

**ЗАЩИТА ЭКОНОМИЧЕСКИХ И ГРАЖДАНСКИХ ОБЪЕКТОВ ОТ ДРОНОВ:
ПРОБЛЕМЫ И ИХ РЕШЕНИЯ**

Юнусов М.Ю., Алимов Б.Б.

*Ташкентский химико-технологический институт,
Университет военной безопасности и обороны Республики Узбекистан*

На сегодняшний день беспилотники развиваются с такой скоростью, что защиту тоже приходится непрерывно совершенствовать в целях обеспечения безопасности и устойчивости экономических объектов, а также объектов мирного населения. Скорость развития технологий такова, что каждые 3–4 месяца появляются новые поколения дронов. Они способны лететь еще дальше, быстрее и ниже, действовать в условиях радиоэлектронных помех. И в целом системы приближаются к полной автономности в режиме радиомолчания.



Вслед за дронами развиваются технологии защиты. В этой области есть несколько направлений разработки, сочетание которых дает максимальную эффективность. Помимо пассивных методов — купольных конструкций, радиоэлектронной борьбы (РЭБ) и т. п. — используют зенитно-ракетный комплекс (ЗРК), переносной зенитно-ракетный комплекс (ПЗРК). Один из простейших способов реагирования для гражданских предприятий — мобильные группы на автомобилях, вооруженные стрелковым оружием или ПЗРК.

Для защиты предприятия необходимо несколько мобильных групп. Их нужно правильно разместить и скоординировать. Зная принципы размещения защитных систем на конкретном предприятии, например, что есть только мобильные группы и их всего две, можно нанести удар сразу с трех направлений. Так ресурсов на защиту точно не хватит. А ещё дроны могут запустить неподалеку от предприятия. Все это усложняет задачу.

В итоге отдельно взятому предприятию очень сложно защитить себя на 100%. К решению проблемы требуется комплексный подход, возможно, даже не на уровне отдельного гражданского объекта, а в рамках целой отрасли, региона или даже страны.

При рассмотрении задачи с технической точки зрения также возникают соответствующие вопросы. Как будет лететь дрон, заранее неизвестно? Откуда он

появится, на какой высоте и с какой скоростью? Не ясен даже тип объекта. Конечно, это не крылатая ракета, которая летит очень быстро. И если мы говорим об угрозах для гражданской инфраструктуры внутри страны, то с большой вероятностью это будет самолетный далеколетящий тип с большим размахом крыла. Но в целом дрон — сложная цель, со множеством сценариев применения. Чтобы обеспечить защиту гражданского объекта, необходимо обнаружить, идентифицировать, сопровождать и перехватить беспилотник.

Один из распространенных вариантов обнаружения — с помощью радиолокационной станции (РЛС). Но для этого дрон должен иметь большую эквивалентную поверхность рассеяния (ЭПР) и лететь на достаточной высоте — объекты в 15–20 метрах от земли РЛС не видят. Также можно применять радиоразведку, но она бесполезна для обнаружения дронов, летящих в полностью автономном режиме, а в последнее время «дальнобойные» летательные аппараты развиваются именно в этом направлении.



Другой вариант — звуковые датчики. По звуковой сигнатуре можно отличить, трактор это или летательный аппарат. Однако дальность действия подобных датчиков ограничена — до километра — и зависит от характеристик объекта и условий окружающей среды: ветра, влажности и прочих погодных условий. Вдобавок могут быть сложности, связанные с зашумленностью окружающей среды, если предприятие находится в черте города или около железнодорожных станций.

Можно применять оптико-электронные станции. По сути, это камера и тепловизор с системой управления, размещенные на поворотной платформе. Устройство обеспечивает визуальный контроль пространства и по ИК-излучению обнаруживает летательные аппараты. Дальность действия такой станции намного больше, чем у звукового датчика, но меньше, чем у РЛС, — порядка 5 км.

Для реагирования на каждом из этапов защиты объекта требуется время, поэтому чем раньше будет обнаружен беспилотник, тем больше будет запас на последующие этапы. Если опираться на среднюю скорость дрона 200 км/ч, то обнаружить такой объект желательно хотя бы за 15 км до защищаемого объекта, чтобы у системы и оператора было хотя бы минут пять для принятия решений.

Это значит, что нужно иметь РЛС или оптико-электронную станцию, которая работает на дальние расстояния, а километров за 10 до защищаемого объекта (причем

со стороны предполагаемого нападения) разместить звуковые датчики. Так что важен не только состав, но и топология системы, которая зависит от конкретной территории.

Также важен вопрос идентификации летательного аппарата. На этом этапе надо определить тип летательного аппарата. Важно не только отличить гражданский объект от военного, но и понять, какую конкретно угрозу он несет. Для идентификации можно сравнивать записанный звуковыми датчиками звук с известными сигнатурами или сопоставлять изображение объекта с имеющимися в базе. Проблема в том, что системы постоянно совершенствуют. Например, против звуковых датчиков на беспилотники устанавливают сирены, которые сбивают с толку инструменты сравнения звуковых сигнатур, рассчитанные на звук от винта или мотора. Сопровождая идентифицированный объект, системы отслеживают его положение в пространстве. Как правило, задача решается с помощью оптико-электронных станций и соответствующего ПО.

Существует проблема перехвата летательного аппарата. Если система идентифицировала объект как опасный, оператор защитного комплекса принимает решение о перехвате с помощью дронов или других элементов системы. Процесс нельзя запустить в полностью автономном режиме, поскольку есть вероятность ошибочного перехвата гражданского объекта. Сам перехват может происходить как в ручном, так и в автоматическом режиме — с помощью дронов, пулеметов, ракет или лазера — в зависимости от условий. Особенность защиты именно гражданских объектов в том, что примерно в 80% случаев угроза приходит издалека, поэтому используют крупные дальнобойные дроны с размахом крыльев до 7 м. Попытка перехватить такой аппарат дроном с легким корпусом, напечатанным на 3D-принтере, потребует ювелирных действий оператора (и его высокой квалификации), а порой и нескольких попыток перехвата для достижения результата. Так что нужны специализированные перехватчики. Лазер как самостоятельный инструмент тоже не самый оптимальный вариант. Его логично использовать для перехвата небольших летательных аппаратов (это дешево). И его работа очень сильно зависит от погодных условий.



Все компоненты системы защиты должны быть соединены связью, которая будет работать в условиях радиоэлектронной борьбы. Самый простой вариант — проводное подключение. Но для успешной защиты элементы комплекса должны

находиться достаточно далеко друг от друга, а все проводные интерфейсы имеют свою «дальность». Тот же RS-485 ограничен примерно 1,2 км. Альтернатива — оптические линии. Они недешевы, но, возможно, как раз за ним будущее. Проблема с проводным подключением в том, что линии связи приходится размещать за территорией предприятия — а это общедоступные зоны, которые невозможно контролировать.

Помимо проводных линий и оптики, есть радиоканалы. Приходится экспериментировать с частотным диапазоном, направленными антеннами и мощностью передатчика, поскольку один из элементов пассивной защиты — радиоэлектронная борьба. Мощность РЭБ, как правило, ограничена — антенна излучает мощный сигнал в узком частотном диапазоне или затрагивает более широкий диапазон, но с сигналом меньшей мощности. При этом РЭБ «накрывает» определенную зону. Зная, как именно работает РЭБ на предприятии, можно выбрать рабочие частоты или мощности. В этих экспериментах тоже много нюансов, особенно с учетом того, что радиочастотный спектр можно анализировать и глушить либо использовать другие диапазоны. Также можно использовать различные топологии сетей. Например, у Mesh-сетей, передающих данные между соседними узлами (а не между узлами и условным центром), устойчивость выше.

Передача данных по воздуху с помощью оптического передатчика и приемника позволяет работать на значительно больших расстояниях, но все, что с ней связано, кратно увеличивает стоимость системы. Кроме того, требуется точная настройка приемо-передающего оборудования.

В целом существуют разные подходы, но нет никакого конкретно определённого решения. Требуется комплексный подход, который можно менять в зависимости от условий.

Разработка защиты сталкивается не только с техническими сложностями. Это такой же рынок, у которого есть свои особенности и ограничения. Например, разработчики решений для гражданского применения не могут использовать военные технологии, специализированные стандарты связи и зарезервированные частотные диапазоны.

Кроме того, не имея соответствующей лицензии, гражданские дроны не могут нести в себе взрывчатые вещества, т. е. им доступен только кинетический перехват. Поэтому приходится либо придумывать альтернативные идеи (ограничиваться кинетическим перехватом), либо кооперироваться с теми, у кого есть соответствующие лицензии и возможности. Второй вариант несет дополнительные сложности как на этапе производства, так и при последующей эксплуатации. Без специального разрешения предприятие-заказчик не может использовать это изделие.

Поэтому разработчики торопятся — сокращают НИР и исследования, сразу переходят к конструкторским работам. А предварительное исследование нужно хотя бы для того, чтобы грамотно разработать и оформить технические условия на

продукцию. Иначе можно столкнуться с большим количеством неучтенных моментов и переделок, которые отнимут много сил и денег.

При этом решение должно быть адекватным по соотношению цены и ценности. Поясню на примере шифрования: более сложный алгоритм, обеспечивающий высокую степень защиты информации при передаче между частями системы, как правило, требует больше вычислительных ресурсов. А ресурсы стоят денег. То есть использование более сложного шифрования может выкинуть систему с рынка — сделать неконкурентоспособной. Так что приходится детально прорабатывать требования к системе. В примере с шифрованием — искать минимально достаточные алгоритмы, которые обеспечат сохранность информации лишь в течение ее требуемого «срока жизни».

А еще есть проблема закрытости разрабатываемых решений. Любая информация, появившаяся в публичном поле, мгновенно устаревает. Это заставляет команды скрывать подробности решения — иначе высоки риски потратить деньги на разработку того, что априори не защищает.

В итоге даже на профильных мероприятиях разработки представлены без характеристик и технических подробностей, и составить представление о рынке довольно сложно.

Прямые обращения к компаниям-разработчикам тоже встречают не самый теплый прием — общение происходит на официальном языке письмами от имени юридического лица. Прорабатывать и тестировать совместные решения в таких условиях очень тяжело. Приходится многие вещи создавать самостоятельно, поскольку использовать партнерские компоненты не получается. Это удлиняет время разработки.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

1. M.Yunusov, B.Alimov, O‘ta muhim va toifalangan obyektlarda yong‘in xavfsizligini ta‘minlashda uchuvchisiz uchish apparatlarining ahamiyati, O‘zbekiston Respublikasi Favqulodda vaziyatlar vazirligi Akademiyasi, “O‘ta muhim va toifalangan obyektlarning yong‘in xavfsizligini ta‘minlashning dolzarb masalalari: muammo va yechimlar” mavzusidagi ilmiy-amaliy anjuman materiallari to‘plami Toshkent sh., 2025-yil 18-dekabr, 429-432 betlar.

2. B.B.Alimov, S.F.Raimqulov, Obyektlarning yong‘in xavfsizligini ta‘minlashda kuch va vositalarning ishlash uslublari // O‘zbekiston Respublikasi Fuqaro muhofazasi instituti, “Fan, muhofaza, xavfsizlik” jurnali, 2019 yil, №2 (3) 71-74 betlar.

3. B.B.Alimov, S.F.Raimqulov, Yengil alanganuvchi va yonuvchi suyuqliklar omborlarining yong‘in xavfsizligini ta‘minlash choralari // O‘zbekiston Respublikasi Favqulodda vaziyatlar vazirligi Akademiyasi, ilmiy-amaliy anjumani materiallari to‘plami. 2020 yil 13 mart. 175-178 betlar.

4. B.B.Alimov. Iqtisodiyot obyektlari faoliyatining barqarorligini ta‘minlash // O‘zbekiston Respublikasi Favqulodda vaziyatlar vazirligi Akademiyasi, «Favqulodda

“O‘ZBEKISTONDA UCHINCHI RENESSANS VA INNOVATSION JARAYONLAR JURNALI”

20-Iyul, 2026-yil

vaziyatlarni oldini olishning dolzarb muammolari va amaliy yechimlari” respublika ilmiy-
amaliy anjumani materiallari to‘plami, 2022 yil 22 iyun, Toshkent sh. 286-288 betlar.