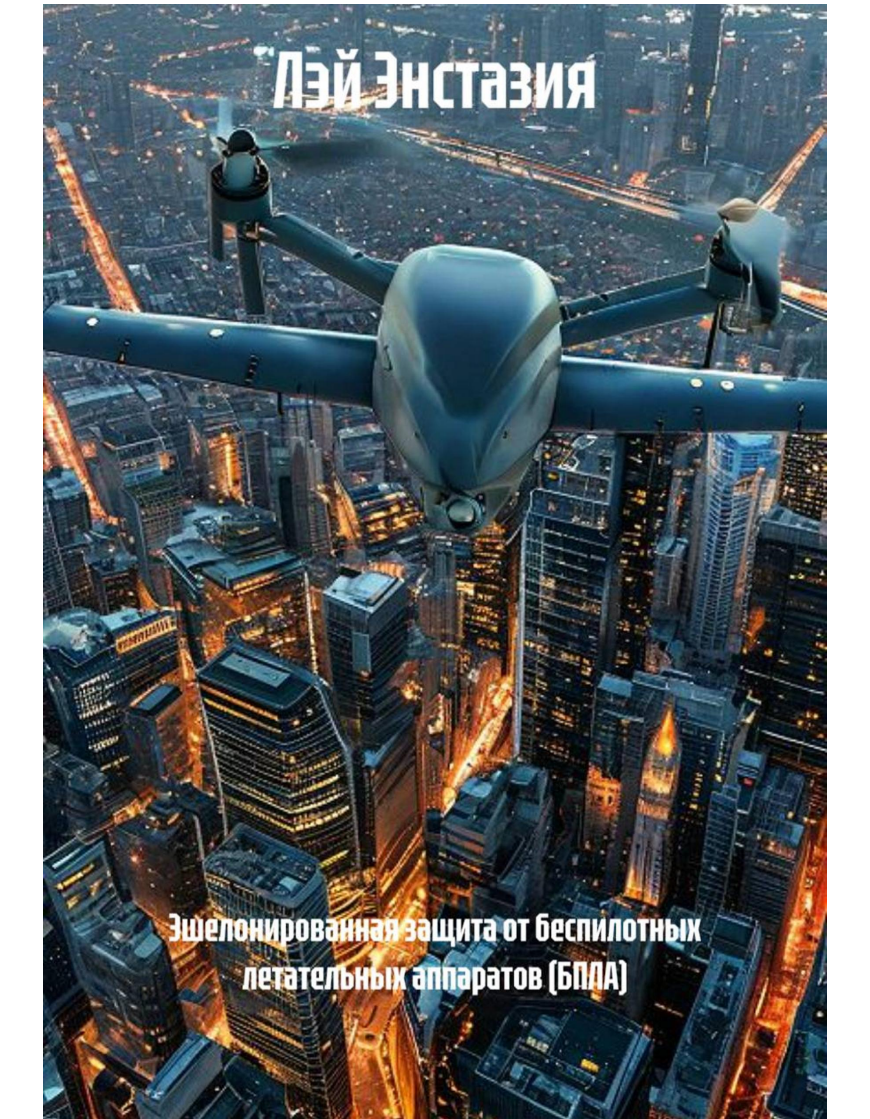


Дэй Энстазия

A large white quadcopter drone is shown from a high-angle perspective, flying over a dense urban landscape at night. The drone's four rotors are visible, and its body is illuminated. Below it, the city is a complex grid of skyscrapers and streets, all glowing with warm yellow and orange lights. The overall scene conveys a sense of high-tech surveillance or defense.

Эшелонированная защита от беспилотных
летательных аппаратов (БПЛА)

Лэй Энстазия

Эшелонированная защита от беспилотных летательных аппаратов (БПЛА)

<https://litres.ru/74294982>

SelfPub; 2026

Аннотация

Книга аналитика по противодействию БПЛА (2026) — это не просто обзор средств борьбы с дронами, а манифест новой военной философии. Автор убедительно доказывает: «серебряной пули» не существует. Современный беспилотник — это «летающий компьютер», эволюционирующий быстрее, чем создаются системы защиты. В работе детально разобраны все уровни эшелонированной обороны: от обнаружения (РЛС, оптика, акустика, RF-сканеры) до нейтрализации (РЭБ, кибератаки, кинетика, лазеры, СВЧ-оружие). Особое место уделено нетрадиционным решениям — от «арканов» и танковой «картечи» до хищных птиц и собак. Автор подчёркивает решающую роль экономики: тратить миллионную ракету на дешёвый FPV-дрон — значит проигрывать войну на истощение. Главный вывод: противодронная оборона — это не статичный набор устройств, а живой процесс, где гибкость, скорость и

слаженность важнее технологического превосходства. Побеждает не оружие — побеждает система.

Содержание

Введение. Экономика, время и ошибка: три столпа поражения при «одном решении»	5
Глава 1. Эшелонированная защита как философия системности	15
Глава 2. Обнаружение и идентификация — глаза, уши и разум системы	28
Глава 3. РЭБ как интеллектуальная экосистема	43
Глава 4. Отечественные и зарубежные комплексы РЭБ	57
Конец ознакомительного фрагмента.	67

Лэй Энстазия Эшелонированная защита от беспилотных летательных аппаратов (БПЛА)

Введение. Экономика, время и ошибка: три столпа поражения при «одном решении»

Это введение не для слабонервных. Оно требует честности с самим собой, готовности признать ошибки и пересмотреть догмы. Но я верю, что мы способны на это. Потому что у нас нет другого выбора. Война с дронами — это война на истощение, но истощение касается не только материальной части. Она касается нашего разума, нашей воли, нашей способности учиться. И если мы освоим этот урок — экономический, временной и когнитивный, — мы не просто выживем. Мы победим.

В войне с дронами есть три столпа, на которых держится

поражение, если мы продолжаем искать одно решение. Их невозможно обойти, их нельзя игнорировать, и каждое из них — это не просто техническая проблема, а философский вызов. Экономический разрыв, временной фактор и ошибка мышления. В этом разделе я разберу их безжалостно и откровенно, потому что только признав их, мы сможем вырваться из порочного круга.

Экономический разрыв: почему нерационально тратить миллион на перехват дешёвого аппарата

Когда я впервые увидел в сводках, что наш FPV-дрон «Упырь» стоимостью всего 350 долларов превратил в пылающий металлолом американский танк «Abrams», оценённый в 8 миллиона долларов, я не испытал удивления. Я испытал чувство глубокого удовлетворения — я знал, что это произойдёт, ещё за год до того, как это случилось. И дело не в том, что западная техника плоха. Дело в том, что экономика войны навсегда перевернулась, и теперь счёт идёт не на миллионы, а на тысячи. Мы первыми поняли это — и первыми начали побеждать по-новому.

Возьмите любую классическую войну XX века. Там стоимость уничтожения цели всегда была сопоставима со стоимостью самой цели, плюс-минус порядок. Зенитная ракета стоила как самолёт, которым она стреляла. Артиллерийский

снаряд — как доля стоимости укрепления. Экономический баланс позволял вести длительные кампании, потому что ресурсы расходовались пропорционально угрозе.

Теперь посмотрите на дронную войну. Противник производит FPV-дроны десятками тысяч штук в месяц. Западные технологии сделали компоненты доступными до смешного — контроллеры полёта, видеопередатчики, бесколлекторные двигатели — всё это продаётся на AliExpress и Amazon по цене обеда в ресторане. И каждый такой аппарат может нести боевую часть весом до полутора килограммов, чего достаточно, чтобы пробить крышу любой бронемашины.

А что мы противопоставляем? Зенитную ракету с лазерным наведением, в которой используются драгоценные металлы, сложнейшие микросхемы и тонны высокоточного топлива. Её производство занимает месяцы и требует высококвалифицированных специалистов. В результате мы имеем разрыв в 40–100 раз. И это не просто «невыгодно». Это катастрофа, потому что противник может позволить себе потерять сотню дронов, чтобы вынудить нас израсходовать десяток ракет. Он истощает нас не ударами, а самой арифметикой.

Я часто вспоминаю разговор с командиром зенитного дивизиона, который признался: «Мы сбиваем по 15–20 дронов в день. На каждую цель — одна ракета. Я уже запросил дополнительный боезапас четыре раза за месяц. Начальство начинает злиться. А что мне делать? Если я не собою их, они

разнесут аэродром». Он был в отчаянии, и я понимал его. Но я знал, что на том конце линии противник едва заметно улыбается, когда видит наши отчёты.

Решение лежит не в создании ещё более мощной и дорогой ракеты. Оно лежит в переходе на пропорциональное поражение. Мы должны научиться сбивать дешёвый дрон дешёвым же способом — дробовиком, «арканом», сеткой, акустической ловушкой. А дорогие средства — лазеры, СВЧ-импульсы, управляемые ракеты — оставлять только для действительно ценных целей, таких как стратегические разведчики или ударные БПЛА дальнего действия. Экономия должна стать не просто пунктом инструкции, а рефлексом командира на всех уровнях.

Временной фактор: цикл разработки средств защиты в разы длиннее цикла обновления дронов противника

Теперь давайте поговорим о времени. Я помню, как в 2020 году мы рассматривали проект нового комплекса РЭБ для защиты аэродромов. Полный цикл — от ТЗ до серийного образца — был заложен в пять лет. Тогда это казалось разумным: самолёты не менялись десятилетиями, системы ПВО стояли на вооружении по 20–30 лет. Но уже через два года, когда в зоне СВО начали массово применять FPV-дроны с псевдослучайной перестройкой частоты, наш «пятилетний»

комплекс оказался устаревшим даже до того, как его первый опытный образец вышел на полигон.

В чём суть проблемы? Разработка средств защиты — это тяжёлая, инерционная машина. Она требует сертификации, испытаний, утверждения стандартов, согласования с десятками инстанций. Это необходимо для надёжности, но цена этой надёжности — скорость. А дроны не ждут. Они развиваются семимильными шагами. Взять хотя бы оптоволокно: в начале 2024 года оно было экзотикой, а к концу года противник выпускал тысячи таких аппаратов в месяц. Мы не могли предсказать это при запуске наших РЭБ-проектов в 2021–2022 годах.

Более того, дроны меняются не только технически, но и тактически. Сегодня они летают поодиночке, завтра — роями с ИИ-координацией, послезавтра — в связке с наземными дронами и морскими беспилотниками. Это не просто «модернизация» — это смена парадигмы каждые полгода. И когда ваш комплекс РЭБ, заказанный три года назад, наконец поступает в войска, вы с ужасом понимаете, что он борется с угрозами вчерашнего дня, а противник уже использует частоты и протоколы, которых нет в его базах данных.

Как с этим бороться? Я вижу только один выход — сократить цикл «решение-внедрение» до минимума. Перейти на модульные архитектуры, где можно менять блоки и прошивки без пересмотра всей конструкции. Использовать гражданские технологии и компоненты с открытыми протоколами,

чтобы быстро адаптироваться к новым частотным диапазонам. Внедрить практику «боевой доработки» прямо на передовой, когда инженеры выезжают в части, общаются с операторами и через неделю выдают обновлённую версию. И главное — перестать мыслить категориями «финального продукта». Система РЭБ не должна быть статичной коробкой. Она должна быть как организм, который дышит, эволюционирует и учится на каждом пролёте вражеского дрона.

**Ошибка мышления: мы пытаемся решить
проблему средствами прошлого века,
тогда как противник мыслит алгоритмами**

Это, пожалуй, самый болезненный пункт. Потому что он касается не денег и не времени — он касается нас самих, нашего мировоззрения. Я часто вижу, как наши лучшие инженеры рассуждают о дронах в терминах баллистики и радиолокации. Они спрашивают: «Какая у него скорость? Какой радиолокационный профиль? Какой поражающий фактор?» Но эти вопросы уже вчерашний день. Противник мыслит иначе — он мыслит потоками данных, нейронными сетями, алгоритмами распознавания и оптимизации маршрутов.

Я видел, как один из наших разработчиков с гордостью рассказывал о системе подавления, которая создаёт помехи на всех частотах, занятых дронами. Я спросил: «А что, если

дрон вообще не использует радиосигналы?» Он пожал плечами: «Тогда мы его не заглушим». Но ведь это же не ответ! Это признание, что мы загнали себя в угол. Мы по-прежнему считаем, что дрон — это объект, который надо «заглушить» или «сбить», как самолёт. А он — это компьютер, который решает задачу доставки боеприпаса в точку. И если мы не можем заблокировать его связь, мы должны атаковать его алгоритмы, его сенсоры, его логику принятия решений.

Посмотрите на FlyTrap, описанный в этой книге. Это не оружие в классическом смысле. Это узор на зонте, который заставляет нейросеть дрона ошибиться. Или спуфинг GPS, который выдаёт ложные координаты, но не глушит сигнал, а имитирует его. Или кибератака, которая внедряет вредоносный код в прошивку дрона ещё на земле. Все эти методы требуют совсем иного склада ума — не инженерного, а скорее хакерского. Мы должны научиться видеть в дроне систему, а не мишень.

Но самое страшное, что эта ошибка мышления пронизывает не только разработку, но и тактику. Наши командиры по-прежнему мыслят эшелонами и рубежами, тогда как противник мыслит сетями и узлами. Они не пытаются прорвать оборону в лоб — они ищут уязвимости в логистике, в управлении, в психологии. И побеждают они не потому, что у них лучше дроны, а потому, что они быстрее перестраивают свои алгоритмы под нашу оборону.

Поэтому я убеждён: чтобы победить в дроновой войне, мы

должны изменить свой язык. Перестать говорить «сбить», начать говорить «нейтрализовать». Перестать говорить «защитить», начать говорить «адаптироваться». Перестать говорить «победить», начать говорить «выжить и научиться». Только тогда мы сможем смотреть на проблему глазами противника и предвосхищать его следующий ход.

Наглядная модель: «гонка вооружений со смещённым финишем» — мы догоняем, а цель убегает быстрее

Когда я пытаюсь визуализировать нашу ситуацию, я представляю забег, где финишная черта постоянно движется вперёд со скоростью, превышающей нашу максимальную. Мы бежим изо всех сил, разрабатывая новые комплексы, закупая оборудование, обучая специалистов. Но каждый раз, когда мы приближаемся к «финишу» — то есть к моменту, когда нам кажется, что мы наконец-то закрыли небо, — противник просто сдвигает черту, выпуская дроны нового поколения. Это не просто игра с постоянным отставанием. Это игра, где само понятие «догнать» теряет смысл.

Возьмите любой временной срез. В 2023 году мы считали себя защищёнными от коммерческих квадрокоптеров. Противник перешёл на FPV с ППРЧ. Мы модернизировали РЭБ — он перешёл на оптоволокно. Мы начали использовать дроны-перехватчики — он внедрил машинное зрение

и автономное наведение. Мы разработали лазеры — он стал применять туман и дымовые завесы. Мы создали СВЧ-пушки — он перешёл на микродроны, которые сложнее засечь и зафиксировать. И так до бесконечности.

Главная опасность этой модели не в том, что мы «отстаём». Опасность в том, что мы тратим колоссальные ресурсы на закрытие уже пройденных этапов, вместо того чтобы перепрыгнуть через них. Мы пытаемся решить частную задачу, тогда как противник решает системную. Он не «улучшает» дроны — он меняет архитектуру войны. Мы же продолжаем дорабатывать старые инструменты, надеясь, что они снова станут эффективны.

Как разорвать этот круг? Единственный способ — перестать играть по его правилам. Не пытаться догнать в той же гонке, а изменить саму гонку. Перейти от реакции к упреждению. Вместо того чтобы разрабатывать защиту от конкретного типа дронов, строить систему, которая не зависит от типа — например, интеллектуальную сеть обнаружения, где любое воздушное движение фиксируется и анализируется, и затем автоматически выбирается наиболее эффективный способ нейтрализации. Или создавать средства, которые действуют не против дрона, а против его оператора, его логистики, его производства. Это уже совсем другой уровень мышления.

Я не предлагаю лёгких ответов. Я лишь констатирую факт: пока мы бежим за убегающим финишем, мы обречены на

вечное отставание. Единственный шанс — перестать бежать за ним и начать бежать к своей собственной цели. К цели, где победа измеряется не сбитыми дронами, а количеством сорванных атак, сохранённых жизней и сбережённых ресурсов. Это более сложная, более амбициозная задача, но именно она стоит перед нами.

Глава 1. Эшелонированная защита как философия системности

Когда я впервые увидел, как FPV-дрон влетает в боевую машину, я понял, что весь мой предыдущий опыт — двадцать лет работы в сфере военных технологий — в одночасье обесценился. Не потому, что я чего-то не знал. А потому, что правила игры изменились так быстро и так радикально, что старые знания стали не просто бесполезными — они стали опасными. Они создавали иллюзию защищённости там, где защищённости не было.

Тот дрон стоил меньше, чем хороший смартфон. Он был собран в гараже из доступных компонентов. И он уничтожил технику стоимостью в несколько миллионов долларов. Это был не просто боевой эпизод. Это был сигнал. Сигнал о том, что война, какой мы её знали, закончилась. И началась другая.

От монолита к системе: почему нельзя победить дроны одним методом

В 2016 году, когда дроны только начинали появляться на полях сражений, военные эксперты всего мира искали «серебряную пулю». Что-то одно. Универсальное. Гарантиро-

ванное.

Сначала такой «пулей» объявили радиоэлектронную борьбу. «Мы просто заглушим их сигнал, и они упадут», — говорили оптимисты. И поначалу это работало. Против коммерческих квадрокоптеров DJI, которые летали на стандартных частотах, РЭБ была эффективна. Мы создавали «цифровые купола», превращали целые районы в «чёрные зоны» для спутниковой навигации. Мы гордились комплексами «СЕРП» и «Двина-100М».

Но противник оказался умнее. Прошло несколько месяцев, и на поле боя появились дроны, работающие на частотах, которые никто не ожидал. Потом — дроны с псевдослучайной перестройкой частоты. Потом — оптоволоконные дроны, которые физически не излучали сигналов, а значит, наши дорогостоящие станции РЭБ превращались в бесполезный металлолом.

Мы попытались перехватить инициативу. Разработали лазеры. Они работали быстро — за доли секунды. Но пришёл туман, и лазеры стали бесполезны. Мы сделали микроволновые пушки, которые выжигали электронику целых роёв. Но они требовали огромной энергии и тоже боялись дождя. Мы усилили кинетику — дроны-перехватчики, специализированные патроны, сетки. Но рой из пятидесяти дешёвых FPV-дронов всё равно прорывался.

И в какой-то момент я понял то, что должно было быть очевидно с самого начала.

Не существует одного средства, которое могло бы эффективно бороться со всем многообразием дроновых угроз.

Почему? Потому что современный БПЛА — это не просто «летающая бомба». Как справедливо отметил генеральный конструктор Центра комплексных беспилотных решений Кузякин, дрон — это «летающий компьютер», обладающий собственной операционной системой, IP-адресом, набором сервисных программ и каналами связи. Против такого противника бессмысленно применять одно средство. Дрон, неуязвимый для РЭБ (например, на оптоволоконном управлении), может быть уязвим для кинетического поражения. Дрон, защищённый от стрелкового оружия бронёй, может быть ослеплён лазером. Рой дронов, против которого бессильны точечные средства, может быть «накрыт» микроволновым импульсом.

Как справедливо подчёркивает западный военный эксперт Пол Стелтинг из компании Moog: «There is not a magic bullet» — нет волшебной пули. Ни одно средство не является достаточным. Противодронная оборона должна быть адаптируемой, доступной по цене и масштабируемой.

Именно поэтому современная противодронная оборона строится на комплексном (эшелонированном) подходе, где методы существуют не вместо, а вместе друг с другом, образуя многослойную систему. Как отмечается в одном из аналитических обзоров, «эффективные контр-дронные операции — это не решение одной "серебряной пули", а много-

уровневый, интегрированный подход "системы систем"».

Природа угрозы как двигатель эшелонирования

Теперь давайте поговорим о том, что на самом деле движет необходимостью эшелонирования. Это не просто теоретическое предпочтение. Это жёсткая необходимость, продиктованная самой природой угрозы.

Многообразие типов БПЛА

Когда я слышу, как люди говорят о «дронах» как о чём-то однородном, я испытываю почти физическую боль. Это всё равно что называть «автомобилями» и гоночный болид, и грузовик, и детскую коляску.

Современный БПЛА — это целая вселенная угроз. Коммерческие квадрокоптеры, FPV-дроны-камикадзе, оптоволоконные аппараты, разведывательные БПЛА среднего радиуса, тяжёлые ударные дроны типа «Герань», рои, автономные аппараты с машинным зрением. Каждый из этих типов требует принципиально разных методов противодействия.

Маленькие дроны из неметаллических материалов уклоняются от радаров. Дроны на неизвестных частотах остаются невидимыми для RF-сканеров. Дроны с автономным наведением по машинному зрению не боятся глушения.

Экономический дисбаланс

Но есть и другой аспект — экономический. И он, возможно, даже важнее технического.

Дешёвый FPV-дрон стоимостью в несколько тысяч долларов заставляет государства тратить миллионы на средства противодействия. Как справедливо отмечается в одном из анализов, «expending a USD 100,000 interceptor missile to neutralise a USD 1,000 drone is an unsustainable economic model» — тратить ракету за 100 тысяч долларов на уничтожение дрона за 1000 долларов — это экономически несостоятельная модель.

Эшелонированный подход позволяет применять пропорциональное средство. Там, где достаточно «аркана» или дробовика, не тратить зенитную ракету. Там, где можно обойтись РЭБ, не использовать кинетику. Там, где достаточно спуфинга, не уничтожать дрон физически.

Эта экономическая логика пронизывает всю современную противодронную оборону. Как подчёркивает Дмитрий Дацыков, руководитель организационного комитета EXPO.UAV, механическая защита должна стать финальным рубежом эшелонированной обороны — «когда по той или иной причине все остальные средства не смогли остановить ударный беспилотник».

Скорость эволюции угрозы

И наконец, третий фактор — скорость. Дроны меняются быстрее, чем создаются средства борьбы с ними.

В начале 2023 года противник активно использовал коммерческие квадрокоптеры на стандартных частотах. К середине 2023 года появились FPV-дроны на новых частотах. К

концу года — дроны с алгоритмом «возврат на базу» при потере сигнала. Начало 2024 года — оптоволоконные аппараты. Сейчас мы наблюдаем массовое внедрение машинного зрения и автономного наведения.

Как справедливо отмечает генеральный конструктор Кузьякин, «дроны меняются очень быстро», а система противодействия должна «меняться в режиме онлайн адекватно скорости изменения атакующих дронов».

Эшелонированная архитектура, построенная на модульных и взаимозаменяемых компонентах, позволяет быстрее адаптироваться к новым тактикам противника. Если один уровень обороны становится неэффективным, другие продолжают работать. Если появляется новый тип угрозы, его можно встроить в существующую архитектуру без полной перестройки всей системы.

Структура эшелонированной обороны: вертикально-интегрированный подход

Теперь, когда мы поняли почему эшелонирование необходимо, давайте разберёмся, как оно устроено.

Эшелонированная противодронная оборона — это вертикально-интегрированная система, состоящая из нескольких последовательных уровней (эшелонов), каждый из которых решает свою задачу. Принципиально важно, что эшелоны не дублируют, а дополняют друг друга: если цель не поражена

на внешнем периметре, её перехватывает следующий уровень.

Генеральный директор компании «Рубеж-инжиниринг» Андрей Демидюк сформулировал это предельно ясно: «Эффективная оборона должна быть выстроена в глубину и по высоте, сочетая различные физические принципы работы».

Я представляю эту структуру как пирамиду или, если хотите, как матрёшку. Каждый следующий уровень — меньше по радиусу, но плотнее по концентрации средств.

Уровень 0: Обнаружение и идентификация (Разведка)

Это фундамент всей системы. Как справедливо указано в информационных документах: «Эффективное подавление невозможно без точного обнаружения». Без него все остальные методы теряют смысл.

Этот уровень включает радиолокационные станции (РЛС) для дальнего обнаружения, оптические датчики для визуального подтверждения, акустические системы для пассивного обнаружения в режиме радиомолчания и RF-сканеры для анализа радиочастотного спектра.

Ключевой тренд на этом уровне — внедрение искусственного интеллекта и нейросетей для автоматической классификации целей и снижения ложных срабатываний. Как отмечается в зарубежных источниках, «обнаружение и отслеживание являются краеугольным камнем технологий C-UAS».

Уровень 1: Радиоэлектронная борьба (РЭБ) и кибервоздействие

Это наиболее распространённый и постоянно развивающийся метод. Он включает подавление (глушение) каналов управления и навигации, спуфинг (подмена сигналов) и кибер-атаки — взлом бортового ПО дрона.

Современные комплексы, такие как «СЕРП-ВС13Д», работают на 13 частотах, создавая «купол безопасности» над объектом. Однако, как уже отмечалось, РЭБ бесполезна против дронов на оптоволокне или с автономным наведением по машинному зрению.

Уровень 2: Кинетическое (физическое) уничтожение

Это «традиционные» способы, которые гарантируют прекращение полёта цели. Стрелковое оружие, зенитные ракетные комплексы, дроны-перехватчики, сетки и сети.

Как подчёркивает Дмитрий Дацыков, механическая защита должна стать финальным рубежом эшелонированной обороны: «когда по той или иной причине все остальные средства не смогли остановить ударный беспилотник».

Уровень 3: Оружие направленной энергии

Это наиболее перспективное направление, находящееся на стыке РЭБ и кинетики. Лазерное оружие физически уничтожает или выводит из строя элементы дрона. Микроволновое (СВЧ) оружие генерирует мощный направленный импульс, вызывающий скачок напряжения и выгорание электроники. Ключевое преимущество СВЧ — площадное поражение, что делает его идеальным против роев дронов.

Уровень 4: Пассивная и физическая защита объекта

Это «последняя миля» обороны, защищающая сам объект. Бронирование, маскировка, создание ложных целей, дымовые завесы, стационарные сетчатые купола.

Тактико-организационный уровень: связующее звено

Эшелонированная защита — это не только технологии, но и организация. Мобильные огневые группы, единая цифровая сеть ПВО, автоматизированные системы поддержки принятия решений с ИИ, психологическая дезинформация.

Как отмечается в зарубежных источниках, «противодронная оборона лучше всего рассматривается как многоуровневая система принятия решений, а не как набор разрозненных датчиков и средств поражения».

Ключевые принципы: обнаружение классификация решение воздействие

Теперь, когда мы понимаем структуру, давайте поговорим о том, как эта структура работает в реальном времени.

Весь процесс противодронной обороны можно свести к четырём последовательным этапам. В западной военной терминологии это называется «kill chain» — цепочка поражения. В российском подходе — «обнаружение, классификация, решение, воздействие».

Этап 1: Обнаружение

Всё начинается с того, что система должна увидеть угрозу. Это самый критический этап, потому что без него все осталь-

ные бессмысленны.

Обнаружение ведётся по нескольким каналам одновременно. Радары видят на десятки километров, но могут пропустить маленький дрон на малой высоте. Акустические системы слышат даже в режиме радиомолчания, но имеют ограниченную дальность. RF-сканеры обнаруживают сигналы управления, но бесполезны против оптоволокну. Оптические камеры дают визуальное подтверждение, но зависят от освещения.

Именно поэтому современные системы используют все эти каналы одновременно, объединяя их данные в единую картину.

Этап 2: Классификация

Обнаружить — это полдела. Нужно ещё понять, что именно ты обнаружил.

Это гражданский квадрокоптер или боевой FPV? Это одиночный разведчик или первый из роя? Это дрон с боевой частью или просто наблюдатель?

На этом этапе ключевую роль играет искусственный интеллект. Нейросети анализируют данные со всех сенсоров и классифицируют цель с точностью, недоступной человеку. Они отличают дрон от птицы по микродоплеровскому сдвигу от вращающихся винтов. Они определяют модель дрона по его радиочастотной сигнатуре. Они оценивают траекторию и прогнозируют намерения.

Этап 3: Решение

Теперь, когда цель идентифицирована, система должна принять решение: как на неё реагировать?

Это, пожалуй, самый сложный этап. Потому что решение должно учитывать множество факторов:

- Тип цели. Рой требует одного ответа (микроволны), одиночный оптоволоконный дрон — другого (кинетика), гражданский квадрокоптер — третьего (спуфинг).

- Экономическая целесообразность. Не тратить ракету на то, что можно сбить «арканом».

- Обстановка. Можно ли применять кинетику в городской застройке? Не создаст ли лазер помех своим системам?

- Время. Чем ближе цель, тем меньше вариантов и тем быстрее нужно действовать.

Именно здесь эшелонированная система раскрывает свой потенциал. У неё есть набор инструментов, и она выбирает оптимальный.

Этап 4: Воздействие

И наконец — действие. Выбранное средство применяется для нейтрализации угрозы.

Если это РЭБ — включается глушение или спуфинг. Если это кинетика — открывается огонь. Если это лазер — активируется луч. Если это механическая ловушка — срабатывает сетка.

Но даже после воздействия процесс не заканчивается. Система оценивает результат: цель нейтрализована? Если нет — следующий эшелон вступает в действие. Если да — си-

стема возвращается в режим мониторинга.

Резюме: почему эшелонирование — это единственный путь

Я хочу завершить эту главу тем, с чего начал: нет «серебряной пули».

Это не пораженчество. Это осознание реальности. И именно это осознание даёт нам ключ к победе.

Противодронная оборона — это не набор устройств. Это процесс.

Процесс, в котором:

- Обнаружение даёт информацию.
- Классификация даёт понимание.
- Решение даёт стратегию.
- Воздействие даёт результат.

И каждый из этих этапов должен работать безупречно. Потому что если на каком-то этапе происходит сбой, вся система даёт трещину. А в условиях, когда противник атакует роями, когда дроны эволюционируют быстрее, чем мы создаём средства противодействия, когда экономический дисбаланс ставит под угрозу саму возможность вести войну — трещина в системе может стоить очень дорого.

Но если все этапы работают слаженно, если каждый уровень дополняет другие, если система способна адаптироваться и перестраиваться — тогда она становится чем-то большим, чем сумма её частей. Она становится непреодолимым барьером.

Именно такую систему мы и будем строить на страницах этой книги.

«Противодронная оборона лучше всего рассматривается как многоуровневая система принятия решений, а не как набор разрозненных датчиков и средств поражения»

Глава 2. Обнаружение и идентификация — глаза, уши и разум системы

Я никогда не забуду один разговор с офицером ПВО, который служил на границе. Он рассказывал, как однажды его расчёт пропустил маленький коммерческий квадрокоптер, который беспрепятственно пролетел над охраняемым объектом и вернулся обратно. Радар его не увидел — слишком маленький, слишком низко. RF-сканер не сработал — дрон летел в режиме радиомолчания, ничего не передавая. Оптический наблюдатель не заметил — была ночь и лёгкий туман.

Акустическая система? Её не было. Её тогда ещё не ставили на объекты такого типа.

Через неделю этот же дрон прилетел снова. С боеприпасом.

Офицер тогда сказал мне фразу, которую я запомнил на всю жизнь: «Мы не заметили угрозу не потому, что у нас не было оружия. А потому, что у нас не было глаз».

С тех пор я твёрдо усвоил: обнаружение — это фундамент. Без него все остальные методы противодействия — дорогие игрушки. Можно поставить новейший комплекс РЭБ за миллионы рублей. Можно развернуть лазерную установку. Можно выставить мобильные огневые группы. Но если

ты не видишь цель — ты стреляешь вслепую. Ты тратишь ресурсы впустую. Ты создаёшь иллюзию защиты там, где защиты нет.

Именно поэтому я посвящаю эту главу тому, что стоит в самом начале цепочки противодействия. Тому, что превращает оборону из «набора устройств» в «систему». Тому, что даёт нам время, информацию и возможность выбора.

Радиолокационные станции (РЛС): дальний рубеж

Когда мы говорим об обнаружении, первое, что приходит на ум, — радиолокация. И это не случайно. РЛС остаются самым мощным инструментом для обнаружения целей на больших дистанциях. Они работают в любую погоду, в любое время суток, сквозь туман и облака. Они видят то, что не видит человеческий глаз.

Но у радаров есть одна фундаментальная проблема. Они плохо видят маленькие цели на малых высотах. Современные БПЛА — это радиолокационный кошмар. Они сделаны из композитных материалов, которые плохо отражают радиоволны. Их эффективная площадь рассеивания может составлять менее 0,01 квадратного метра. Они летают на высоте нескольких метров над землёй, прячась в складках местности. Классические радары, разработанные для обнаружения самолётов и вертолётв, просто «не видят» такие

цели.

Именно поэтому отрасль сейчас активно работает над новыми поколениями радиолокационных станций.

Российская система 3D ПКЛ, разработанная в рамках проектов Ростеха, специально нацелена на эту проблему. Как отмечают разработчики, «современные БПЛА обладают низкой радиолокационной заметностью и используют небольшие высоты». Эта система способна обнаруживать такие дроны благодаря высокой чувствительности к радиолокационно малозаметным и низколетящим целям, а также функции трёхмерного сопровождения.

Ещё одна перспективная разработка — проект «Лори», радиолокационная станция с максимальной дальностью обнаружения 10 километров и возможностью сопровождения целей на скорости до 200 км/ч. Это позволяет работать по лёгким и малым БПЛА самых распространённых моделей.

Но, пожалуй, самый впечатляющий пример того, как далеко зашла эволюция радаров, — это разработка учёных Новгородского государственного университета. Они создали радар, который способен обнаруживать беспилотники в зоне порядка трёх километров, включая безэкипажные катера и другие подвижные цели. И это при том, что технология активной радиолокации, которую они используют, считается безопасной для человека.

Тем не менее, даже самые современные РЛС не решают всех проблем. Радар — это «дальний рубеж». Он даёт пер-

вое предупреждение. Он показывает, что в воздухе что-то есть. Но он не всегда может сказать, что именно это за объект. Он не всегда может отличить дрон от птицы, особенно на больших дистанциях. И он совершенно бесполезен, когда цель скрывается за зданием или холмом.

Поэтому радары никогда не работают в одиночку.

Оптические датчики: видимый и инфракрасный диапазоны

Если радар — это «дальний слух» системы, то оптика — это её «зоркий глаз».

Оптические датчики дают то, чего не может дать ни один радар: визуальное подтверждение. Ты видишь цель. Ты понимаешь, что это действительно дрон, а не стая птиц. Ты видишь его модель, его размеры, его вооружение. Ты можешь оценить его траекторию и намерения.

Но у оптики есть свои ограничения. Она зависит от освещения. Она «слепнет» в тумане и в темноте. Поэтому современные системы используют два подхода одновременно: видимый диапазон и инфракрасный.

Видимый диапазон — это то, что мы видим своими глазами. Камеры высокого разрешения, работающие в дневное время, дают чёткую картинку, позволяют идентифицировать модель дрона, прочитать его серийный номер, если повезёт. Но как только солнце садится, эффективность таких камер

резко падает.

Инфракрасный диапазон — это тепловое зрение. Каждый дрон, даже самый маленький, нагревает свой двигатель и аккумулятор. Инфракрасные камеры видят это тепло, позволяя обнаруживать цели в полной темноте, сквозь дым и лёгкий туман.

Именно поэтому современные оптико-электронные системы объединяют оба подхода. Например, российские изделия ГОЭН-60, разработанные для ударных дронов и систем противодействия, работают одновременно в видимом и инфракрасном диапазонах. В них реализованы нейросетевые алгоритмы, которые автоматически обнаруживают, распознают и сопровождают объекты.

Западные системы идут ещё дальше. Например, система VAR300 обеспечивает обнаружение в дневное время на дистанции более одного километра, а ночью — на дистанции более 500 метров. При этом она способна не только обнаруживать, но и отслеживать цели на дистанции до 1,5 километра.

Но даже самые лучшие оптические системы имеют один фундаментальный недостаток: они требуют прямой видимости. Если дрон скрывается за зданием, за деревом, за холмом — оптика его теряет. Именно поэтому оптические датчики всегда работают в связке с другими средствами обнаружения.

Акустические системы пассивного обнаружения

А теперь давайте поговорим о том, что я считаю самым недооценённым инструментом в арсенале противодронной обороны.

Акустика.

В то время как инженеры бьются над созданием всё более совершенных радаров и оптических систем, на передовой всё чаще используют то, что всегда было под рукой, — слух.

Акустические системы пассивного обнаружения — это «невидимое ухо» системы. Они ничего не излучают. Их невозможно засечь средствами радиотехнической разведки. Они работают в режиме полного радиомолчания, когда дрон не передаёт и не принимает сигналы. Они слышат то, что не видят радары и не замечают оптические камеры.

Как это работает? Любой летящий дрон производит звук. Винты, двигатель, вибрации корпуса — у каждого аппарата есть своя акустическая «подпись». Задача акустической системы — уловить этот звук среди тысяч других шумов окружающей среды, идентифицировать его как принадлежащий именно беспилотнику и определить направление, с которого он приближается.

Российский комплекс «Атака-Шорох» — яркий пример такого подхода. Как образно выразились разработчики, это

«умное ухо», которое различает звук беспилотника от тысячи других возможных шумов большого города. Система оснащена сверхчувствительными микрофонами и интеллектуальной системой анализа внешней обстановки. Она способна не только обнаруживать дроны, но и выявлять чрезвычайные ситуации или правонарушения по характерным шумам.

Что особенно важно, «Атака-Шорох» можно интегрировать в единую систему с комплексом радиочастотного обнаружения и подавления «Атака-DBS». Если акустика «слышит» дрон в режиме радиомолчания, RF-комплекс может подавить его навигацию. Это классический пример того, как разные сенсоры дополняют друг друга.

Дальность обнаружения акустических систем зависит от типа дрона и уровня фонового шума. Электрические дроны (малые квадрокоптеры, FPV-аппараты) слышны на дистанциях 150–500 метров. Дроны с двигателями внутреннего сгорания (тяжёлые разведывательные и ударные БПЛА) — на дистанциях до нескольких километров.

И главное преимущество акустики — абсолютная скрытность. Система не демаскирует своё присутствие. Она не создаёт помех. Она просто слушает. И в этом её сила.

Анализ радиочастотного спектра (RF-сканеры)

Если акустика — это «ухо», а оптика — «глаз», то RF-

сканеры — это «радиоприёмник» системы.

RF-сканеры — это пассивные детекторы, которые анализируют радиочастотный спектр в поисках сигналов управления и телеметрии, характерных для БПЛА. Они работают «на приём», не демаскируя себя излучением. И это их главное преимущество.

Большинство коммерческих и многих тактических дронов передают три типа сигналов: восходящий канал (управление от оператора к дрону), нисходящий канал (телеметрия и видеопоток от дрона к оператору) и сигналы спутниковой навигации (GPS, ГЛОНАСС). RF-сканер может обнаружить эти сигналы, идентифицировать их как принадлежащие дрону и даже определить модель аппарата по его радиочастотной «подписи».

Современные RF-сканеры используют машинное обучение для обнаружения и классификации сигналов. Исследования показывают, что нейросетевые модели могут достигать точности обнаружения дронов до 98,23% и точности идентификации до 95,39%. Это не просто «есть сигнал/нет сигнала» — это интеллектуальный анализ, который позволяет отличать дрон от других источников радиоизлучения.

Однако у RF-сканеров есть два фундаментальных ограничения.

Первое: они бесполезны против дронов, которые ничего не излучают. Оптоволоконные аппараты, дроны в режиме радиомолчания, полностью автономные системы с машин-

ным зрением — все они «невидимы» для RF-сканеров.

Второе: они требуют базы данных сигнатур. Чтобы определить, что данный сигнал принадлежит именно дрону, система должна иметь эталон для сравнения. Если противник использует новый тип дрона на неизвестной частоте — RF-сканер может его пропустить.

Именно поэтому RF-сканеры, как и все другие сенсоры, никогда не работают в одиночку. Они — часть более широкой системы, где каждый инструмент закрывает «слепые зоны» других.

Искусственный интеллект и нейросети в обнаружении: от шума к сигнатуре

Теперь мы подходим к самому важному. К тому, что превращает набор сенсоров в интеллектуальную систему.

Я часто говорю своим коллегам: «Сенсоры дают данные. Искусственный интеллект даёт понимание».

Представьте себе ситуацию: радар видит движущуюся точку. Акустическая система слышит шум. Оптическая камера фиксирует тёмный силуэт. RF-сканер улавливает слабый сигнал на частоте 2,4 ГГц.

Что это? Дрон? Птица? Беспилотник соседей? Или, может быть, ложное срабатывание?

Без искусственного интеллекта ответить на этот вопрос сложно. Данные противоречивы, неполны, зашумлены. Че-

человеческий оператор может ошибиться, может не успеть обработать информацию, может просто не заметить угрозу среди сотен других сигналов.

Искусственный интеллект решает эту проблему.

Нейросети, обученные на огромных массивах данных, способны анализировать информацию со всех сенсоров одновременно, выделять закономерности и принимать решения за доли секунды. Они видят то, что не видит человек. Они слышат то, что не слышит человек. И они делают это быстрее, чем любой оператор.

Как именно это работает?

В радиолокации нейросети анализируют микродоплеровскую модуляцию эхо-сигнала — тонкие изменения частоты, вызванные вращением винтов дрона. По этим изменениям можно не только обнаружить цель, но и определить её тип — мультироторный дрон, самолётный БПЛА или птица.

В оптике нейросетевые алгоритмы автоматически обнаруживают, распознают и сопровождают объекты на видео- и фотоизображениях. Они могут работать в реальном времени, обрабатывая видеопоток с камер и выделяя дроны среди тысяч других объектов.

В акустике нейросети анализируют звуковой спектр, сравнивая его с базой акустических сигнатур. Они могут отличить звук винтов DJI Mavic от звука винтов FPV-дрона, даже если оба звучат похоже для человеческого уха.

В RF-анализе нейросети классифицируют сигналы по их

частотным и временным характеристикам, определяя модель дрона и даже его состояние.

И самое главное — нейросети умеют интегрировать данные со всех этих источников. Они создают единую картину, где каждый сенсор дополняет другие. Где радар даёт расстояние, оптика — визуальное подтверждение, акустика — подтверждение в режиме радиомолчания, а RF-сканер — идентификацию модели.

Именно так, как это делают современные системы, объединяющие акустические, визуальные, радарные и другие сенсорные данные через трёхуровневую архитектуру слияния.

Заместитель директора НИИ «Вектор» Наталия Котляр сформулировала это предельно ясно: внедрение ИИ в антидроновые системы для автоматического обнаружения и сопровождения цели необходимо, поскольку «человек физически не успевает обрабатывать все поступающие данные». Нейросети, в том числе свёрточные и рекуррентные, успешно применяются для обнаружения сигналов БПЛА даже при низком отношении сигнал/шум.

Искусственный интеллект — это не просто «дополнительная функция». Это разум системы. Это то, что превращает хаос данных в структурированную информацию. Это то, что даёт нам время и возможность принять правильное решение.

Интеграция сенсоров: закрывая «слепые зоны»

И вот мы подходим к кульминации. К тому, ради чего всё это затевалось.

Ни один сенсор в отдельности не даёт полной картины. Радар видит далеко, но слепнет на малых высотах. Оптика даёт детализацию, но зависит от освещения. Акустика слышит в режиме радиомолчания, но имеет ограниченную дальность. RF-сканер идентифицирует сигналы, но бесполезен против оптоволокну.

Только вместе они создают надёжную систему обнаружения.

Современная архитектура противодронной обороны строится на принципе мультисенсорной интеграции. Это когда данные от разных датчиков объединяются в единую картину, где каждый источник информации закрывает «слепые зоны» других.

Как пишут западные исследователи, «противодронная оборона лучше всего рассматривается как многоуровневая система принятия решений, а не как набор разрозненных датчиков и средств поражения». Мультисенсорное слияние объединяет разнообразные модальности — RF, радар, оптику, акустику, пассивные излучатели, Remote ID — в единый, дедуплицированный трек с оценкой достоверности и чёткими процедурами передачи управления средствам пора-

жения.

Что это означает на практике?

Это означает, что акустический датчик, услышав шум дрона в режиме радиомолчания, даёт команду оптической системе развернуться в направлении звука. Оптика подтверждает визуальный контакт. RF-сканер в это время пытается перехватить сигналы управления. Радар отслеживает траекторию. Все данные стекаются в единый центр, где искусственный интеллект анализирует их и выдаёт рекомендацию: что это за дрон, откуда он летит, куда направляется и какое средство противодействия следует применить.

И всё это происходит за секунды. Автоматически. Без участия человека.

Именно такую систему, по словам разработчиков, представляет собой единая система контроля воздушно-го пространства, представленная Ростехом на выставке «Нева-2025». Она способна автоматически обнаруживать цели, в том числе крайне малые воздушные объекты на малых высотах, и объединять радиолокационную информацию с 24 локаторов на одно рабочее место.

Именно такую систему строят учёные, работающие над «интеллектуальной мультимодальной мультисенсорной системой» для идентификации, локализации и противодействия БПЛА, которая интегрирует восприятие на основе слияния нескольких сенсоров, точное позиционирование и скоординированные контрмеры в единый замкнутый про-

цесс управления — от раннего предупреждения до финальной нейтрализации.

Именно такую систему, в конечном счёте, мы должны построить.

Резюме: от сенсоров к системе

Я хочу завершить эту главу тем, с чего начал: обнаружение — это фундамент.

Но фундамент не бывает монолитным. Он состоит из множества элементов, каждый из которых выполняет свою функцию. Радар видит далеко. Оптика — детально. Акустика — скрытно. RF-сканер — точно. Искусственный интеллект — быстро.

Вместе они создают то, что невозможно создать по отдельности: полную картину воздушной обстановки.

Без радара мы не увидим угрозу на дальних подступах. Без оптики мы не сможем подтвердить, что это действительно дрон. Без акустики мы пропустим аппараты в режиме радиомолчания. Без RF-сканера мы не идентифицируем модель и не поймём, с чем имеем дело. Без искусственного интеллекта мы не успеем обработать все данные и принять решение.

Но когда все эти элементы работают вместе — когда они интегрированы в единую систему, где каждый дополняет другого, — тогда у нас появляется реальное преимущество.

Тогда мы видим угрозу до того, как она становится опасной. Тогда мы успеваем подготовиться. Тогда у нас есть вре-

мя и информация для выбора правильного средства противодействия.

Тогда мы не пропускаем дрон, который пролетает над объектом ночью, в тумане, в режиме радиомолчания.

Потому что у нас есть «уши», которые его слышат. И «глаза», которые его видят. И «разум», который понимает, что это такое.

И это — единственный способ выжить в новой войне.

«Обнаружение и отслеживание являются краеугольным камнем технологий C-UAS»

Глава 3. РЭБ как интеллектуальная экосистема

Был момент, который я никогда не забуду. 2022 год. Мне показали запись с камеры одного из наших комплексов РЭБ. На экране — FPV-дрон противника, который должен был упасть. По всем расчётам, по всем характеристикам нашей станции — он должен был потерять управление и рухнуть на землю. Но он не упал. Он продолжал лететь. Он слегка покачивался, терял ориентацию, но упрямо двигался вперёд. А потом — провал. Сигнал пропал. Запись оборвалась.

Через двадцать минут мы узнали, что этот дрон поразил цель.

Я сидел и смотрел на чёрный экран, чувствуя, как внутри меня поднимается холодная ярость. Не на противника. На себя. На нас. На всех, кто думал, что мы уже всё поняли про эту войну.

Мы думали, что РЭБ — это просто «включил и заглушил». Что достаточно поставить станцию, и она создаст невидимую стену, о которую разобьются все дроны. Мы думали, что боремся с радиосигналами. А на самом деле мы боролись с интеллектом. С адаптацией. С живой, эволюционирующей системой, которая училась быстрее, чем мы успевали переписывать свои алгоритмы.

С тех пор я понял: РЭБ — это не глушилка. Это экосистема. Это живой организм, который видит, думает, выбирает и только потом действует. И если хотя бы один элемент этой системы даёт сбой — вся конструкция рушится.

От точечного глушения к интеллектуальному «куполю»

В начале 2010-х годов, когда дроны только начинали представлять угрозу, подход к РЭБ был до смешного прост. Берёшь мощный передатчик, настраиваешь на частоту GPS или канал управления — и глушишь. Всё. Точечное, грубое, неинтеллектуальное воздействие.

И оно работало. Против DJI Phantom, против первых квадрокоптеров, которые использовали стандартные частоты и простые протоколы — работало блестяще.

Но дроны эволюционировали. Быстро. Беспощадно.

Появились частоты, которых не было в базах данных. Появились алгоритмы псевдослучайной перестройки рабочей частоты (ППРЧ) — когда дрон «прыгает» по спектру, уходя от помех. Появились оптоволоконные аппараты, которые вообще не излучают сигналов. Появились автономные системы с машинным зрением, которым не нужен GPS.

И в какой-то момент стало очевидно: глушить вслепую нельзя.

Этот тезис стал краеугольным. Сегодня эффективная РЭБ

— это не просто «глушилка». Это интеллектуальный «купол», который:

- Видит — обнаруживает дроны, анализирует их сигналы.
- Понимает — классифицирует тип угрозы, определяет её частотные характеристики.
- Выбирает — решает, какое воздействие применить: глушение, спуфинг или вообще ничего, если это свой дрон.
- Действует — применяет выбранный метод, но только на то время и в том диапазоне, которые необходимы.

Как справедливо отмечают разработчики, «эффективное подавление невозможно без точного обнаружения». Современный комплекс РЭБ — это не передатчик. Это система, объединяющая детектор, анализатор и блок подавления.

Именно так работает, например, обновлённый «СЕРП-ВС13Д». Он совмещает в себе комплекс РЭБ и высокоточный детектор, который обнаруживает даже FPV-дроны. Высокоточный детектор и алгоритмы искусственного интеллекта позволяют с предельной точностью обнаруживать цели, создавая купол безопасности над охраняемым периметром.

Или комплекс «Солярис НС» — интеллектуальная система, которая объединяет функционал двух предыдущих изделий: «Солярис-О» для обнаружения БПЛА и «Солярис-Н» для их подавления. Несколько комплексов могут объединяться в кластер для круговой защиты объекта.

Это и есть интеллектуальный «купол». Не просто стена, а живая, адаптивная система, которая видит угрозу, понимает

её и реагирует именно так, как нужно в данный момент.

Компонент 1: обнаружение и идентификация — «глаза» системы

Я часто говорю своим коллегам: «РЭБ без обнаружения — это стрельба вслепую. Ты можешь потратить всю энергию на помехи, которые вообще не нужны, и пропустить настоящую угрозу».

Обнаружение и идентификация — это первый и самый важный компонент современной РЭБ. Это «глаза» системы. Без них все остальные компоненты — просто дорогие игрушки.

Как это работает на практике?

Представьте себе систему «СЕРП-ВС13Д». Она постоянно сканирует радиочастотный спектр, анализируя каждый сигнал. Высокоточный детектор вылавливает даже слабые, замаскированные сигналы управления. А алгоритмы искусственного интеллекта мгновенно классифицируют обнаруженный объект.

Но «глаза» РЭБ — это не только RF-сканеры. Это ещё и акустика, и оптика, и радары. Современные системы интегрируют данные со всех сенсоров, создавая единую картину воздушной обстановки.

Например, система «Купол», разработанная «Кулибин-клубом», состоит из оборудования по обнаружению

дронов и станции радиоэлектронного подавления. В неё можно интегрировать умные камеры, которые будут визуально фиксировать объекты в небе. Программное обеспечение системы отличает летящий дрон от птицы или самолёта.

Комплекс «Солярис НС» ведёт непрерывное радионаблюдение по трём независимым каналам, что позволяет одновременно выявлять не менее трёх дронов. Это не просто «видеть» — это видеть одновременно в разных направлениях, разными методами, с разных углов.

Зачем это нужно? Затем, что дроны бывают разными. Коммерческий квадрокоптер излучает мощный сигнал на стандартной частоте. FPV-дрон работает на других частотах, часто с псевдослучайной перестройкой. Оптоволоконный аппарат вообще ничего не излучает — его можно обнаружить только акустикой или оптикой.

Именно поэтому у РЭБ должны быть разные «глаза». RF-сканер для радиочастотных сигналов. Акустика для шума винтов. Оптика для визуального подтверждения. Радар для дальнего обнаружения. И всё это — объединённое в единую систему, где каждый сенсор дополняет другие.

Когда все «глаза» работают вместе, система видит всё. И это — основа для принятия правильного решения.

Компонент 2: подавление (глушение) — «слепой» и «немой» дрон

Теперь представьте: система увидела дрон. Она его идентифицировала. Она поняла, что это угроза. Что дальше?

Дальше — подавление. Это второй компонент РЭБ, его «рука». И здесь современная РЭБ ушла далеко от примитивного «включил и заглушил».

Современное подавление — это точная хирургия. Система не просто создаёт шум по всему спектру. Она генерирует целевые помехи на той частоте, где работает дрон, с идентичными принципами модуляции. Это лишает дрон связи с оператором и возможности получения корректных навигационных данных независимо от используемого протокола.

Как это выглядит на примере конкретных комплексов?

«СЕРП-ВС13Д». В новой модели количество рабочих частот увеличено с шести до тринадцати. Это позволяет обезвреживать дроны, которые ранее было практически невозможно подавить. Например, квадрокоптеры Autel Robotics EVO Max 4T, которые выживают в схватке с обычными системами РЭБ за счёт функции управления в широком диапазоне частот. В период активации системы радиосигналы подавляются во всех доступных диапазонах.

«Двина-100М». Эта система, запущенная в производство в сентябре 2025 года, предназначена для защиты крупных

промышленных объектов и критической инфраструктуры. Она создаёт купол безопасности радиусом в несколько сотен метров. Дальность подавления — не менее 1,5 км в ненаправленном режиме и не менее 2,1 км в направленном. Система функционирует в экстремальном температурном диапазоне от 40 °С до +50 °С. Она осуществляет глушение каналов управления, передачи данных и навигационных сигналов спутниковых систем (GPS/ГЛОНАСС) в широком частотном спектре, включая аппараты с псевдослучайной перестройкой рабочей частоты.

«Омут». Система РЭБ, которая после модернизации обеспечивает защитный купол диаметром до 400 метров. Предназначена для защиты военной техники и автомобилей от атак дронов, подавляя каналы связи и управления. Новые антенны улучшили показатели системы на 20 процентов. Как образно выразился представитель компании-производителя, это «невидимый круг радиопомех, в пределах которого вам не страшны БПЛА и FPV-дроны противника».

«Солярис НС». Эта система использует комбинацию прицельного и заградительного подавления. Когда в одном из девяти передатчиков включается режим прицельной помехи (в момент обнаружения объекта), остальные начинают работать в режиме заградительной помехи, чтобы не дать беспилотнику «прыгать» по частотам и выйти из зоны блокировки. Одновременно устройство запускает работу четырёх каналов радиоподавления спутниковых навигационных си-

стем: GPS, ГЛОНАСС, BeiDou и Galileo.

Но самое важное — современное подавление стало избирательным. Система не глушит всё подряд, создавая помехи своим же средствам связи. Она работает точно, только по тем частотам, которые использует противник. Применение таких средств позволяет точно противодействовать БПЛА, не нарушая работы инфраструктуры, использующей радиоэфир.

Цель подавления — сделать дрон «слепым» и «немым». Лишить его управления. Лишить навигации. Лишить возможности передавать видео. И тогда он либо зависнет на месте, либо попытается вернуться на базу, либо просто упадёт.

Компонент 3: спуфинг — «тонкая хирургия» в мире РЭБ

Но есть метод, который я считаю самым элегантным во всей системе РЭБ. Метод, который не грубо обрывает связь, а обманывает. Тонко. Изящно. Почти по-джентльменски.

Это спуфинг.

Если глушение — это «молот», то спуфинг — это «скальпель». Вместо того чтобы создавать шум и обрывать связь, система-спуфер передаёт ложные навигационные сигналы, имитирующие настоящие. Дрон, принимая их за истинные, начинает верить, что находится в другом месте.

И тогда происходит чудо. Дрон, который должен был ата-

ковать ваш объект, вдруг разворачивается и улетает в совершенно другую сторону. Он не понимает, что его обманули. Он просто следует командам, которые кажутся ему правильными.

Как это работает технически?

Спуфер создаёт фальшивый GPS-сигнал, который является более сильным и привлекательным для приёмника дрона, чем настоящие спутники на орбите. Обманув навигационную систему, можно взять дрон под контроль. Оператор способен приказать дрону лететь в определённом направлении, отправив его на расстояние до четырёх километров. Более того, БПЛА можно заставить приземлиться в безопасном месте.

Этот метод особенно эффективен против дронов, которые при потере сигнала GPS переходят в режим удержания позиции или возврата на базу — их можно «увести» в безопасную зону.

У спуфинга есть огромное преимущество перед глушением. Он не создаёт помех. Он не забивает эфир. Он работает тихо, незаметно, избирательно. Он не нарушает работу своих систем связи и навигации.

Но самое главное преимущество спуфинга — возможность захватить вражеский дрон. Не уничтожить, а захватить. Анализируя его оборудование и данные, можно потенциально отследить его оператора. Как справедливо заметил один из экспертов: «Дрон, который является просто кучей

дымящихся обломков на земле, вам этого не даст. Эта система позволяет не только остановить непосредственную угрозу, но и расследовать её. Это очень умный ход».

Американская компания DZYNE Technologies воплотила этот принцип в своей антидроновой винтовке DroneBuster. Она не глушит беспилотник, а берёт его под контроль. Это не просто оружие — это инструмент разведки.

Однако, как и любой метод, спуфинг не является панацеей. Противник постоянно внедряет алгоритмы детекции для противодействия подмене сигналов. Некоторые боевые дроны постепенно переходят на машинное зрение, отказываясь от спутниковой навигации, сигнал от которой может быть подменён. Это создаёт классическую гонку вооружений в цифровой сфере, где каждая новая защита порождает новый метод взлома.

Но пока эта гонка продолжается, спуфинг остаётся одним из самых эффективных и элегантных инструментов в арсенале РЭБ.

Кибер-атаки: взлом дронов прямо в воздухе

И наконец, мы подходим к самому, пожалуй, футуристичному компоненту современной РЭБ. К тому, что ещё пять лет назад казалось научной фантастикой, а сегодня стало реальностью.

Кибер-атаки на дроны.

Как справедливо отметил генеральный конструктор Центра комплексных беспилотных решений Кузякин, «дроны взламывают прямо в воздухе». И это не преувеличение.

Современный дрон — это не просто кусок пластика с мотором. Это компьютер. У него есть операционная система, процессор, память, сетевые интерфейсы. У него есть уязвимости, как у любого компьютера.

И эти уязвимости можно использовать.

Какие типы кибератак возможны против дронов?

Атаки на каналы управления. Перехват управления — когда злоумышленник внедряется в канал связи между оператором и дроном и берёт управление на себя. Это требует глубокого понимания протоколов связи, но технически реализуемо.

Атаки на телеметрию. Перехват и подмена телеметрических данных — когда системе показывают ложную информацию о состоянии дрона. Например, можно «убедить» дрон, что у него разрядился аккумулятор, и он автоматически садится.

Внедрение вредоносного кода. Если удаётся получить доступ к бортовой системе дрона — можно загрузить вредоносную программу, которая изменит его поведение. Можно заставить его атаковать свои же позиции. Можно просто выключить его в воздухе.

Атаки отказа в обслуживании (DoS). Перегрузка системы дрона запросами, которые выводят его из строя.

Исследования показывают, что наиболее распространёнными типами кибератак на дроны являются атаки типа «отказ в обслуживании» (25%), взлом паролей и протоколов (17%), атаки «человек посередине» (MitM) (15%), глушение (10%), внедрение команд и кода (7%) и несанкционированный доступ (6%).

И это не просто теория. В апреле 2026 года в «Руднево» провели эксперимент, в ходе которого проверяли устойчивость каналов управления дронами к кибератакам. Главная цель — проверить, насколько легко злоумышленник может взломать системы управления дронами и что нужно сделать, чтобы защитить эти системы.

Особенно уязвимы коммерческие дроны. Например, уязвимость CVE-2025-10250 была выявлена в моделях DJI Mavic Spark, Mavic Air и Mavic Mini. Она позволяет злоумышленнику получить доступ к телеметрическому каналу.

Но самое интересное — как кибератаки интегрируются в общую систему РЭБ.

Представьте: система обнаружила дрон. RF-сканер определил его модель. Искусственный интеллект проанализировал его сигналы и нашёл уязвимость. И вместо того чтобы глушить или обманывать — система просто взламывает дрон. Перехватывает управление. Сажает его на свою территорию. И получает доступ к его данным, его камере, его боеприпасам.

Это не фантастика. Это реальность, которая уже наступа-

ет.

Как отметил начальник войск РЭБ группировки «Восток», в зоне специальной военной операции началось тестирование новой автоматизированной системы управления радиоэлектронной борьбы. И я уверен, что кибер-компонент в этой системе занимает далеко не последнее место.

Резюме: РЭБ как живой организм

Я хочу завершить эту главу тем, с чего начал: РЭБ — это не глушилка. Это экосистема.

Это живой организм, у которого есть:

- Глаза — обнаружение и идентификация, которые видят угрозу среди тысяч других сигналов.

- Мозг — искусственный интеллект, который анализирует, классифицирует и принимает решения.

- Руки — подавление, которое делает дрон «слепым» и «немым».

- Скальпель — спуфинг, который обманывает дрон, уводя его с охраняемой территории.

- Ключ — кибератаки, которые взламывают дрон прямо в воздухе.

И все эти компоненты работают вместе. Не вместо, а вместе. Не по отдельности, а как единая система.

Это и есть интеллектуальный «купол». Не просто стена, а живая, адаптивная система, которая видит угрозу, понимает её и реагирует именно так, как нужно в данный момент.

Но даже такая система не является абсолютной. Дро-

ны эволюционируют. Появляются оптоволоконные аппараты, которые невозможно заглушить. Появляются автономные системы, которые невозможно обмануть. Появляются новые протоколы, которые невозможно взломать.

Именно поэтому РЭБ никогда не будет завершённой. Она всегда будет находиться в процессе развития. Она всегда будет догонять угрозу. Она всегда будет адаптироваться.

Но именно в этой адаптации — её сила. Потому что РЭБ — это не конечный продукт. Это процесс. Процесс, который продолжается до тех пор, пока существует угроза.

И мы будем продолжать этот процесс. Потому что другого выбора у нас нет.

«Эффективное подавление невозможно без точного обнаружения»

Глава 4. Отечественные и зарубежные комплексы РЭБ

Когда я начинал свой путь в этой сфере, мне казалось, что все комплексы РЭБ похожи друг на друга. Ну, подумаешь, антенны, передатчики, блоки питания. Глушат — и глушат. Какая разница?

Какая же это была наивность.

Со временем я понял: каждый комплекс РЭБ — это не просто «глушилка». Это философия. Это ответ на конкретный вызов, рождённый в конкретных условиях. Это история о том, как инженеры, военные и стратеги пытаются переиграть противника в бесконечной игре, где правила меняются каждые несколько месяцев.

И когда я смотрю на российские комплексы РЭБ — от крошечного «СЕРП-П6» до гигантской «Волны Купол Гарант», — я вижу не просто технику. Я вижу живую, дышащую историю адаптации. Историю о том, как страна, столкнувшаяся с беспрецедентной дроновой угрозой, учится выживать и побеждать.

«СЕРП» и «Двина-100М»: защита инфраструктуры

Начну с того, что находится ближе всего к моему сердцу. С защиты того, что нельзя потерять.

Критическая инфраструктура. Мосты, тоннели, аэропорты, железнодорожные станции, нефтеперерабатывающие заводы. Это не просто объекты. Это артерии страны. И противник знает это лучше нас.

Когда я впервые увидел спецификацию «СЕРП-П6», я испытал странное чувство. С одной стороны — восхищение. С другой — лёгкую грусть. Потому что я понял: мы дошли до того, что вынуждены защищать каждый мост, каждую архитектурную ценность от дешёвого дрона, который может принести больше разрушений, чем диверсионная группа.

Но разработчики из холдинга «Росэл» справились с этой задачей блестяще.

«СЕРП-П6» — это не просто ещё один комплекс РЭБ. Это произведение инженерного искусства. Компактный модуль, который можно монтировать на несущие элементы сооружений, полностью сохраняя их культурно-исторический или инженерно-технический внешний вид. Представьте себе: вы защищаете мост, которому сто лет, и при этом никто не увидит, что он защищён. Никаких уродливых антенн, никаких проводов, ничего, что испортило бы его облик.

Но за этой элегантностью скрывается серьёзная мощь. «СЕРП-П6» способен подавлять сигналы всех глобальных спутниковых навигационных систем — GPS, ГЛОНАСС, Galileo и BeiDou — в диапазоне L1-1,5 ГГц. Параллельно блокируются каналы связи и управления дронами в широком частотном диапазоне. Результат? Дрон теряет ориентацию в пространстве, лишается управления и срывает полётное задание.

Но «СЕРП-П6» — это лишь вершина айсберга. Вся линейка комплексов «СЕРП» работает в нескольких диапазонах от 300 МГц до 5,8 ГГц. А флагман линейки — «СЕРП-ВС13Д» — работает на тринадцати частотах, совмещая в себе комплекс РЭБ и высокоточный детектор, обнаруживающий даже FPV-дроны. Это уже не просто «глушилка». Это интеллектуальная система, которая видит, анализирует и подавляет.

И всё это — результат постоянной эволюции. Как отметили в «Росэле», «в условиях растущей угрозы со стороны БПЛА вопросы защиты периметра, воздушного пространства и критически важных объектов выходят на первый план».

А теперь — о системе, которую я называю «большой сестрой» «СЕРПа».

«Двина-100М» .

Когда я впервые услышал о ней, я подумал: «Ну, ещё одна система подавления. Их уже десятки». Но потом я вчитался в характеристики, и у меня перехватило дыхание.

«Двина-100М» — это не просто защита объекта. Это купол безопасности радиусом в несколько сотен метров над охраняемым объектом. Дальность подавления — не менее 1,5 километра в ненаправленном режиме и не менее 2,1 километра в направленном. Она способна противостоять не только одиночным дронам, но и роевым атакам.

Но самое главное — её интеллектуальная составляющая.

«Двина-100М» работает в комплексе со специализированными средствами радиомониторинга. Они получают информацию о характеристиках сигналов, используемых беспилотником, и формируют в ответ целевые помехи именно на этой частоте и с такими же принципами передачи информации. Это не тупое «включил и заглушил». Это точная хирургия. Это когда система понимает, с каким протоколом работает противник, и создаёт помеху, которая идеально «ложится» на его сигнал, не затрагивая ничего лишнего.

И всё это — в экстремальном температурном диапазоне от 40 °С до +50 °С. От арктического холода до пустынной жары. «Двина-100М» работает везде.

Как выразились в холдинге «Росэл», «на сегодня Двина-100М — одна из самых современных систем подавления, которая эффективно противостоит вражеским БПЛА». И я с ними согласен.

«Фумигатор»: от солдата до бронемашины

А теперь — о том, что я считаю самым человечным из всех комплексов РЭБ. О том, что защищает не объекты, а людей.

«Фумигатор» .

Когда я впервые увидел фотографию бойца с рюкзаком «Фумигатор-Н» на спине, я улыбнулся. Не потому, что это выглядело смешно. А потому, что я понял: наконец-то кто-то подумал о пехоте. О тех, кто идёт в атаку и не может тащить за собой стационарную станцию РЭБ весом в полтонны.

Разработка белорусского ОАО «КБ Радар», «Фумигатор» — это эшелонированный подход в рамках одной линейки. Два комплекса, две задачи, два уровня защиты.

«Фумигатор-Н» — носимый. 12 блокираторов. Работает от аккумуляторов. Защищает личный состав от атак мультикоптеров и FPV-дронов, подавляя их каналы управления, передачи данных и навигации. Создаёт купол радиусом 250-300 метров. И всё это — в рюкзаке, который можно надеть на спину и идти в бой.

«Фумигатор-В» — возимый. 14 блокираторов. Питается от бортовой сети автомобиля или бронемашины. Предназначен для прикрытия техники и стационарных объектов. Обеспечивает непрерывную защиту в движении и на месте.

Оба комплекса построены по модульному принципу: каж-

дый передатчик подавляет определённый частотный диапазон, что позволяет гибко размещать блокираторы на технике, стационарных объектах или в составе мобильных групп, подстраиваясь под конкретные задачи.

И самое главное — они созданы на основе реального боевого опыта. Это не кабинетная разработка, не теоретическая модель. Это система, рождённая в окопах, обкатанная в бою и доведённая до ума инженерами, которые понимают, что нужно солдату на передовой.

Как отметили в Госкомвоенпроме, «Фумигатор — современное решение, созданное с учетом опыта реальных боевых действий, для надежного противодействия беспилотным угрозам».

И знаете, я им верю. Потому что когда я вижу, как система РЭБ может поместиться в рюкзак и защитить штурмовую группу от FPV-дронов — я понимаю, что мы на правильном пути.

«Волна Купол Гарант»: подавление спутниковой связи Starlink

А теперь — о самом амбициозном проекте. О том, что заставило меня пересмотреть всё моё представление о возможностях РЭБ.

«Волна Купол Гарант» .

Когда я впервые услышал о ней, я подумал: «Это невоз-

можно. Нельзя заглушить спутник. Спутник — это не дрон, это космический аппарат на орбите. Как ты можешь до него добраться?».

Но российские инженеры сделали невозможное.

Starlink стал для противника тем, без чего они уже не могут воевать. Это не просто интернет — это управление дронами, координация артиллерии, разведка, связь между подразделениями. Спутники Илона Маска стали костылём, на котором держится вся система управления войсками противника.

И «Волна Купол Гарант» этот костыль ломает.

Как объяснил генеральный конструктор Центра комплексных беспилотных решений Дмитрий Кузякин, система не пытается нарушить связь между дроном и спутником. Она подавляет работу самого спутника, буквально «ослепляя» его на радиочастотах.

Технически это выглядит так: спутники Starlink принимают сигналы от земли в диапазоне 14-14,5 ГГц. Этот диапазон разбит на восемь каналов. «Волна Купол Гарант» работает по принципу заградительных помех: восемь антенн, каждая на свой канал, бьют мощным сигналом прямо в пролетающий спутник. В итоге он перестаёт слышать наземные терминалы — и связь обрывается.

Один комплекс покрывает около 20 квадратных километров — это круг радиусом примерно 2,5 километра. Система разбита на шесть прицепов, по две антенны на каждом.

Если один прицеп уничтожен — остальные продолжают работать.

Стоимость комплекса — около 1,5 миллиона долларов. Дорого? Да. Но когда речь идёт о защите стратегического предприятия, где работают тысячи людей, — тут уже не до бухгалтерии.

У системы есть и слабые места. Мощную станцию РЭБ невозможно сделать малозаметной — её видно и с воздуха, и по излучению. Противник уже начал охоту на такие комплексы. Поэтому «Волну Купол Гарант» нужно прикрывать — мобильными огневыми группами, ПВО, маскировкой.

Но сам факт её существования меняет правила игры. Как сказал Кузякин: «Если связь между дроном и спутником нельзя нарушить, то почему бы не нарушить работу самого спутника или даже не вывести его из строя?».

И это — не просто слова. Это новая философия РЭБ. Не «бороться с сигналом», а «бороться с источником сигнала». Не «глушить дрон», а «ослеплять спутник».

Международный опыт: сравнение подходов

И наконец — о том, что происходит за пределами нашей страны. Потому что война с дронами — это не только российская история. Это глобальный вызов.

США и НАТО.

Американцы подходят к РЭБ системно и дорого. Их флаг-

ман — самолёт радиоэлектронной борьбы EA-18G Growler. Это не просто «глушилка» — это целый боевой комплекс, способный подавлять ПВО противника на десятки километров. Но цена такого решения — сотни миллионов долларов за самолёт и миллионы за каждый час полёта.

На тактическом уровне у американцев есть DroneGun от австралийской компании DroneShield. Компактное, лёгкое (3,2 кг) ружьё, которое нарушает управление, видео и навигационные сигналы на нескольких частотных диапазонах. DroneShield — единственная компания, специализирующаяся исключительно на противодронных системах, которая ближе всего к лидеру рынка для западных клиентов.

Есть и более экзотические решения. Например, THOR — система высокомошного микроволнового излучения для поражения роёв дронов. Или AN/ALQ-249 — новая система РЭБ для истребителей.

Израиль.

Израильтяне — отдельная история. Они живут под дронной угрозой десятилетиями, и их опыт бесценен.

Rafael Drone Dome — комплекс противодействия БПЛА, который уже экспортирован в Великобританию и проходит оценку в странах Персидского залива. Система включает радар, оптику и средства РЭБ, работающие в едином контуре.

Elbit ReDrone — ещё одна израильская система, предназначенная для обнаружения, идентификации и нейтрализации БПЛА.

Storm Shield от Rafael — лёгкий, полностью автономный комплекс РЭБ, который непрерывно отслеживает электромагнитный спектр, обнаруживает враждебные излучения и реагирует с помощью специально разработанных методов дезинформации.

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.