УДК 623.746.519

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ СВЯЗИ В СИСТЕМАХ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

А. Н. БЕЛЕГОВ, А. В. АСКЕРКО, Р. А. РАЦ
Военная академия Республики Беларусь
Минск, Беларусь

Стремительное развитие технологий беспилотной авиации привело к массовому внедрению как разведывательных, так и ударных беспилотных летательных аппаратов (БПЛА) в военные структуры. Сегодня они выступают не только как средство тактической разведки и ретрансляции, но и как эффективное оружие для точечного поражения целей в реальном времени [1].

Одновременно с этим ведущие мировые державы активно разрабатывают тактику «роя БПЛА», предполагающую координированное применение множества аппаратов для одновременного воздействия по всем типам целей с минимальными потерями [2].

Типовая архитектура сети БПЛА (рис. 1) строится на двух основных типах соединений: вертикальных (БПЛА – наземная станция управления) и горизонтальных (БПЛА – БПЛА) [3]. Однако функционирование в открытой беспроводной среде делает такие сети крайне уязвимыми для внешних помех, перехвата управления и целенаправленных кибератак [4].

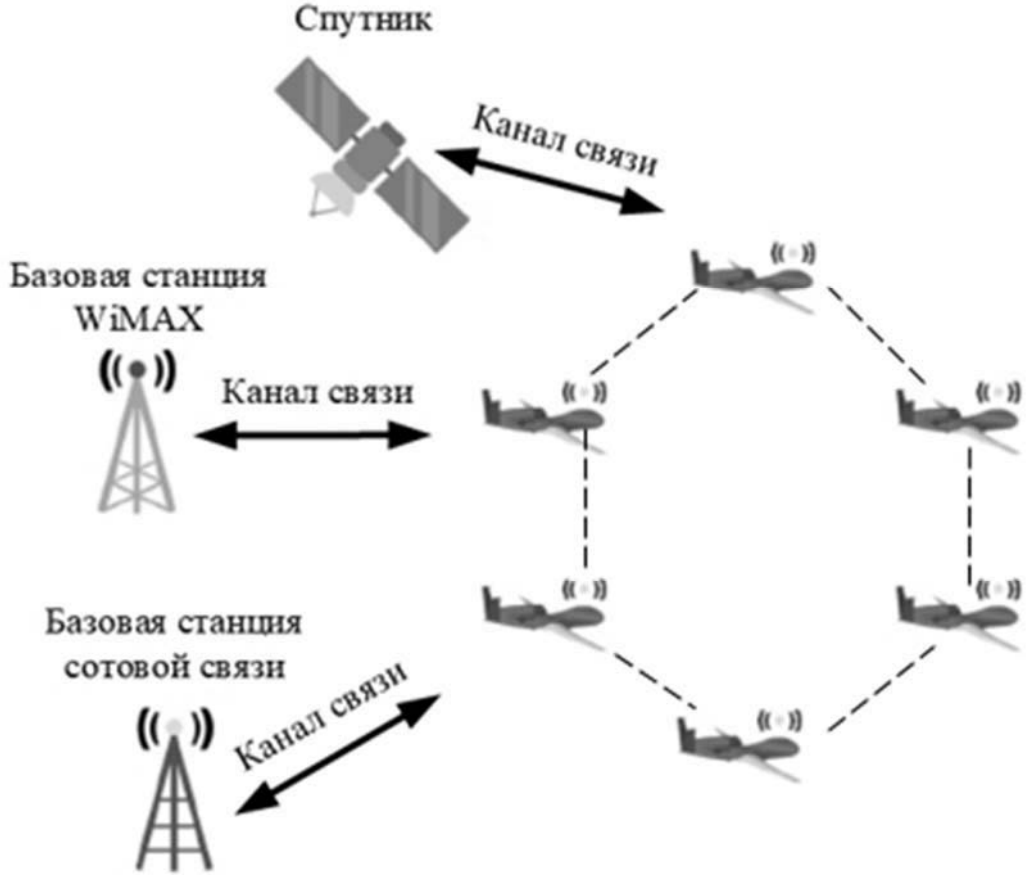

Рис. 1. Модель архитектуры сети БПЛА

Помимо сетевых угроз, существуют и технические ограничения. Корпус беспилотного аппарата с его углами, кромками и выступающими элементами вызывает перераспределение вторичных токов, что приводит к значительному искажению формы диаграммы направленности бортовых антенн [2].

Надёжная связь является критическим условием выполнения боевых задач. БПЛА должны обеспечивать устойчивую коммуникацию в любом направлении, а при необходимости – выполнять функции ретрансляторов, увеличивая зону покрытия и живучесть всей группировки.

Особого внимания заслуживают вопросы информационной безопасности. Связь с наземным оператором осуществляется через динамически формируемую сеть «на лету», однако частая смена топологии, высокая мобильность и ограниченный ресурс каналов создают благоприятную среду для злоумышленников [1]. Передача больших объёмов видео- и телеметрической информации перегружает полосу пропускания, провоцируя сбои и потерю управления. Возникающие задержки открывают возможности для атак переполнения буфера, постановки помех, DDoS-атак и манипуляции протоколами маршрутизации [2]. На физическом уровне возможно глушение каналов связи, а на сетевом – изоляция отдельных устройств от общей инфраструктуры. В условиях дефицита пропускной способности аппараты вынужденно переходят в автономный режим, что повышает риски несанкционированных действий и снижает эффективность [5].

Таким образом, эффективность применения группировок БПЛА в современных конфликтах определяется не только тактическими и техническими характеристиками аппаратов, но и устойчивостью, защищённостью и адаптивностью их сетей связи. Основными препятствиями остаются электромагнитная несовместимость бортового оборудования, искажение антенных характеристик из-за конструктивных особенностей корпуса, а также широкая уязвимость каналов управления к кибератакам всех уровней.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. **Куижева, С. К.** Анализ протоколов связи для автономных беспилотных летательных аппаратов, выполняющих совместный полет / С. К. Куижева, В. А. Довгаль // Вестник ДонНУ. Серия Г. Технические науки. – 2025. – № 2. – С. 76–84.

2. Оценка характеристик производительности беспроводной сети на базе привязных БПЛА / В. М. Вишневский, Ю. А. Авраменко, В. Х. Нгуен, Н. С. Калмыков // Проблемы информатики. – 2025. – № 1. – С. 60–77.

3. Selection of Routing Metrics and Service Channel Characteristics of ad hoc Network for UAV swarm / V. Borodin, A. Selin, V. Kolesnichenko, M. Kalyagin // Journal of Aerospace Technology and Management. – 2024. – Vol. 16.

4. **Patil, A.** Performance of UAV Networks Over the Ocea n: A Perspective Towards Connected Ocean / A. Patil, P. Muthuchidambaranathan, D. N. K. Jayakody // Wireless Personal Communications. – 2024. – Vol. 134, № 1. – P. 347–366.

5. **Урюпин, И. В.** Об универсальных моделях состояния для задач слежения и навигации беспилотных движущихся объектов / И. В. Урюпин // Системы и средства информатики. – 2025. – Т. 35, № 2. – С. 31–44.