не птица — слишком регулярная модуляция сигнала, характерная для

вращающихся винтов. Но уверенность пока не абсолютна: 78%. Узел формирует «сырой» трек — координаты, скорость, направление — и передаёт его в mesh-сеть.

Шаг 2. Сеть просыпается. Соседние узлы получают трек. Их радары автоматически перенаправляются в указанный сектор. Через 200 миллисекунд два соседних узла подтверждают: да, в том же направлении есть движущийся объект. Три радара видят одну цель с разных точек — это уже не случайность.

Шаг 3. Акустика вступает в игру. Дрон приближается — дистанция сокращается до 400 метров. Микрофонные решётки трёх узлов улавливают характерный звук винтов. NPU на каждом узле строит Mel-спектрограмму и прогоняет её через нейросеть. Все три узла сходятся в одном: это квадрокоптер коммерческого типа, уровень доверия 96%. Акустика не только подтверждает, что это дрон, но и называет его модель.

Шаг 4. RF-датчик проверяет «свой-чужой». RF-детекторы сканируют эфир в направлении цели. Сигналов управления не обнаружено — дрон не передаёт телеметрию и не отвечает на запросы опознавания. Это либо свой аппарат, либо вражеский. RF-датчик не даёт однозначного ответа, но его «молчание» — это тоже данные: дрон не свой.

Шаг 5. Командир берёт слово. Трек с пометкой «неопознанный, вероятно вражеский» достигает МОГ. Командир наводит тепловизор в указанный сектор. Инфракрасная ка-

мера видит чёткий тепловой след от четырёх моторов — характерная картина для квадрокоптера. Тепловизор подтверждает: цель реальна, это дрон, своих сигналов нет.

Шаг 6. Огневое решение. Система на МОГ автоматически рассчитывает время подлёта к охраняемому объекту, зону поражения и выбирает средство перехвата. Через 1,2 секунды после первого обнаружения цель взята на сопровождение, и средства поражения получают точные координаты.

Весь цикл — от первого сигнала радара до готовности к поражению — занимает менее двух секунд. Без участия человека.

Коллективный разум: как сеть отсеивает ложные тревоги

Ложные срабатывания — это проклятие всех систем обнаружения. Птицы, облака, отражения от зданий, автомобильный шум, радиопомехи — в реальной оперативной среде количество ложных тревог может сделать систему бесполезной. Именно здесь децентрализованная архитектура «Фрактала» даёт решающее преимущество.

Протокол трек-верификации: консенсус вместо паники.

Когда один узел обнаруживает потенциальную цель, он не объявляет тревогу немедленно. Вместо этого он отправляет запрос соседям: «Я вижу объект на азимуте 45 градусов, дальность 3 километра. Подтвердите?»

Ответы соседей проходят через три уровня фильтрации:

1. Пространственное подтверждение. Если три узла в разных точках зафиксировали объект в одном направлении с согласующимися координатами — это уже сильный аргумент в пользу реальности цели. Случайные ложные срабатывания (птица, отражение) почти никогда не совпадают у нескольких узлов одновременно.

2. Модальное подтверждение. Даже если радары трёх узлов видят объект, это может быть стая птиц. Но если одновременно с радарным треком акустические датчики тех же узлов зафиксировали спектральный портрет, характерный для дрона, — вероятность ошибки резко падает. Каждая модальность подтверждает другие.

3. Временная когерентность. Все треки снабжены временными метками от GPS с точностью <1 мс. Система проверяет, совпадают ли временные профили сигналов с разных узлов. Если радар видит объект, акустика слышит его с задержкой, соответствующей скорости звука, а RF-датчик фиксирует сигнал с той же задержкой — это практически неопровержимое доказательство.

Результат: драматическое снижение ложных тревог.

Исследования показывают, что системы сенсорной фузии с распределённой верификацией способны удерживать уровень ложных срабатываний ниже 10% при точности обнаружения более 90%. Для традиционных одиночных сенсоров эти цифры выглядят иначе: радары на открытой местности могут давать сотни ложных тревог в час от птиц и отраже-

ний.

Но самое важное — это живучесть системы. Если один узел повреждён или ослеплён помехами, сеть продолжает работать. Если командир потерял связь со спутником — МОГ переходит в автономный режим, но продолжает получать данные от своих бойцов. Если RF-датчик «оглох» из-за мощных помех — радар и акустика всё ещё видят и слышат.

Сенсорная фузия в системе «Фрактал» — это не просто технический приём. Это философия: ни один датчик не является достаточным, но каждый — необходим. Радар видит первым. Акустика опознаёт. RF-датчик отличает своих от чужих. Тепловизор выносит окончательный вердикт. А децентрализованная mesh-сеть превращает разрозненные показания в коллективный разум, который не обмануть ни одной уловкой противника.

Глава 9. От облака к периферии — почему задержка недопустима

В предыдущих главах мы подробно разобрали, как работает каждый из четырёх сенсоров системы, как нейросети на NPU анализируют спектрограммы и как узлы обмениваются данными через самоорганизующуюся mesh-сеть. Но все эти технические решения подчинены одному главному императиву — времени. Именно время является тем ресурсом, которого в войне дронов всегда не хватает, и именно оно диктует фундаментальный выбор архитектуры: обработка данных должна происходить на периферии, а не в облаке.

Критичность времени: дрон пролетает километр за 10 секунд

Чтобы понять, почему задержка в системе обнаружения и поражения неприемлема, достаточно посмотреть на цифры. Современные ударные беспилотники — это не медлительные аппараты, зависающие над полем боя. Это стремительные машины, способные пересекать охраняемое пространство быстрее, чем оператор успевает моргнуть.

Возьмём для примера реальные данные 2026 года. Российские реактивные дроны серии «Герань-3» развивают скорость 300–330 км/ч. Их преемник, «Герань-4», разгоняется уже до 450–500 км/ч, а «Герань-5» до 600 км/ч. Дроны-пере-

хватчики, создаваемые для борьбы с ними должны достигать скорости не менее более 750 км/ч. Это не гоночные рекорды и не лабораторные эксперименты — это боевая реальность.

Теперь переведём эти цифры в понятные категории. При скорости 360 км/ч (ровно 100 метров в секунду) дрон преодолевает один километр за 10 секунд. При 500 км/ч (около 140 м/с) тот же километр занимает всего 7 секунд.

Семь-десять секунд — это время, за которое дрон, появившись на горизонте, достигает охраняемого объекта.

Это время, за которое система должна:

- обнаружить цель,
- классифицировать её,
- верифицировать угрозу,
- принять решение о поражении,
- выдать целеуказание средствам поражения.

Каждая потерянная миллисекунда приближает дрон к цели. Каждая задержка в обработке данных — это метры, которые дрон успевает пролететь.

Неприемлемость отправки «сырых» данных в центр

Теперь представим традиционный подход к обработке данных. Радар видит объект. Камера фиксирует изображение. Акустика записывает звук. Все эти «сырые» данные — видеопотоки, аудиофайлы, радарные отсчёты — отправляются по сети в облачный центр или на мощный сервер для обработки. Там нейросети анализируют информацию, при-

нимают решение и отправляют команду обратно.

Сколько времени это занимает?

Путь данных в облачной архитектуре:

1. Сбор данных на сенсоре — миллисекунды.

2. Передача по сети до ближайшего узла связи — зависит от типа сети. Спутниковый канал — десятки миллисекунд. Наземная сеть — единицы-десятки миллисекунд.

3. Маршрутизация и передача в облачный дата-центр — может составлять от 10 до 100 и более миллисекунд в зависимости от удалённости.

4. Обработка в облаке — даже при самых быстрых инстансах загрузка модели, предобработка данных и инференс занимают десятки-сотни миллисекунд.

5. Передача ответа обратно — ещё одна задержка, сопоставимая с передачей запроса.

6. Исполнение команды на средстве поражения — дополнительные миллисекунды.

Даже в идеальных условиях, с выделенным каналом и мощным облачным вычислителем, совокупная задержка редко опускается ниже 200–300 миллисекунд. В реальных условиях — с перегруженными сетями, помехами или проблемами на стороне провайдера — задержка легко вырастет до секунд.

Для веб-приложения секунда — это неприятно, но терпимо. Для системы перехвата дрона секунда — это 100–140 метров, которые цель успела пролететь. А за три секунды за-

держки дрон преодолевает уже почти полкилометра.

Но проблема не только в задержке. Облачная архитектура страдает от трёх фундаментальных пороков:

Первый — зависимость от связи. В условиях активных помех, боевых действий или просто сложного рельефа местности связь может быть нарушена. Прервался канал — система ослепла. Облачный центр не получил данных — решения нет.

Второй — уязвимость центра. Облачный дата-центр или штабной сервер — это единая точка отказа. Вывели его из строя — и вся система рухнула. В условиях войны это не гипотетическая угроза, а повседневная реальность.

Третий — стоимость передачи данных. Видеопотоки с тепловизоров, высокочастотные отсчёты радаров, многоканальные аудиозаписи — всё это создаёт колоссальный трафик. Передавать такие объёмы данных в облако в реальном времени дорого, а в условиях ограниченной полосы пропускания — часто просто невозможно.

Периферийная обработка: решение на месте

Именно поэтому в нашей системе обработка данных происходит на месте — непосредственно на каждом узле сети.

Вот как выглядит та же цепочка в архитектуре «Фрактал»:

1. Сбор данных на сенсоре — миллисекунды.
2. Обработка на NPU того же узла — инференс лёгкой свёрточной нейросети занимает миллисекунды. Современ-

ные NPU способны выполнять квантованные модели INT8 с частотой 10–30 Гц, то есть каждые 33–100 миллисекунд выдавая новый результат.

3. Формирование трека — MCU упаковывает результат в компактное сообщение размером 50–100 байт (координаты, тип, уровень доверия).

4. Передача по mesh-сети — несколько миллисекунд до соседних узлов.

Вся цепочка от момента, когда звук достиг микрофона или радиоволна отразилась от дрона, до момента, когда решение сформировано и передано в сеть, укладывается в десятки миллисекунд. Без интернета. Без облака. Без зависимости от дата-центра за сотни километров.

Для сравнения: исследования показывают, что периферийные архитектуры существенно превосходят облачные как по задержке, так и по пропускной способности. Обработка на границе сети сокращает среднюю задержку инференса почти на 87% по сравнению с облачными подходами. И это не говоря о том, что периферийная обработка вообще не требует передачи «сырых» данных — в сеть уходят только сжатые треки, а не гигабайты видео и аудио.

Что мы выигрываем

Переход от облачной к периферийной архитектуре даёт системе три критических преимущества:

Скорость. Задержка сокращается с сотен-тысяч миллисекунд до десятков. Дрон, летящий на скорости 500 км/ч, за

это время успевает пролететь всего несколько метров вместо сотен. Система получает возможность реагировать на угрозу до того, как она достигнет охраняемого объекта, а не после.

Автономность. Каждый узел работает независимо. Если связь с «внешним миром» потеряна — узлы продолжают обнаруживать, классифицировать и передавать треки внутри mesh-сети. МОГ продолжает принимать решения и поражать цели. Система не парализуется обрывом кабеля или глушением спутникового сигнала.

Эффективность. Вместо передачи терабайтов «сырых» данных по дорогим и узким каналам связи узлы обмениваются только метаданными — компактными треками размером в десятки байт. Это позволяет сети работать даже при минимальной пропускной способности и делает её нечувствительной к перегрузкам.

Где облако всё-таки нужно

Сказанное не означает, что облачные вычисления в системе «Фрактал» не используются вовсе. Они есть — но на совершенно другом уровне.

В нашей фрактальной архитектуре обработка на периферии отвечает за тактические решения: «есть ли дрон?», «какой это тип?», «куда он летит?», «открывать ли огонь?». Это решения, которые должны приниматься за миллисекунды, на месте, без оглядки на внешние каналы.

Облачные же мощности (или, что более реалистично в боевых условиях, вычислительные ресурсы вышестоящего

штаба) отвечают за стратегические задачи: обучение и обновление нейросетевых моделей, анализ общей воздушной обстановки на огромной территории, координация между несколькими МОГ, интеграция с данными от других родов войск.

Эти задачи не критичны ко времени в том же смысле. Обновлённая модель может быть распространена по сети в течение минут или даже часов — это не снижает боеспособности системы, потому что старые модели продолжают работать. Анализ общей обстановки может выполняться с задержкой в несколько секунд — это всё равно даёт штабу понимание картины боя.

Главный принцип нашей архитектуры можно сформулировать так: данные обрабатываются там, где они возникают, а в облако уходит только то, что действительно требует облака. Это не компромисс и не уступка обстоятельствам — это осознанный выбор, продиктованный физикой и логикой войны дронов.

Война дронов — это война миллисекунд. И в этой войне побеждает тот, кто обрабатывает данные быстрее, а не тот, у кого дата-центр мощнее. Именно поэтому каждый узел «Фрактала» — это не просто датчик, а полноценный вычислительный центр, способный мыслить самостоятельно, не оглядываясь на облако.

Глава 10. Нейронный процессор (NPU) как основа каждого узла

В предыдущих главах мы говорили о датчиках — радарах, микрофонах, RF-приёмниках. Но датчик без интеллекта — это просто источник сырых данных. Вопрос в том, где и как эти данные превращаются в решение. Традиционный подход — отправить всё в облако или на мощный сервер — в условиях войны дронов неприемлем. Связь может быть нарушена, задержка в секунду оборачивается поражённой целью, а централизованная обработка создаёт единую точку отказа.

В нашей системе ответ на этот вызов — нейронный процессор (NPU), установленный на каждом узле сети. Это не просто микросхема, а фундаментальное архитектурное решение, которое переносит «мозг» системы на периферию, туда, где рождаются данные.

Технические характеристики: производительность и энергопотребление

NPU — это специализированный чип, спроектированный для одной задачи: максимально быстро и энергоэффективно выполнять алгоритмы искусственного интеллекта. В отличие от универсального центрального процессора (CPU), который тратит такты на переключение контекстов и обслуживание периферии, NPU построен вокруг матричных умно-

жителей-аккумуляторов (МАС) — аппаратных блоков, которые выполняют миллиарды операций умножения и сложения за секунду, потребляя при этом доли ватта.

Что даёт NPU на практике.

Современные исследования показывают, что NPU обеспечивает ускорение до 5,2 раз по сравнению с CPU при инференсе свёрточных нейросетей (CNN). Для более сложных задач, таких как обработка больших языковых моделей, NPU достигает ускорения до 4 раз на этапе префилла. Но главное — не просто скорость, а энергоэффективность: гибридные реализации NPU + GPU превосходят CPU-решения как по задержке, так и по энергопотреблению.

Ключевые требования к NPU в нашей системе:

- Производительность: достаточная для инференса лёгкой 2D свёрточной нейросети размером 5 МБ с частотой 10–30 Гц. Это означает, что каждый узел способен обрабатывать данные с датчиков десятки раз в секунду — в реальном времени.

- Поддержка квантованных моделей (INT8): квантование — это техника сжатия нейросетей, при которой веса модели хранятся в 8-битных целых числах вместо 32-битных чисел с плавающей запятой. Это уменьшает размер модели в 4 раза и кратно ускоряет вычисления на NPU.

- Объём встроенной памяти для весов: не менее 10 МБ — достаточно для хранения нескольких свёрточных моделей одновременно.

- Энергопотребление в режиме активной обработки: 1 Вт. Это критическое требование. Узел-боец должен работать автономно от аккумулятора часами, а в некоторых сценариях — сутками. Для сравнения: современные NPU для встраиваемых систем, такие как Axon NPU от Nordic Semiconductor, потребляют в активном режиме около 2,7–3,5 мА, а некоторые ультранизкопотребляющие решения, как BrainChip Akida Pico, — менее 1 милливатта.

- Возможность работы в связке с MCU по SPI или общей шине.

Эти характеристики делают NPU идеальным «мозгом» для каждого сенсорного узла. Он не требует массивного охлаждения, не сажает батарею и при этом способен выполнять сложный анализ данных за миллисекунды.

Обработка спектрограмм вместо видеокадров — экономия ресурсов в десятки раз

Ключевой вопрос: что именно обрабатывает NPU? На первый взгляд, логичнее всего было бы анализировать «сырые» сигналы с датчиков — видеопоток с тепловизора или временные ряды с радара. Но этот путь ведёт в тупик.

Обработка полноценного видеокадра — это вычислительно дорогая операция. Она требует обработки миллионов пикселей, работы с цветом, яркостью, контрастностью. Даже на мощном NPU такой анализ потребляет ватты энергии и занимает десятки миллисекунд. Для системы, где каждый узел должен работать от батареи, это неприемлемо.

Вместо этого наша система анализирует спектрограммы — визуальные представления сигналов в частотно-временной плоскости. Это принципиально иной подход, который даёт колоссальный выигрыш в эффективности.

Почему спектрограмма эффективнее видеокадра:

1. Размер данных. Спектрограмма размером 128×128 точек — это 16 384 значения. Видеокадр в разрешении 640×480 — это 307 200 пикселей, каждое из которых может содержать три цветовых канала. Спектрограмма меньше видеокадра в десятки раз.

2. Информационная плотность. Спектрограмма — это не просто «картинка». Каждая её точка несёт физически значимую информацию: частота и время сигнала. Нейросеть, обученная на спектрограммах, учится распознавать именно паттерны сигнала, а не случайные визуальные артефакты.

3. Энергопотребление. Обработка спектрограммы требует в десятки раз меньше операций MAC, чем обработка видеокадра. А значит — и энергии. Экспериментальные данные показывают, что построение Mel-спектрограммы на NPU может занимать всего 0,015 секунды (15 миллисекунд) при использовании оптимизированных MLIR-ядер. Это в 20 раз быстрее, чем на CPU.

4. Универсальность. Спектрограмма — это универсальный формат. Звук, радарный сигнал, RF-излучение — все эти разнородные данные могут быть представлены в виде спектрограмм и обработаны одной и той же нейросетевой ар-

хитектурой. Это упрощает разработку и позволяет использовать одни и те же NPU на всех типах узлов.

Именно поэтому в нашей системе NPU не анализирует «сырые» данные. Вместо этого MCU собирает данные с датчиков, строит спектрограмму и передаёт её на NPU. NPU прогоняет спектрограмму через лёгкую свёрточную нейросеть и за миллисекунды выдаёт результат: есть ли дрон, какой у него тип и насколько система уверена в этом решении.

Примеры моделей: Mel-спектрограмма для звука

Звук — это колебания воздуха. Человеческое ухо воспринимает их как громкость и высоту тона. Но для машины звук — это просто последовательность чисел — отсчётов амплитуды во времени. Чтобы превратить эту последовательность в то, что «понимает» нейросеть, используется Mel-спектрограмма.

Что такое Mel-спектрограмма.

Mel-спектрограмма — это визуальное представление звукового сигнала, где:

- Ось X — время.
- Ось Y — частота, но не в линейной шкале (герцы), а в Mel-шкале, которая отражает нелинейное восприятие частоты человеческим ухом.
- Цвет или яркость каждой точки — амплитуда сигнала на данной частоте в данный момент времени.

Почему именно Mel-шкала? Человеческий слух гораздо лучше различает низкие частоты, чем высокие. Mel-шкала

построена так, чтобы отражать это свойство: она «растягивает» низкие частоты и «сжимает» высокие. Нейросеть, обученная на Mel-спектрограммах, «слышит» звук так же, как его слышит человек, но с гораздо большей детализацией и без усталости.

Как это работает в системе.

Когда акустический датчик (микрофонная решётка) фиксирует звук, MCU буферизует аудиопоток с частотой дискретизации 44,1 кГц. Затем он разбивает его на короткие фреймы (обычно по 25–50 миллисекунд), для каждого фрейма вычисляет спектр мощности и преобразует его в Mel-шкалу. Результат — Mel-спектрограмма размером, например, 128×128 точек.

Эта спектрограмма подаётся на вход NPU, где работает лёгкая свёрточная нейросеть (CNN). Модель обучена на миллионах аудиосэмплов — звуках различных типов дронов, птиц, автомобилей, строительной техники, голосов и других городских шумов.

Результаты впечатляют. Современные CNN-классификаторы на основе Mel-спектрограмм достигают точности обнаружения дронов 98,23% и точности идентификации типа дрона 95,39%. Это означает, что из ста пролетающих дронов система не пропустит почти ни одного, а из ста правильно обнаруженных — правильно определит тип в 95 случаях.

В условиях реального боя, где на кону — жизни и инфраструктура, эти цифры означают, что акустический канал ста-

новится не просто «вспомогательным», а полноценным и надёжным источником информации.

Примеры моделей: микродоплеровский профиль для радара

Радар видит не «картинку», а отражённый радиосигнал. Когда этот сигнал отражается от движущегося объекта, его частота меняется — это эффект Доплера. Но если объект не просто движется, а вращается (например, винты дрона), то в отражённом сигнале появляются дополнительные частотные компоненты — микродоплеровские составляющие.

Что такое микродоплеровский профиль.

Микродоплеровский профиль — это спектрограмма радарного сигнала, которая показывает, как частота отражённого сигнала меняется во времени. Для дрона этот профиль имеет характерный вид: периодические колебания, соответствующие вращению лопастей винтов. Для птицы — совсем другой паттерн: машущие крылья создают иной микродоплеровский «почерк».

Именно это различие позволяет нейросети отличить дрон от птицы — задача, с которой классические радары справляются крайне плохо.

Как это работает в системе.

Радарный сенсор на узле излучает когерентный сигнал (обычно в миллиметровом диапазоне, около 60 ГГц) и принимает отражённый сигнал. MCU оцифровывает принятый сигнал, выделяет доплеровский сдвиг и строит микродопле-

ровскую спектрограмму — изображение, где по горизонтали отложено время, по вертикали — доплеровская частота, а яркость показывает мощность сигнала.

Эта спектрограмма подаётся на NPU, где работает лёгкая CNN, обученная на размеченных микродоплеровских профилях различных объектов: квадрокоптеры с разным числом лопастей, самолёты, птицы, наземный транспорт.

Современные исследования показывают, что такой подход даёт впечатляющие результаты. Одна из последних работ демонстрирует точность классификации 96,8% для много-роторных БПЛА с использованием микродоплеровских сигнатур и нейросетей с двойными потоками внимания. Другие исследования подтверждают, что микродоплеровские сигнатуры — это «уникальный способ характеристики движения летящих объектов на основе их радиолокационных отражений».

Более того, существуют специализированные лёгкие нейросети, такие как ECM Net, разработанные именно для классификации микродоплеровских сигналов в сложных сценариях. Эти модели специально оптимизированы для работы на периферийных устройствах с ограниченными вычислительными ресурсами — идеально для нашего NPU.

Почему это критично.

Именно микродоплеровский анализ позволяет системе видеть дрон даже тогда, когда он «молчит» (не излучает радиосигналов) и когда он скрыт туманом или ночью. Радар

видит движущийся объект, NPU анализирует его микродоплеровский профиль и определяет: это дрон или птица. И делает это за миллисекунды, потребляя доли ватта.

Синтез: NPU как универсальный классификатор

Объединяя сказанное, мы получаем картину: NPU на каждом узле — это универсальный классификатор спектрограмм.

- От акустического датчика он получает Mel-спектрограмму — и определяет, какой дрон «шумит» поблизости.
- От радара он получает микродоплеровскую спектрограмму — и отличает дрон от птицы.
- От RF-датчика он получает спектрограмму частотно-временного распределения сигнала — и идентифицирует тип управления.

Все эти задачи решаются одной и той же аппаратной платформой (NPU) и одним и тем же классом алгоритмов (лёгкие свёрточные нейросети). Различаются только входные данные и обученные веса моделей.

Это архитектурное единообразие даёт колоссальные преимущества:

- Унификация производства: все узлы используют одинаковые NPU.
- Гибкость: при необходимости NPU можно перепрошить для решения новых задач.
- Масштабируемость: добавление нового типа датчика не требует изменения аппаратной платформы — достаточно

обучить новую модель и загрузить её в NPU.

И главное — скорость. NPU работает на периферии, там, где рождаются данные. Решение принимается за миллисекунды, без отправки данных в облако, без задержек связи, без риска потерять связь с центром. Это и есть «интеллект на границе» — основа децентрализованной сети, которая видит, слышит и понимает быстрее, чем противник успевает нанести удар.

Глава 11. Локальное принятие решений

Представьте себе организм, у которого каждый нерв способен не просто передавать сигнал, а самостоятельно анализировать ситуацию и принимать элементарные решения. Именно так устроена наша сеть — каждый узел-«боец» обладает собственным «интеллектом» на борту, который позволяет ему не быть просто пассивным датчиком, а стать активным участником коллективного разума.

Это кардинально меняет логику работы системы. Вместо того чтобы гнать в центр управления терабайты «сырых» данных — аудиопотоки, радарные эхо, RF-спектры — каждый узел самостоятельно решает, что именно он видит и слышит, и передаёт в сеть только сжатую, осмысленную информацию. Это не просто экономия трафика. Это вопрос выживания системы в условиях, когда связь может быть нарушена, а каждая миллисекунда задержки стоит поражённой цели.

Что вычисляет NPU на узле-бойце

Нейронный процессор на каждом узле-бойце решает три последовательные задачи: детекцию, классификацию и оценку уровня доверия. Вся цепочка занимает миллисекунды и выполняется без участия внешних вычислительных ресурсов.

Детекция: есть ли вообще что-то?

Первая и самая фундаментальная задача — бинарный ответ на вопрос «дрон или не дрон?». NPU получает на вход спектрограммы от трёх типов датчиков: Mel-спектрограмму звука от акустической решётки, микродоплеровский спектр от радара и частотно-временную спектрограмму от RF-датчика. Каждая из них — это двухмерное изображение, где по одной оси отложено время, по другой — частота, а яркость или цвет отражают интенсивность сигнала.

Для акустического канала это могут быть нормализованные log-mel-спектрограммы с 64 mel-полосами, построенные на окнах в 1.0 секунды при частоте дискретизации 16 кГц. Для радарного канала — микродоплеровские спектрограммы, отражающие тончайшие изменения частоты отражённого сигнала, позволяющие отличить вращающийся винт дрона от машущего крыла птицы. Для RF-канала — спектрограммы, фиксирующие кратковременные всплески радиоизлучения.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.