УДК 623.76

Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 3. Радиоэлектронное подавление систем навигации и радиосвязи

Макаренко С. И.

Актуальность. *Начиная с середины 2000-х годов в средствах массовой информации стали регулярно появляться сообщения о несанкционированном использовании беспилотных летательных аппаратов (БПЛА) в особо контролируемых зонах: в аэропортах, на военных объектах, против критической промышленной инфраструктуры и т.д. В настоящее время малые БПЛА широко используются для несанкционированного наблюдения важных объектов, проведения терактов и диверсий, переноски запрещенных грузов (оружия, наркотиков), а также в военном деле. В связи с этим, актуализировалась задача противодействия БПЛА, и особенно – малым БПЛА. Анализ публикаций в этой области, показывает, что аналитических статей по данной тематике довольно мало. В подавляющем числе работ в этой области преобладают излишне оптимистические выводы относительно эффективности противодействия БПЛА существующими средствами радиоэлектронного подавления (РЭП). Вместе с тем, проблема противодействия БПЛА, и, в особенности, малым БПЛА, является чрезвычайно сложной, многогранной и до сих пор эффективно не решенной.* ***Целями работы*** *являются систематизация и анализ различных способов и средств противодействия БПЛА, а также формирование общих направлений эффективного решения данной проблемы. Материал, представленный в данной статье, в частности, посвящен анализу возможностей средств РЭП в части подавления систем навигации и радиосвязи БПЛА.* ***Результаты.*** *В статье представлены результаты систематизации и анализа различных способов и средств радиоэлектронного подавления БПЛА, основанных на нарушении функционирования их навигационных систем, командных радиолиний управления и радиолиний передачи данных бортовых средств полезной нагрузки. В основу систематизации положено более 140 открытых источников, анализ которых позволил вскрыть основные особенности БПЛА, как объекта радиоэлектронного подавления, а также провести многоаспектный подробный анализ современных комплексов радиоэлектронной борьбы и их эффективности при работе по воздушным целям такого типа.* ***Элементами новизны работы*** *являются выявленные особенности процессов радиоэлектронного подавления БПЛА, а также системные недостатки используемых технологических решений в комплексах радиоэлектронной борьбы, приводящих к снижению их эффективности при применении против БПЛА.* ***Практическая значимость.*** *Материал статьи может использоваться для формирования исходных данных для моделирования и исследования эффективности комплексов радиоэлектронной борьбы при их противодействии БПЛА. Также, данная статья может быть полезна конструкторам, проектирующим системы РЭП для противодействия БПЛА, а также специалистам при оценке параметров группы БПЛА, гарантированно вскрывающих и преодолевающих зону радиоэлектронного подавления противника при решении своих целевых задач.*

Ключевые слова: *беспилотный летательный аппарат, БПЛА, БЛА, противодействие беспилотным летательным аппаратам, подавление беспилотного летательного аппарата, радиоэлектронное подавление, радиоэлектронная борьба, навигационная система, спутниковая радионавигационная система, инерциальная навигационная система, командная радиолиния управления, помехозащищенность, помехоустойчивость.*

Библиографическая ссылка на статью:
Макаренко С. И. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 3. Радиоэлектронное подавление систем навигации и радиосвязи // Системы управления, связи и безопасности. 2020. № 2. С. 101-175. DOI: 10.24411/2410-9916-2020-10205.

Reference for citation:
Makarenko S. I. Counter Unmanned Aerial Vehicles. Part 3. Electronic Warfare against Navigation and Radio Connection Subsystems of Unmanned Aerial Vehicles. *Systems of Control, Communication and Security*, 2020, no. 2, pp. 101-175 (in Russian). DOI: 10.24411/2410-9916-2020-10205.

Введение

С появлением средних и малых беспилотных летательных аппаратов (БПЛА) задачи противодействия их применению в особо контролируемых зонах существенно актуализировались. Начиная с середины 2000-х годов в средствах массовой информации стали регулярно появляться сообщения об опасном использовании малых БПЛА в районах аэропортов, а с середины 2010-х – об применении малых БПЛА для ведения несанкционированного наблюдения важных объектов, проведения терактов и диверсий, транспортировки запрещенных грузов (оружия, наркотиков), и широком использовании БПЛА в военном деле. В связи с этим на Западе началась активная научная разработка данного направления исследований, о чем можно судить по работам [1-9]. При этом данная проблематика является относительно новой, так как самая ранняя из работ по тематике противодействия БПЛА относится к 2008 г., а начало активных научных публикаций по этой тематике относится к 2016-2017 гг. В результате к 2020 г. в Западной научной печати были введены относительно устоявшиеся термины, а также определены основные направления исследований в этой предметной области: «противодействие БПЛА» – используются такие термины как «C-UAV», «CUAV», «C-UAVs», «CUAVs» (Counter Unmanned Aerial Vehicles); «системы противодействия БПЛА» – используются такие термины как «C-UAS», «CUAS» (Counter Unmanned Aircraft Systems), «C-UAV system», «CUAV-system», «AUDS» (Anti-UAV Defense System), Counter-Drone Systems; «технологии противодействия БПЛА» – используются такие термины как «Anti-Drone Technologies» и «Counter-UAVs Technologies».

При этом, если на начальном этапе появления задачи противодействия БПЛА (в начале 2000-х гг.), эта задача решалась исключительно средствами поражения зенитно-ракетных комплексов (ЗРК) противовоздушной обороны (ПВО), то в настоящее время специалисты осознали, что прямое отражение массированного налета БПЛА средствами ЗРК ПВО, во-первых, неоправданно экономически из-за использования дорогостоящих ракет по большому числу относительно дешевых БПЛА, а во-вторых, это ведет к быстрому исчерпанию боевого ресурса ЗРК и последующей их неспособности отразить удар уже пилотируемой авиации, а также крылатых ракет высокоточного оружия (ВТО). В связи с этим, в настоящее время широко исследуются дополнительные способы противодействия БПЛА, в том числе такие как применение средств радиоэлектронного подавления (РЭП), а также средств направленного излучения энергии – лазерного оружия. При этом, если применение лазерного оружия является еще относительно экспериментальной технологией, то способы противодействия БПЛА на основе совместного использования комплексов РЭП и ЗРК уже активно используются в практике локальных боевых действий (например, при действиях войск Воздушно-космической обороны (ВКО) России в Сирии), а также для формирования периметра защиты особо охраняемых объектов (например, специальных объектов РФ – объектов МО, МВД, ФСО, ФСИН и т.д.).

Анализ публикаций в области противодействия БПЛА показывает, что статей по данной тематике довольно мало, а в подавляющем числе работ в этой

области преобладают излишне оптимистические выводы относительно успешности поражения всех видов БПЛА существующими отечественными средствами ПВО или же глубокое убеждение авторов в поистине «фантастических» возможностях средств РЭП. При этом многие авторы не вполне понимают сложность задачи противодействия БПЛА, рассматривают исключительно отдельные, частные аспекты этой проблематики, а также не обладают сведениями о реальных возможностях существующих комплексов ПВО и РЭП. Вместе с тем, проблема (как видится автору – именно проблема) противодействия БПЛА, и, в особенности, малым БПЛА, является чрезвычайно сложной, многогранной, и до сих пор эффективно не решенной. Автор, имея определенный опыт разработки подобных систем, хотел бы отразить в данной работе всю сложность и многоаспектность проблематики разработки эффективных систем противодействия БПЛА, а также неприемлемость «поверхностных» и «однобоких» подходов к построению таких систем.

Обобщая вышесказанное, целями работы являются систематизация и анализ различных способов и средств противодействия БПЛА, а также формирование общих направлений эффективного решения данной проблемы.

Авторский материал по противодействию БПЛА, ввиду его большого объема, был разделен на несколько относительно независимых частей. Первая часть, представленная в статье [10], посвящена анализу БПЛА как объекта обнаружения и поражения. Вторая часть, представленная в статье [11], посвящена исследованию возможностей средств огневого поражения и физического перехвата БПЛА. Третья часть, представленная в этой статье, посвящена исследованию возможностей средств РЭП по подавлению систем управления, связи и навигации БПЛА. В следующей работе предполагается рассмотреть противодействие БПЛА средствами функционального поражения электромагнитным излучением (ФП ЭМИ) – генераторами мощного сверхвысокочастотного (СВЧ) и лазерного излучения.

Материал данной статьи, ввиду своей объемности, декомпозирован на ряд логических подразделов.

1. Особенности противодействия БПЛА средствами РЭП.
2. Состав и характеристики типовых комплексов РЭП.
   2.1. Боевые комплексы РЭП.
   2.2. Коммерческие комплексы РЭП.
   2.3. Малогабаритные носимые средства РЭП.
3. Радиоэлектронное подавление навигационной системы БПЛА.
   3.1. Проблемные вопросы радиоэлектронного подавления навигационной системы БПЛА.
   3.2. Особенности радиоэлектронного подавления навигационной системы БПЛА, основанной на приеме сигналов спутниковых радионавигационных систем (СРНС).
   3.3. Особенности радиоэлектронного подавления интегрированной навигационной системы БПЛА, основанной на комплексировании данных микромеханических инерциальных систем и сигналов СРНС.

3.4. Возможности акустического подавления автономной навигационной системы БПЛА, основанной на микромеханических инерциальных системах.

4. Радиоэлектронное подавление радиолиний управления и передачи данных БПЛА.
   4.1. Проблемные вопросы радиоэлектронного подавления радиолиний управления и передачи данных БПЛА.
   4.2. Особенности организации связи в командной радиолинии управления БПЛА.
      4.2.1. Специальные и военные БПЛА.
      4.2.2. Коммерческие БПЛА.
   4.3. Особенности организации связи в радиолиниях передачи данных с БПЛА.
      4.3.1. Специальные и военные БПЛА.
      4.3.2. Коммерческие БПЛА.
   4.4. Особенности радиоэлектронного подавления радиолиний управления и передачи данных БПЛА.
   4.5. Особенности информационно-технического воздействия с целью вмешательства в процесс функционирования систем БПЛА или перехвата управления.

Данная работа продолжает и развивает предыдущие работы автора, опубликованные по тематике оценки эффективности применения БПЛА и способов противодействия им, а именно – работы [10-13].

1. Особенности противодействия БПЛА средствами РЭП

В работе [11] показано, что поражение БПЛА средствами ЗРК ПВО, в большинстве случаев, является низкоэффективным, при этом приводит в высокому расходу боеприпасов – невосполнимого материального ресурса. В связи с этим перспективным направлением противодействия БПЛА считается примените средств РЭП, ресурс которых, при наличии внешнего питания, практически неограничен. При этом средства РЭП могут применяться одним из нескольких способов или их комбинацией:

- подавление или навязывание ложных режимов работы командной радиолинии управления (КРУ) и радиолиниям передачи данных БПЛА;
- подавление или навязывание ложных режимов работы каналу навигации БПЛА, основанному на приеме и обработке сигналов одной или нескольких СРНС.

Этапу применения средств РЭП предшествует вскрытие средствами радио- и радиотехнической разведки (РТРР) факта полета БПЛА как источника радиоизлучения (ИРИ), вскрытие сигнально-частотных параметров КРУ и сигналов СРНС, которые потенциально могут быть использованы для навигации БПЛА в данном районе. Эти сигнально-частотные параметры предаются средствам РЭП в качестве целеуказания. Особенности ведения РРТР против БПЛА рассмотрены в работе [10].

Применение средств РЭП против БПЛА по сравнению со средствами огневого поражения обладает следующими преимуществами:

- в процессе применения средства РЭП не расходуют каких-либо материальных средств поражения, а только возобновляемый ресурс электромагнитной энергии;
- средства РЭП обладают «площадным эффектом», позволяющим одновременно поражать большое количество БПЛА, имеющих сходное радиоэлектронное оборудование (РЭО), единую КРУ, принципы навигации, основанные на использовании сигналов одних и тех же СРНС;
- при условии успешного разрешения целей, как отдельных источников радиоизлучений (ИРИ), средства РЭП могут быть избирательными, подавляя только ИРИ с определенными параметрами, например, пункт управления (ПУ) БПЛА формирующий КРУ с определенной структурой сигналов, или сигналы определенной СРНС;
- в отдельных случаях, при условии успешного вскрытия структуры сигналов и формата передаваемых сообщений в КРУ и в канале навигации, средства РЭП позволяют перехватить управление БПЛА и навязать ему ложную траекторию полета.

Вместе с тем, одновременно с вышеуказанными достоинствами, средствам РЭП свойственны и определенные недостатки:

- воздействие средств РЭП возможно только при условии соблюдения электромагнитной доступности БПЛА;
- подавление канала управления и навигации БПЛА возможно только при условии активного дистанционного управления БПЛА, с использованием навигации по сигналам СРНС. Полет БПЛА в режиме «радиомолчания» по заблаговременно заложенной программе, как правило, не позволяет вскрыть факт полета такого БПЛА средствами РРТР и, соответственно, сформировать целеуказания средствам РЭП на противодействие таким БПЛА;
- применение средств РЭП против БПЛА в условиях мирного времени ограниченно относительно небольшой мощностью, вследствие необходимости выполнения требований по электромагнитной совместимости (ЭМС) с другими радиоэлектронными средствами (РЭС). Эти РЭС могут находиться как на защищаемом от БПЛА объекте, так и могут являться другими средствами противодействия БПЛА, которые, наряду со средствами РЭП, интегрированы в комплекс противодействия, например, радиолокационные станции (РЛС) или средства РТРР обнаружения БПЛА;
- энергетическая эффективность средств РЭП убывает пропорционально квадрату расстояния, вследствие этого средства РЭП являются средствами ближнего действия, причем их эффективность возрастает по мере приближения БПЛА к месту расположения средств РЭП (контролируемому рубежу);
- заградительные помехи, обладающие «площадным эффектом» и ориентированные на подавление нескольких каналов управления и нави-

гации, одновременно с этим имеют и низкую энергетическую эффективность, особенно, в условиях использования для управления и навигации БПЛА широкополосных сигналов (ШПС) и сигналов с псевдослучайной перестройкой рабочей частоты (ППРЧ);

- помехи, прицельные по частоте и структуре сигналов КРУ и СРНС, которые являются наиболее эффективными для нарушения управления БПЛА, в том числе, путем навязывания ложных режимов полета. данные тип помех для своего формирования требует либо оперативного вскрытия средствами РРТР структуры сигналов и формата передаваемых сообщений в КРУ и в канале навигации, либо заблаговременного формирования баз данных (БД) соответствующих сигналов, используемых БПЛА. В результате, такие высокоэффективные помехи эффективно могут быть использованы только против ограниченного числа отдельных моделей БПЛА, а основанные на этих помехах способы подавления – как отдельные режимы, более пригодные для демонстрации возможностей средств РЭП, чем для реального противодействия налету группы БПЛА;
- эффективность средств РЭП существенно зависит от сценария применения БПЛА, профиля их полета, уровня автономности и т.д. Изначальный учет в сценарии применения БПЛА возможности использования против них средств РЭП, выбор профиля полета на низкой высоте, с учетом складок местности, заблаговременное формирование для навигационной системы профиля полета по электронной карте местности, соблюдение режима «радиомолчания», а также применение других способов радиоэлектронной защиты БПЛА, существенно снижает возможности средств РЭП.

Основным недостатком средств РЭП, основанных на подавлении каналов управления и навигации БПЛА радиоэлектронными помехами, является то, что излучение соответствующих помех никак не гарантирует требуемой реакции БПЛА на подобное воздействие, а именно – прекращение полета в направлении защищаемого объекта. Действия БПЛА в результате воздействия могут варьироваться в широком диапазоне, от продолжения полета по заданной траектории (например, за счет использования лазерного высотомера и электронной карты местности) до включения «режима возврата» на своей ПУ.

Обобщая вышесказанное, можно сделать вывод о том, что средства РЭП действительно являются высокоэффективным и перспективным средством противодействия БПЛА, однако на современном этапе своего развития они не позволяют самостоятельно гарантированно предотвратить полет БПЛА к контролируемому периметру, имеют ограничения по применимости, в связи с необходимостью обеспечения ЭМС с другими РЭС, не обладают высокой степенью избирательности в отношении поражаемых целей, и как следствие – могут быть использованы в составе комплекса противодействия БПЛА только в совокупности с другими средствами, прежде всего, со средствами физического и огневого поражения.

2. Состав и характеристики типовых комплексов РЭП

Рост угрозы со стороны БПЛА, привел к резкому повышению предложений, со стороны производителей соответствующих средств. Анализ информации, доступной из открытых источников и на сайтах производителей [14-21], показывает, что в настоящее время доступен широкий спектр комплексов РЭП, специально ориентированных на противодействие БПЛА. К таким комплексам можно отнести комплексы РЭП: Р-330Ж «Житель», «Шиповник-АЭРО», «Репеллент-1», «Серп», «Атака-DBS», «Заслон», «Крона-2М», «Солярис-Н», «REX 1», «Пищаль-ПРО», «Таран-ПРО», «Stupor» и многие др. При этом данные комплексы можно четко разделить на три типа, каждый из которых имеет принципиально разные возможности и особенности применения:

1) «боевые» комплексы РЭП, имеющие относительно высокий энергетический потенциал и большую дальность действия, ориентированные на применение в условиях мирного и военного времени против БПЛА, в том числе, специального и военного назначения (к таким комплексам можно отнести: Р-330Ж «Житель», «Репеллент-1», «Шиповник-АЭРО»);
2) «коммерческие» комплексы РЭП, имеющие относительно невысокий энергетический потенциал и среднюю дальность действия, ориентированные на защиту периметра критических объектов от малых БПЛА-квадрокоптеров исключительно в мирное время (к таким комплексам можно отнести: «Серп», «Заслон», «Атака-DBS», «Крона-2М», «Солярис-Н» и др.);
3) малогабаритные носимые средства РЭП, имеющие относительно низкий энергетический потенциал и малую дальность действия, ориентированные на использование одним человеком против одного или нескольких БПЛА, выполненные в формате «носимого орудия» (к таким средствам можно отнести: «REX 1», «Пищаль-ПРО», «Таран-ПРО», «Stupor» и др.).

Рассмотрим возможности и особенности применения данных комплексов РЭП более подробно.

2.1. Боевые комплексы РЭП

Наземными комплексами РЭП комплектуются соответствующие батальоны мотопехотных и бронетанковых дивизий. Данные комплексы предназначены для выявления и радиоэлектронного подавления систем и средств КВ и УКВ радиосвязи, а также РЛС в тактическом звене управления в частях сухопутных войск, в армейской и фронтовой авиации на дальности до 100 км.

В работах [22, 23] рассмотрены такие наземные комплексы РЭП как: AN/TLQ-17A (V)1 Traffic Jam, AN/ALQ-151(V)2 Quick Fix II, IEWCS, EFVS, AN/MLQ-40 Prophet, Р-378, Р-330, Р-325У, Р-939Б, МВША «Атлант». Принимая эти средства как прототипы, возможно сформировать обобщенные ТТХ типового комплекса РЭП.

Типовой комплекс РЭП выполняет следующие задачи:

- ведение РРТР;
- обработка разведывательных данных и формирование карты текущей радиоэлектронной обстановки;
- определение параметров и координат ИРИ для обеспечения целеуказания и оценки эффективности подавления;
- осуществление радиоэлектронного подавления средств связи и радиолокации в зоне своей ответственности.

Как правило, современные комплексы РЭП состоят из двух подсистем:

1) воздушная подсистема (на основе средств РРТР, размещенных на вертолетах армейской авиации и/или на тактических БПЛА);
2) наземная подсистема (на основе территориально-распределенной группировки средств РЭП).

Воздушная подсистема комплекса РЭП обеспечивает ведение РРТР, а также РЭП объектов, находящихся на удалении 15-30 км от мест размещения элементов наземной подсистемы комплекса РЭП. В качестве носителей средств воздушной подсистемы выступают вертолеты и тактические БПЛА. Воздушная подсистема способна обнаруживать, идентифицировать, определять местоположение, а также осуществлять радиоэлектронное подавление ИРИ.

Обобщенные тактико-технические характеристики (ТТХ) средств РРТР воздушной подсистемы комплекса РЭП [22]:

- диапазон частот, в котором ведется РРТР: 1,5-3000 МГц;
- зона ведения разведки: 150×50 км;
- точность пеленгования: 0,5°-1°;
- точность определения местоположения ИРИ: на расстоянии до 40 км – 150-500 м; на расстоянии 80-120 км – 450-1500 м;

ТТХ средств РЭП воздушной подсистемы комплекса РЭП [22]:

- диапазон частот, в котором ведется подавление: 20-450 МГц;
- мощность излучения помех: 40-150 Вт;
- ширина мгновенно подавляемой полосы частот: 10-25 кГц.

Радиоразведка и постановка радиопомех средствами воздушной подсистемы осуществляются с высоты полета 60-180 м в течение 2-2,5 ч на удалении 5-15 км от линии соприкосновения войск и на глубину до 30 км [22].

Наземная подсистема обеспечивает вскрытие радиоэлектронной обстановки и постановку помех для линий радиосвязи преимущественно в УКВ диапазоне, при координации совместных действий средств РРТР и РЭП наземной и воздушной подсистем.

Типовые ТТХ средств РРТР наземной подсистемы комплекса РЭП [22, 23]:

- диапазон частот, в котором ведется радиоразведка (РР): 20-15000 МГц;
- зона ведения разведки: 150×120 км;
- мгновенная полоса обзора: около 2,5 ГГц;
- разрешающая способность: не хуже 1 кГц;
- скорость поиска в разведываемом диапазоне: порядка 3000 ГГц/с;
- чувствительность (при отношении сигнал/шум (ОСШ) на входе приемника не менее 10 дБ в полосе частот 20 кГц): не хуже 5 мкВ/м;

- вероятность распознавания вида сигнала и типа РЭС за время 0,2 с: не менее 0,8;
- точность пеленгования: 0,5°-1°.

Типовые ТТХ средств подавления наземной подсистемы комплекса РЭП [22, 23]:

- диапазон частот, в котором ведется подавление: 1,5-2500 МГц (в перспективных образцах – до 6 ГГц);
- мощность излучения помех: 0,5-1 кВт;
- высота антенн средств РЭП: 6-20 м;
- количество одновременно подавляемых целей: 5-300;
- ширина спектра помех: прицельных по частоте 3-50 кГц; заградительных 150-3000 кГц;
- время реакции при постановке помех: по неизвестной частоте 0,8 с; по известным частотам 0,04 с;
- обнаружение и подавление РЭС с режимом ППРЧ до 1000 скачков/с;
- дальность подавления: до 100 км.

Необходимо отметить, что вышеуказанные ТТХ относятся к комплексам РЭП общего назначения. Вместе с тем, в последние время на вооружение активно поступают комплексы РЭБ, специально ориентированные на противодействие именно БПЛА.

Обобщая данные об отечественных комплексах Р-330Ж «Житель», «Шиповник-АЭРО», «Репеллент-1» [16, 18, 19, 24], можно сформировать обобщенные ТТХ боевого комплекса РЭП, ориентированного на противодействие БПЛА.

ТТХ подсистемы РРТР:

- диапазон частот, в котором ведется РРТР: 200-6000 МГц;
- дальность разведки ПУ БПЛА: до 10-30 км;
- дальность разведки БПЛА: до 30-50 км;
- вероятность пеленгования сигналов типа ППРЧ со скоростью не менее 1000 скачков/с: не менее 0,85;
- среднеквадратическая ошибка (СКО) пеленгования ИРИ в диапазоне от 200 до 6000 МГц: не более 2°.

ТТХ подсистемы РЭП:

- диапазон частот, в котором ведется подавление: 200-6000 МГц;
- подавление литерных частот:
    а) частоты типовых каналов нелицензированных средств радиосвязи: 20-80, 135-174, 400-470 МГц;
    б) частоты типовых каналов авиационной радиосвязи в диапазоне 220-400 МГц;
    в) частоты типовых каналов коммерческих систем связи: 430-460, 860-880, 902-928 МГц, CDMA800 (850-894 МГц), GSM900 (890-915, 935-960 МГц), GSM1800 (1710-1880 МГц), 3G (2110-2170 МГц), 4G (725-770, 780-960, 925-960 МГц; 1,7-2,2, 2,5-2,7 ГГц), Wi-Fi (2,4-2,5, 4,9-6,425 ГГц);

г) частоты каналов «вниз» спутниковых систем связи (ССС) L-диапазона: Инмарсат (1518-1660,5 МГц), Иридиум (1616-1626,5 МГц);
д) частоты каналов СРНС: GPS (L1 – 1575,42 МГц / L2 – 1227,6 МГц / L5 – 1176,45 МГц), ГЛОНАСС (L1 – 1602 МГц / L2 – 1246 МГц), BeiDou (B1 – 1561,098 МГц / B2 – 1207,14 МГц / B3 – 1268,52 МГц), Galileo (E1 – 1575,42 МГц / E6 – 1278,75 МГц / E5 – 1191,79 МГц);

- дальность подавления приемных трактов:
  а) средств связи на ПУ: до 10-25 км;
  б) средств связи на БПЛА: до 30-50 км;
  в) канала СРНС на БПЛА: до 30-50 км;
- энергопотенциал воздействия:
  а) на канал передачи данных «БПЛА – ПУ»: 300-500 Вт;
  б) на канал управления «ПУ – БПЛА» и телеметрии «БПЛА – ПУ»: 500-1000 Вт;
  в) на канал СРНС на БПЛА: 300-1000 Вт;
- тип формируемых помех:
  а) для каналов связи и управления: прицельная и скользящая по частоте, заградительная по диапазону частот;
  б) для канала навигации по СРНС: прицельная по частоте и структуре сигнала с целью формирования ложной навигационной информации (по открытым частотам СРНС); шумовая прицельная по частоте (по открытым или закрытым частотам СРНС).

Отметим, что в ТТХ некоторых комплексов указывается опциональная возможность формирования ложных режимов работы для каналов управления и навигации БПЛА, которая называется «перехват управления». Вместе с тем, производители данных комплексов, как правило, подробно не раскрывают механизмы такого «перехвата», и что конкретно под ним понимается. Более подробно возможность формирования ложных режимов работы для каналов управления и навигации БПЛА будет рассмотрена далее, здесь же необходимо отметить, что подобная функциональность может быть реализована в отношении исключительно отдельных типов БПЛА, принципы функционирования которых были заблаговременно изучены, и в соответствии с ними были сформированы соответствующие программы «перехвата управления».

В целом боевые комплексы РЭП противодействия БПЛА являются эффективным средством решения задач подавления каналов управления и навигации. Недостаточная «интеллектуальность» постановки помех в данных комплексах компенсируется их высокими энергетическими возможностями и универсальностью применения по отношению ко всем типам БПЛА. Недостатком данных комплексов является низкий уровень ЭМС по отношению к другим РЭС связи и навигации в зоне применения, что делает практически невозможным их широкое использование для противодействия БПЛА в условиях мирного времени.

2.2. Коммерческие комплексы РЭП

Необходимость обеспечения защиты критической инфраструктуры и важных объектов в мирное время, при обеспечении требований ЭМС со существующими связными и навигационными РЭС, привело к формированию отдельного направления в области противодействия БПЛА, заключающегося в создании, так называемых, коммерческих комплексов РЭП.

В настоящее время к таким коммерческим комплексам РЭП, предназначенным для противодействия БПЛА можно отнести: «Серп», «Заслон», «Атака-DBS», «Крона-2М», «Солярис-Н» и др. [14, 15, 17, 20].

Отличительными чертами коммерческих комплексов РЭП, по сравнению с боевыми, являются:

- относительно невысокий энергопотенциал, в связи чем – меньшая дальность действия, при одновременном обеспечении требований ЭМС за пределами зоны подавления;
- использование направленных антенных систем, которые позволяют создавать модульные комплексы РЭП, со сложной конфигурацией подавляемых секторов и контролируемого периметра;
- использование для вскрытия факта полета БПЛА и контроля их траектории неизлучающих средств – как средств РРТР, так и пассивных РЛС, основанных на приеме отраженных сигналов от внешних источников радиоизлучения, например, от ретрансляционных телевизионных вышек;
- использование режимов подавления каналов управления БПЛА, основанных не на заградительных помехах, перекрывающих отдельный диапазон частот, а на помехах прицельных по частоте и структуре широко распространенных средств связи с малыми БПЛА-квадрокоптерами;
- использование режимов «вскрытия» каналов управления, основанных на автоматическом определении типа протокола, из числа наиболее широко используемых, с последующем использовании известных уязвимостей в них;
- использование режимов подавления и навязывания ложных режимов работы каналов навигации БПЛА, основанных на формировании шумовых помех, прицельных по частоте, для закрытых каналов СРНС, при одновременном формировании ложных сигналов – имитирующих помех, прицельных по частоте и структуре сигнала, для открытых каналов СРНС (преимущественно по каналу L1 GPS), так называемый, «спуфинг» (от англ. spoofing – подмена) сигналов СРНС.

Анализ этих отличительных черт коммерческих комплексов РЭП относительно боевых позволяет сделать вывод о том, что, с одной стороны, данные комплексы реализуют более «интеллектуальные» режимы противодействия БПЛА, основанные на имитирующих помехах, прицельных по частоте и структуре широко распространённых полезных сигналов управления и навигации БПЛА-квадрокоптеров. С другой стороны, данные комплексы утратили существенную часть универсальности применения и ориентированы, прежде всего,

на широко распространенные коммерчески доступные малые БПЛА, оборудованные исключительно стандартными средствами связи и навигации по СРНС.

Обобщая данные об отечественных комплексах «Серп», «Заслон», «Атака-DBS», «Крона-2М», «Тревога-Шит», «Blighter AUDS», «Drone Dome», «Falcon Shield» и др. [17, 20, 21, 25-31], можно сформировать обобщенные ТТХ коммерческого комплекса РЭП, ориентированного на противодействие БПЛА.

ТТХ подсистемы разведки:

- ведение разведки БПЛА:
  а) РРТР каналов связи и управления БПЛА;
  б) использование РЛС с пассивным или активным принципом подсветки целей;
  в) использование оптико-электронного средства (ОЭС) в видимом и ИК-диапазоне;
- дальность обнаружения БПЛА:
  а) средствами РРТР: до 5-10 км;
  б) путем использования РЛС: до 8-30 км;
  в) путем использования ОЭС (в видимом диапазоне с оптическим увеличением): до 3-5 км;
- литерные частоты широко распространениях средств связи, на которых ведется РРТР каналов управления БПЛА:
  а) RC433: 433 МГц;
  б) сети 4G: 725-770, 790-830, 850-894 МГц;
  в) сети CDMA: 850- 894 МГц:
  г) RC868: 868-916 МГц;
  д) GSM900: 890-915, 935-960 МГц;
  е) GSM1800: 1710-1880 МГц;
  ж) сети 3G: 2110-2170 МГц;
  з) сети Wi-Fi на базовой частоте 2,4 ГГц: 2,4-2,5 ГГц;
  и) сети 4G: 2,5-2,7 ГГц;
  к) сети Wi-Fi на базовой частоте 5,2 ГГц: 4,9-5,5 ГГц;
  л) сети Wi-Fi на базовой частоте 5,8 ГГц: 5,5-6,1 ГГц.

ТТХ подсистемы РЭП:

- литерные частоты широко распространениях средств связи, на которых ведется подавление:
  а) частоты типовых каналов коммерческих систем связи:
    - RC433: 433 МГц;
    - сети 4G: 725-770, 790-830, 850-894 МГц;
    - сети CDMA: 850- 894 МГц:
    - RC868: 868-916 МГц;
    - GSM900: 890-915, 935-960 МГц;
    - GSM1800: 1710-1880 МГц;
    - сети 3G: 2110-2170 МГц;
    - сети Wi-Fi на базовой частоте 2,4 ГГц: 2,4-2,5 ГГц;
    - сети 4G: 2,5-2,7 ГГц;
    - сети Wi-Fi на базовой частоте 5,2 ГГц: 4,9-5,5 ГГц;

- сети Wi-Fi на базовой частоте 5,8 ГГц: 5,5-6,1 ГГц;

б) частоты каналов навигации по СРНС:
- GPS (L1 – 1575,42 МГц / L2 – 1227,6 МГц);
- ГЛОНАСС (L1 – 1602 МГц / L2 – 1246 МГц);
- BeiDou (B1 – 1561,098 МГц / B2 – 1207,14 МГц);
- Galileo (E1 – 1575,42 МГц / E5 – 1191,79 МГц);

- дальность подавления приемных трактов средств связи и средств навигации по СРСН на БПЛА: до 6 км;
- энергопотенциал воздействия: 5-10 Вт;
- направленность антенн: направленные антенны с шириной главного лепестка диаграммы направленности 45-90º;
- типы формируемых помех:

а) для «закрытых» каналов связи и управления, имеющих криптографическую защиту: шумовая помеха, прицельная по частоте;

б) для «открытых» каналов связи и управления или каналов, имеющих типовые уязвимости в протоколах шифрования: имитирующая помеха, прицельная по частоте и структуре полезного сигнала, с целью навязывания ложных режимов работы;

в) для «открытых» каналов навигации по СРНС: шумовая помеха, прицельная по частоте; имитирующая помеха, прицельная по частоте и структуре полезного сигнала, с целью навязывания ложных траекторий полета.

В целом коммерческие комплексы РЭП для противодействия БПЛА являются эффективным средством решения задач подавления каналов управления и навигации исключительно широко распространённых малых коммерческих БПЛА-квадрокоптеров. Наличие априорных данных о стандартах связи, используемых для управления БПЛА (в основном это каналы Wi-Fi на опорных частотах 2,4, 5,2 и 5,8 ГГц), а также об уязвимостях криптографических протоколов защиты, встроенные в эти стандарты (WEP, WPA и др.), позволяет производителям комплексов РЭБ реализовывать в них режимы автоматического «взлома» каналов управления, с последующем формированием для них помех, прицельных по частоте и структуре полезного сигнала, имитирующих команды управления «посадка» или «снижение». То же самое относится и к возможностям коммерческих комплексов РЭП в отношении подавления каналов навигации по СРНС. Однако такая строгая ориентированность комплексов на малые коммерческие БПЛА, существенно снижает возможности данных комплексов по противодействию БПЛА, имеющих другие, отличные от широко используемых, частоты и стандарты каналов управления.

2.3. Малогабаритные носимые средства РЭП

Малогабаритные носимые средства РЭП, в формате различного рода «электронных автоматов» или «электронных винтовок» с регулярным постоянством стали презентоваться начиная с 2015 г., когда проблеме противодействия БПЛА стали уделять повышенное внимание.

В настоящее время к таким малогабаритным носимым средствам РЭП, предназначенным для противодействия БПЛА, можно отнести: «REX 1», «REX 2», «Пищаль-ПРО», «Таран-ПРО», «Stupor» и др. [15, 17, 20, 21].

Отличительными чертами этих носимых средств РЭП, по сравнению с боевыми и коммерческими комплексами, являются:

- отсутствие какой-либо разведывательной подсистемы, вскрывающей параметры каналов управления БПЛА;
- использование для подавления шумовых помех, прицельных по частоте широко распространенных каналов навигации СРНС и каналов связи с малыми БПЛА-квадрокоптерами;
- малый энергопотенциал, в связи чем – малая дальность действия;
- использование направленных антенных систем, совпадающих по ориентации с направлением самого устройства;
- использование в составе средств РЭП аккумуляторных батарей с ограниченным «боезапасом» – на несколько часов эпизодического применения;
- для некоторых мобильных средств РЭП указываются медицинские ограничения на длительность применения данных устройств человеком-оператором, ввиду негативного влияния электромагнитного излучения (ЭМИ).

Обобщая данные о малогабаритных носимых средствах РЭП «REX 1», «Пищаль-ПРО», «Таран-ПРО», «Stupor», «DroneDefender», «UAV-D04JA», «DroneGun» и др. [15, 17, 20, 21, 28, 32], можно сформировать обобщенные ТТХ таких средств, ориентированных на противодействие БПЛА:

- литерные частоты широко распространениях средств связи, на которых ведется подавление:
  а) частоты типовых каналов коммерческих систем связи:
    - RC433: 433 МГц;
    - сети 4G: 725-770, 790-830, 850-894 МГц;
    - сети CDMA: 850- 894 МГц:
    - RC868: 868-916 МГц;
    - GSM900: 890-915, 935-960 МГц;
    - GSM1800: 1710-1880 МГц;
    - сети 3G: 2110-2170 МГц;
    - сети Wi-Fi на базовой частоте 2,4 ГГц: 2,4-2,5 ГГц;
    - сети 4G: 2,5-2,7 ГГц;
    - сети Wi-Fi на базовой частоте 5,2 ГГц: 4,9-5,5 ГГц;
    - сети Wi-Fi на базовой частоте 5,8 ГГц: 5,5-6,1 ГГц;

  б) частоты каналов навигации по СРНС:
    - GPS (L1 – 1575,42 МГц, L2 – 1227,6 МГц);
    - ГЛОНАСС (L1 – 1602 МГц / L2 – 1246 МГц);
    - BeiDou (B1 – 1561,098 МГц / B2 – 1207,14 МГц);
    - Galileo (E1 – 1575,42 МГц / E5 – 1191,79 МГц);
- дальность подавления приемных трактов средств связи и средств навигации по СРСН на БПЛА: до 0,4-2 км;

- энергопотенциал воздействия: 5-10 Вт;
- тип формируемых помех: шумовая или скользящая помеха, прицельная по частотам каналов средств связи и каналов СРСН;
- масса: 2,5-6,5 кг;
- время непрерывной работы: 0,5-4,5 ч.

Анализ отличительных черт малогабаритных средств РЭП и их ТТХ, позволяет сделать вывод, что эти средства являются наименее «интеллектуальными» и наименее эффективными при решении задачи противодействия малым БПЛА. С одной стороны, простота и мобильность этих средств позволяет их применять отдельным людям-операторам без специализированного обучения, с другой стороны, данные средства могут применяться только эпизодически и ориентированы на самые простые малые БПЛА-квадрокоптеры. При этом отсутствие в функционале данных устройств режимов формирования имитирующих помех по каналу навигации СРНС, приводит к тому, что поведение БПЛА, в условиях «грубого» шумового подавления каналов управления и навигации, становится фактически непредсказуемым. Несмотря на декларирование производителями подобных устройств таких эффектов как «падение БПЛА», «приземление БПЛА» или «возврат БПЛА к ПУ», фактическое поведение БПЛА определяется исключительно программой их действий в случае отсутствия связи и может существенно отличаться от вышеуказанных, вплоть до продолжения полета в соответствии с заблаговременно заданной программой.

3. Радиоэлектронное подавление навигационной системы БПЛА

3.1. Проблемные вопросы радиоэлектронного подавления навигационной системы БПЛА

При рассмотрении вопросов подавления канала навигации БПЛА необходимо учитывать, что навигационная система БПЛА может иметь различный уровень сложности и учитывать для определения местоположения БПЛА несколько сигналов, поступающих от датчиков различной физической природы:

1) навигационная система, основанная только на аппаратуре потребителей (АП) наиболее распространенных СРНС – такая система характерна для самых простых малых БПЛА-квадрокоптеров;
2) простая интегрированная навигационная система, на основе комплексирования данных микромеханических инерциальных навигационных систем (ИНС) и АП СРНС – такая навигационная система характерна для широкого класса малых БПЛА-квадрокоптеров для профессионального использования в различных целях;
3) интегрированная навигационная система, на основе комплексирования данных нескольких навигационных устройств: микромеханических ИНС, АП СРНС, барометрического высотомера, радио или лазерного высотомера – такая навигационная система характерна для профессиональных малых БПЛА, а также для БПЛА среднего класса;

4) интегрированная навигационная система, на основе комплексирования данных нескольких навигационных устройств: авиационных ИНС, АП СРНС, высотомеров (барометрического и радио), радиотехнической системы ближней навигации (РСБН) VOR/DME (Very high frequency Omni directional radio Range / Distance Measuring Equipment), системы АЗН-В (автоматического зависимого наблюдения-вещания) – такая навигационная система фактически полностью повторяет навигационную систему пилотируемого летательного аппарата (ЛА) и характерна для БПЛА тяжелого класса.

Говоря о подавлении канала навигации БПЛА, необходимо четко понимать, что сам факт радиоэлектронного воздействия (подавления или навязывания ложных режимов работы) относится только к сигналам, принимаемым АП от одного или нескольких СРНС, что соответствуют только одному каналу из всего множества каналов поступления данных в навигационную систему БПЛА. Таким образом с использованием РЭП возможно обеспечить значимое нарушение работы только наиболее простых навигационных систем БПЛА (типы 1-3 из списка). Для БПЛА с полноценной интегрированной навигационной системой (тип 4 из списка), основанной на использовании нескольких каналов получения навигационных данных, нарушение спутникового канала (в том числе и поступление по нему ложных навигационных данных, вступающих в противоречие в данными других каналов), в большинстве случаев будет обнаружено, после чего навигационная система перестанет использовать спутниковый канал для определения местоположения БПЛА. Отметим, что в средних и тяжелых БПЛА, в подавляющем числе случаев, в качестве основного канала формирования навигационных данных используется информация именно от авиационных ИНС на основе лазерных или волоконно-оптических гироскопов. Подробно ТТХ таких ИНС рассмотрены в работе [33]. Данные ИНС в среднем обеспечивают ошибку счисления пути порядка 1,85 км за 1 ч полета. При этом информация по другим каналам (данные от АП СРНС, данные высотомеров, сигналы РСБН и АЗН-В) является вторичной и после верификации и комплексирования она используются только для коррекции показаний ИНС [34, 35]. Дополнительно отметим, что средние и большие БПЛА используемые для решения специальных и военных задач, при этом в них АП СРСН использует не «открытые», а «закрытый» сигналы СРНС, имеющие более высокую помехозащищенность и криптозащиту [36, 37]. При этом оборудование навигационных спутников может формировать отдельные помехозащищенные зоны. Например, функционал спутников GPS-III предусматривает возможность формирования отдельных зон с повышенной на 20 дБ энергетикой сигналов «закрытых каналов». Вследствие этого задача нарушения корректного функционирования навигационных систем таких БПЛА становится еще более затруднительной, фактически невозможной.

Быстрое развитие БПЛА приводит к усовершенствованию их навигационного обеспечения, в том числе, для применения в условиях плохого приема сигналов СРНС.

К таким направлениям усовершенствования относятся следующие:

1) использование для повышения точности навигации многостанционных локальных РСБН или систем – имитаторов сигналов СРНС [35, 38], при этом станции этих систем могут быть мобильными, находясь на автомобилях, и заблаговременно развертываться в зоне планируемого применения БПЛА. В частности, использование подобных систем позволяет повысить отношение сигнал/шум (ОСШ) на 35-50 дБ в зоне подавления (или плохого приема) сигналов СРНС и обеспечить прием навигационных сигналов при мощностях активных шумовых и доплеровских (уводящих по скорости) помех в зоне действия РСБН до 100 Вт [38];
2) использование для навигации электронных карт местности, полет по которым осуществляется в соответствии с данными радио- или лазерного высотомера, РЛС или ОЭС видимого диапазона [39, 40];
3) использование для навигации различных автономных систем технического зрения [39], а также технологии SLAM (Simultaneous Localization and Mapping) – технологии автоматического одновременного построения карты местности в неизвестном пространстве, контроля текущего местоположения БПЛА и пройденного пути [41, 42];
4) автономный прямолинейный полет БПЛА в направлении цели, подсвечиваемой внешним источником излучения.

Таким образом, обобщая вышесказанное, можно сделать вывод, что применение средств РЭП, в том числе и путем формирования «интеллектуальных» помех, прицельных по частоте и структуре сигналов СРНС, с целью навязывания ложного местоопределения и траектории полета, ориентировано на малые БПЛА с самыми простыми навигационными системами. При этом высокий темп развития БПЛА, а также возможность разработки в самом ближайшем будущем навигационных систем на основе электронных карт местности или систем технического зрения, сделает подавление каналов СРСН бесполезным даже против малых БПЛА.

Далее рассмотрим особенности подавления каналов навигации в БПЛА с навигационными системами на основе только АП СРСН, а также с простыми инерциальными системами на основе комплексирования данных микромеханических ИНС и сигналов СРНС, так как именно для таких БПЛА подавление канала спутниковой навигации может дать какой-либо значимый эффект.

3.2. Особенности радиоэлектронного подавления навигационной системы БПЛА, основанной на приеме сигналов СРНС

Систему навигации на подавляющем числе малых БПЛА составляет АП, принимающая сигналы одной или нескольких СРНС. К наиболее распространенным СРНС относятся системы: ГЛОНАСС (Россия), GPS/NAVSTAR (США), Beidou (Китай), Galileo (ЕС). Сигналы СРНС формируются на литерных частотах в диапазоне 1,1-1,6 ГГц. Как правило, простые навигационные системы, устанавливаемые на малые БПЛА, используют интегрированный режим

обработки сигналов от нескольких СРНС, что обеспечивает точность навигации 1-2,5 м как в горизонтальной плоскости, так и по высоте.

Теоретические оценки помехоустойчивости сигналов СРНС и режимов их интегрированной обработки в АП рассмотрены в работах [36, 43-48]. Экспериментальные оценки помехоустойчивости сигналов СРНС и уровня помех, при котором навигационные устройства сохраняют приемлемую эффективность функционирования, рассмотрены в работах [49, 50]. Обобщая материал вышеуказанных работ можно сделать следующие выводы.

1) Среди помех, используемых для подавления каналов СРНС в наиболее широкой степени применяются [45, 46]:

- шумовая помеха (белый шум высокой мощности на частотах каналов СРНС);
- гармоническая (полигармоническая) помеха (одночастотное или модулированное гармоническое колебание на частоте (на частотах) полезного сигнала);
- прицельная имитирующая помеха (помеха имитирует структуру сигналов СРНС с частотным и временным рассогласованием, а также с фиксированным значением фазы огибающей манипулирующей функции);
- следящая имитирующая помеха (помеха имитирует структуру сигналов СРНС, но с переменной начальной фазой манипулирующей функции, закон изменения которой соответствует изменению расстояния от приемника до станции РЭП);
- заградительная имитирующая помеха (имитирует набор сигналов спутников СРНС с одинаковым частотным рассогласованием для всех компонентов и разным временным рассогласованием для каждого компонента).

Для организации имитирующих помех требуется разведка не только несущей частоты и фазы, но и амплитуды сигналов СРНС, а также манипулирующих функций, представляющих собой кодовую последовательность для разделения сигналов и навигационных данных. При этом для формирования следящей и прицельной имитирующих помех необходима разведка частотных, фазовых и временных параметров полезных сигналов СРНС. Более простой в реализации является заградительная имитирующая помеха, поскольку она не требует для формирования точных временных параметров сигнала [45].

2) Наиболее эффективными помехами для нарушения нормального функционирования АП СРНС являются имитирующие помехи, воспроизводящие структуру реального сигнала СРНС с частотными, фазовыми и временными параметрами, позволяющими навязать АП СРНС ложный режим работы и как следствие – ложное местоопределение БПЛА. Модификация значащих параметров имитирующей помехи позволяет управлять траекторией полета БПЛА. При этом значащие параметры помехи должны быть как можно более близкими к соответствующим параметрам реальных сигналов СРНС.

Постановка имитационных помех производится в два этапа:

1) постановка шумовой помехи, заградительной по каналам СРНС – вызывает «отвязку» АП от текущих сигналов СРНС, прерывание режима слежения и переход в режим обнаружения и поиска сигналов;
2) формирование имитирующей помехи с высоким энергетическим потенциалом – вызывает «привязку» АП СРНС к ложным сигналам, с последующим переходом в ложный режим работы.

Результаты теоретических исследований помехоустойчивости АП СРНС GPS, представленные в работе [43], обобщены в таблице 1.

Таблица 1 – Результаты исследований подавления каналов АП СРНС при использовании различных типов помех для ситуаций, когда АП функционирует автономно в штатном режиме [43]

Канал АП СРНС	Тип помехи	Вероятность успешного подавления канала АП	Требуемый энергопотенциал станции РЭП, $P_{ПП}G_{ПП}$, дБВт
Канал обнаружения	Шумовая	0,5	8,5
	Гармоническая	0,5	8,5
	Заградительная имитирующая	0,67	–3,6…–9,5
Канал слежения за частотой	Шумовая	0,32	19,5
	Гармоническая	0,32	24,4
Канал слежения за задержкой сигнала	Шумовая	0,5	10,4
	Гармоническая	0,5	54
	Заградительная имитирующая	0,67	–3,6…–9,5
Квадратичный детектор	Шумовая	0,1	18,7
	Гармоническая	0,1	18,7

Примечание: дальность между АП СРНС и станцией РЭП – 10 км.

Из приведённых в таблице 1 результатов следует, что из всех рассматриваемых помех наименьший энергетический потенциал станции РЭП требуется при постановке заградительной имитирующей помехи. При воздействии заградительной имитирующей помехи на канал обнаружения и канал слежения за задержкой вероятность подавления АП СРСН составит порядка 0,9. При постановке шумовой или гармонической помех с энергетическим потенциалом станции РЭП, равным 8,5 дБВт вероятность подавления АП СРНС составит порядка 0,5. С целью увеличения вероятности подавления АП РЭП необходимо при постановке шумовых помех иметь энергетический потенциал станции РЭП порядка 20 дБВт, а при постановке гармонических помех – порядка 25 дБВт [43].

В работах [50, 51] показано, что помехоустойчивость стандартных АП СРНС составляет 34-36 дБ для динамично движущихся АП и 38-40 дБ для слабо динамичных АП.

В работе [52] приведены оценки уровня мощности преднамеренных помех, которые могут быть созданы типовыми средствами РЭП на входе приемника АП СРНС авиационного базирования:

- при высоте полета летно-подъемного средства с АП СРНС 100 м:

- от наземных средств РЭП: –78...–166 дБВт;
- от авиационных средств РЭП: –82...–103 дБВт;
- от тактического БПЛА со средствами РЭП: –94...–96 дБВт;
- от малогабаритного забрасываемого передатчика помех (ЗПП): –81...–83 дБВт;

- при высоте полета летно-подъемного средства с АП СРНС 5 км:
  - от наземных средств РЭП: –81...–102 дБВт;
  - от авиационных средств РЭП: –82...–103 дБВт;
  - от тактического БПЛА со средствами РЭП: –97...–99 дБВт;
  - от малогабаритного ЗПП: –101...–103 дБВт;

Проведенные испытания АП СРНС отечественного производства «Грот-Н», «Бриз-КМИ», «МРК-32Р», «МРК-33» показали, что при реальной чувствительности приемного устройства –165 дБВт срыв сопровождения наступает при уровне помех на входе –120 дБВт, т.е. превышение помехи над сигналом составляет примерно 40-45 дБ. Это объясняется применением ШПС и их накоплением на интервале времени 1 мс. Результаты этих экспериментальных исследований, в части способности выполнения АП СРСН навигационных задач в режимах обнаружения и слежения за сигналами СРСН в условиях шумовых и гармонических помех, по данным работ [49, 50, 51], представлены в таблице 2.

Таблица 2 – Значение ОСШ на входе АП СРНС, при котором отсутствует решение навигационной задачи [49, 50, 51]

Виды помехи	Режим работы АП СРСН	Значение ОСШ, дБ
Гармоническая	обнаружение	–36…–46
	слежение	–57…–60
Шумовая широкополосная	обнаружение	–41…–48
	слежение	–44…–49

Более полная информация о РЭП СРНС, а также о помехоустойчивости АП, представлена в работах [36, 43, 52].

Для повышения помехозащищенности АП СРНС в БПЛА могут быть использованы следующие способы и средства [46, 52, 53]:

- использование дальномерных кодов повышенной точности, поступающих по «закрытым» каналам СРНС;
- одновременный прием и обработка в АП сигналов от различных СРНС (ГЛОНАСС, GPS, Galileo и т.д.);
- пространственная селекция сигналов СРНС;
- комплексирование АП с ИНС;
- предкорреляционная обработка смеси сигналов и помех;
- алгоритмическая посткорреляционная обработка сигналов;
- поляризационная селекция сигналов.

Из указанных способов, помимо комплексирования АП с ИНС (данный способ будет рассмотрен далее), наибольшее распространение получил способ пространственной селекции сигналов СРНС за счет установки на БПЛА фази-

рованной антенной решетки (ФАР). Как показано в работе [54], наличие на БПЛА всего лишь 6 элементов в ФАР позволяет достаточно эффективно формировать «нули» диаграммы направленности антенны (ДНА) в направлении на наземные источники помех и «максимумы» ДНА ФАР – в направлении на космические аппараты СРНС, тем самым обеспечивая пространственную режекцию помех.

3.3. Особенности радиоэлектронного подавления интегрированной навигационной системы БПЛА, основанной на комплексировании данных микромеханических инерциальных систем и сигналов СРНС

Выше были рассмотрены навигационные системы самых простых малых БПЛА, основанные на приеме и обработке сигналов СРНС. На более сложных БПЛА устанавливаются элементы автономной навигационной системы – акселерометры, гироскопы, барометры, лазерные высотомеры и т.д. Общепринятой нормой точности авиационных инерциальных ИНС «средней точности» является ошибка счисления пути в 1,85 км за 1 ч полета. Такая точность достигается авиационными ИНС на основе лазерных или волоконно-оптических гироскопов. Однако масса таких ИНС составляет от 8 кг, что делает проблематичным их использование на малых и даже на средних БПЛА.

В результате на малых БПЛА устанавливается более простая ИНС, оснащённая микромеханическими датчиками движения – акселерометрами и гироскопами. Такая ИНС, без ее коррекции по сигналам СРНС, не в состоянии осуществлять автономное счисление пройденного пути ввиду высоких скоростей дрейфа гироскопических датчиков. Накапливаемая ошибка микромеханических ИНС, в условиях отсутствия корректирующих сигналов СРНС, за 1 мин составляет до 3 м по горизонтали и 2 м по вертикали. Таким образом, эти ИНС способны без сигналов СРНС поддерживать приемлемую точность полета на уровне 100-150 м в течении не более 10 мин. При этом, как правило, имеется ввиду поддержание режима прямолинейного полета без ускорений и маневров. Примерами таких образцов микромеханических ИНС могут являться устройства Geo-iNAV (масса порядка 3 кг). Таким образом на современном этапе развития навигационных систем малых БПЛА для счисления пути с приемлемой точностью требуется использование сигналов СРНС [34]. Дополнительными способами повышения автономности и точности навигационных систем БПЛА является установка барометра, радио- или лазерного высотомера. Приблизительный диапазон измерений простого барометрического высотомера для малых БПЛА до 9 км, точность 0,1 м. Диапазон измерений радиовысотомера до 700 м, точность по высоте 2-5%, точность по углу 0,25° [55]. Диапазон измерений лазерного высотомера 0,1-120 м (статические поверхности) и 2-40 м (движущиеся поверхности), разрешение 1 см, точность 0,1 м (объект с 70% светоотражением при 20° С) [60]. Это оборудование позволяет повысить точность определения координат за счет использования дополнительных каналов поступления навигационных данных, а также формировать профили автономного

полета БПЛА по электронным картам местности содержащим барометрические данные или высотные профили подстилающей поверхности [35].

Особенности функционирования интегрированных навигационных систем БПЛА рассмотрены в работах [55-59].

В работе [55] показано, что стандартным режимом интегрированной навигационной системы БПЛА, является следующая иерархия обработки навигационных данных (по мере снижения значимости и приоритета источника навигационных данных): «ИНС – СРНС – ОЭС – барометр – радиовысотомер». В случае затрудненного приема сигналов СРНС навигационная система БПЛА переходит в режим «ИНС – ОЭС – барометр – радиовысотомер», причем в этом случае ОЭС может быть использовано как для автономного контроля полета по визуальным ориентирам, так и для организации прямого дистанционного управления оператором по визуальным данным от ОЭС. При отсутствии ОЭС на БПЛА навигационная система переходит в режим «ИНС – барометр – радиовысотомер», для полета по барометрической и электронной карте местности. При этом, как отмечается в работах [57, 61] в настоящее время наблюдается уход от использования ОЭС для прямого управления БПЛА оператором, в направлении автономного использования ОЭС, а также других радиотехнических средств БПЛА, в режиме SLAM – режим автоматического одновременного построения карты местности в неизвестном пространстве и одновременного контроля текущего местоположения БПЛА, а также счисления пройденного пути.

В работе [58] исследуется функционирование интегрированных навигационных систем в режимах «ИНС – СРНС» и «ИНС – СРНС – АЗН-В», где наземные опорные станции (НОС) АЗН-В формируют своеобразную локальную РСБН. Показано, что в режиме «ИНС – СРНС» при полном созвездии навигационных спутников (4-е и более) обеспечивается погрешность местоопределения БПЛА на уровне 6-8 м. В случае, когда количество видимых навигационных спутников снижается до 2-3, погрешность квазилинейно растет (рис. 1) при этом ИНС способна без сигналов СРНС поддерживать приемлемую точность полета на уровне 30 м в течении не более 2-4 мин, на уровне 60 м – в течении 4-6 мин [58].

В режиме «ИНС – СРНС – АЗН-В» интегрированная инерциальная система корректирует показания ИНС как по сигналам СРНС, так и по сигналам наземных опорных станций системы АЗН-В с точно известными координатами. Использование подобного режима позволяет значительно снизить погрешность местоопределения БПЛА. Так, при видимости 2 навигационных спутников и 2 станций АЗН-В погрешность местоопределения снижается до 18-20 м (рис. 2). Фактически станции АЗН-В создают избыточность псевдодальномерных наблюдений и компенсируют отсутствие видимости полного созвездия спутников СРНС. В целом интегральные навигационные системы БПЛА в режиме «ИНС – СРНС – АЗН-В» обеспечивают точность навигации 16-18 м [58]. Такой подход к повышению точности интегрированных навигационных систем БПЛА за счет внешних источников псевдодальномерных сигналов схож с предложениями по созданию локальных РСБН, представленных в работах [35, 38].

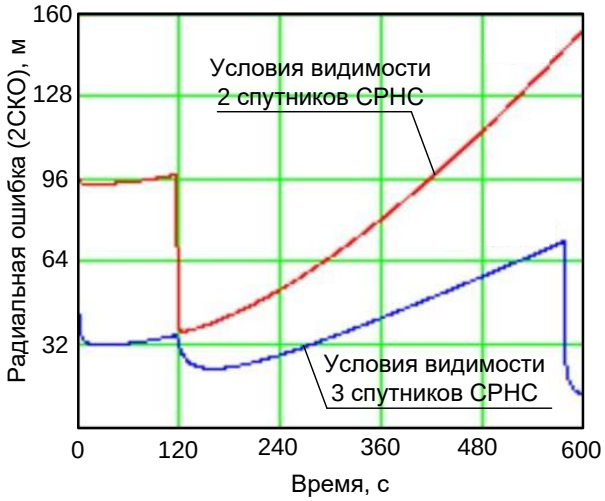


Рис. 1. Ошибка оценки координат в режиме «ИНС – СРНС» при видимости 2, 3 навигационных спутников СРНС [58]

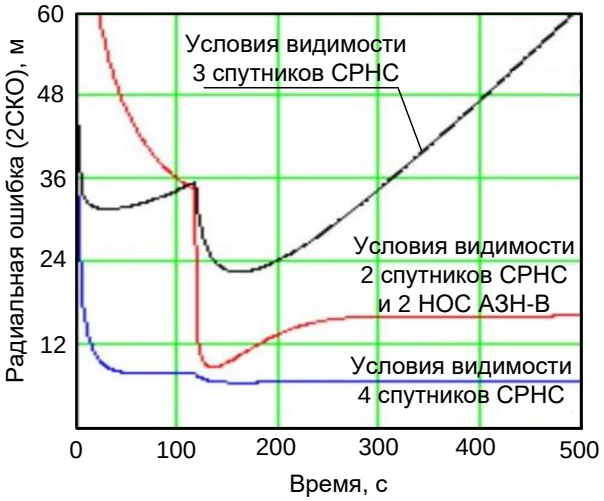
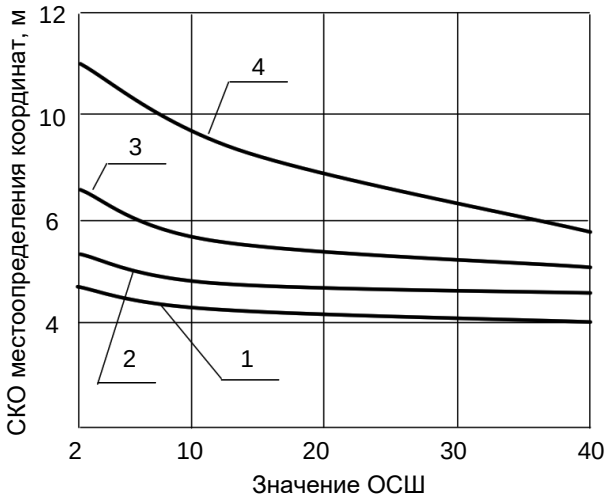
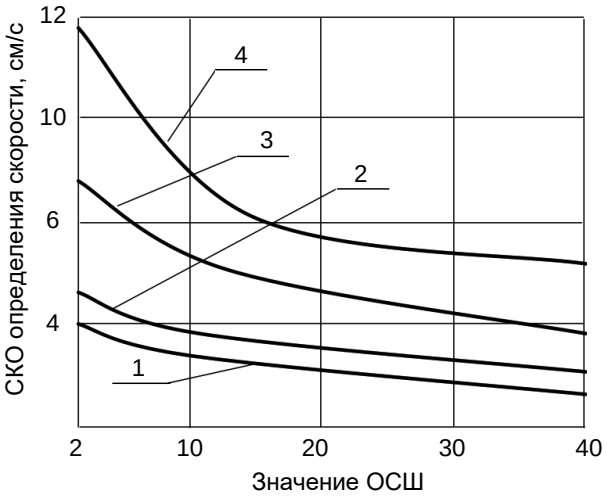


Рис. 2. Ошибка оценки координат в режиме «ИНС – СРНС – АЗН-В» при видимости 2, 3, 4 навигационных спутников СРНС и 2 НОС АЗН-В [58]

В работе [59] исследуется функционирование интегрированной навигационной системы «ИНС – СРНС» в зависимости от ОСШ сигналов СРНС на приемнике АП. Результаты этого исследования приведены на рис. 3.



а.



б.

Рис. 3. Точность интегрированной навигационной системы «ИНС – СРНС» по параметрам СКО местоопределения координат (а) и скорости (б) в зависимости от ОСШ сигналов СРНС на приемнике АП в различных режимах [59]

Обозначения цифрами на рис. 3 соответствуют следующим режимам комплексирования данных в навигационной системе:

1) режим, при котором данные от ИНС комплексируются с сигналами АП СРНС, после чего осуществляется их одноэтапная обработка без разделения на первичную и вторичную;

2) режим, при котором в АП СРНС производится разделение обработки на первичную и вторичную, а комплексирование с данными ИНС осуществляется на уровне вторичной обработки;
3) режим с одноэтапной обработкой сигналов в АП СРНС без комплексирования ее с ИНС;
4) режим с двухэтапной обработкой сигналов в АП СРНС без комплексирования ее с ИНС.

Результаты данных исследований показывают, что снижение ОСШ на входе АП СРНС отражаются на текущей точности интегрированных навигационных систем БПЛА. Причем наибольшую точность и устойчивость к снижению ОСШ на входе АП СРНС демонстрирует режим, при котором данные от ИНС комплексируются с сигналами СРНС, после чего осуществляется их одноэтапная обработка без разделения на первичную и вторичную обработку [59].

Подробные теоритические исследования помехозащищенности навигационной системы в режиме «ИНС – СРНС» представлены в работе [43]. Результаты этих исследований относительно АП СРНС GPS обобщены в таблице 3.

Таблица 3 – Результаты исследований подавления каналов АП СРНС при использовании различных типов помех для ситуаций, когда АП СРНС GPS функционирует интегрировано с ИНС [43]

Канал АП СРНС	Тип помехи	Вероятность успешного подавления канала АП	Требуемый энергопотенциал станции РЭП, $P_{ПП}G_{ПП}$, дБВт
Канал обнаружения	Шумовая	0,745	16,5
	Гармоническая	0,745	16,5
	Заградительная имитирующая	0,67	–3,6…–9,5
Канал слежения за частотой	Шумовая	0,32	36,5
	Гармоническая	0,32	41,4
Канал слежения за задержкой сигнала	Шумовая	0,5	50,4
	Гармоническая	0,5	94
	Заградительная имитирующая	0,67	–3,6…–9,5
Квадратичный детектор	Шумовая	0,1	28,7
	Гармоническая	0,1	28,7

Примечание: дальность между АП СРНС и станцией РЭП – 10 км.

Из приведённых в таблице 3 результатов следует, что из всех рассматриваемых помех наименьший энергетический потенциал требуется при постановке заградительной имитирующей помехи. При постановке шумовой и гармонической помех в случае использования комплексирования АП СРНС с ИНС требуется дополнительное увеличение энергетического потенциала станции РЭП для обеспечения вероятности подавления до $P_п$=0,5 на 8 дБВт, а для $P_п \rightarrow 1$ на 15-20 дБВт [43].

Сравнительный анализ вероятности подавления АП СРНС интегрированного с ИНС с использованием шумовых, гармонических и заградительной имитационной помех позволяет однозначный вывод о целесообразности перехода

от «силовых» помех (шумовых и гармонических) к имитационным помехам, навязывающим навигационной системе ложный режим работы по определению местоположения БПЛА и траектории его полета.

В работе [56] исследовались различные варианты реакции интегрированных навигационных систем «ИНС – СРНС» на постановку имитационных помех. Показано, что для обеспечения наилучшего навязывания БПЛА ложной траектории параметры имитационных помех, навязываемое ложное местоположение, а также ложная траектория должны быть согласованны с такими параметрами как: текущее местоположение БПЛА, скорость его полета, дальность до цели, величина требуемого отклонения от цели, и самое главное – функция дрейфа датчиков микромеханических ИНС, при отсутствии сигналов СРНС. Формирование такого индивидуального режима подавления для каждого БПЛА требует, чтобы в формируемых имитационных помехах для АП СРНС учитывалась нарастающая ошибка ИНС. Это позволяет «мягко» перевести БПЛА на нужную траекторию, при этом на начальном этапе постановки таких интеллектуальных имитационных помех, между данными ложных сигналов СРНС и ИНС не будет наблюдаться критического рассогласования, что исключит переход навигационной системы в режимы навигации без использования СРНС (например, в режим «ИНС – ОЭС – барометр – радиовысотомер»). Это позволит «привязать» БПЛА к ложным сигналам СРНС, а затем сформировать ложную траекторию с учетом дрейфа показаний ИНС во времени. Вместе с тем, практическая реализация такого многопараметрического индивидуального режима помех для каждого БПЛА, представляет собой сложнейшую научно-техническую задачу, которая до сих пор не решена.

Обобщая вышеизложенное, можно сделать вывод, что подавление интегрированных навигационных систем БПЛА в режиме «ИНС – СРНС» является принципиально возможным. Однако такое подавление требует создания территориально-распределенной группировки станций РЭП работающих в режиме псевдо-спутников, при этом формируемые имитационные помехи, навязывающие ложную траекторию полета, должны учитывать диапазоны дрейфа гироскопических датчиков ИНС, а также индивидуальный режим полета каждого подавляемого БПЛА. Использование же энергетических помех (шумовых и заградительных) для нарушения функционирования интегрированной навигационной системы БПЛА сопряженно с необходимостью формирования высокоэргических помех, при этом применение таких помех обладает потенциально низкой результативностью.

3.4. Возможности акустического подавления автономной навигационной системы БПЛА, основанной на микромеханических инерциальных системах

Одним из относительно новых способов нарушения нормального функционирования навигационной системы БПЛА является воздействие на его автономную ИНС акустическими колебаниями. В работе [62] показано, что для противодействия БПЛА, оснащенных автономными ИНС с микромеханически-

ми датчиками, можно использовать мощные акустические колебания, негативно влияющие на дрейф гироскопических датчиков из-за эффекта резонанса.

Исследования, проведенные учеными из южнокорейского института Korea Advanced Institute of Science and Technology (KAIST) [63], показали, что будучи механической системой, гироскоп имеет свою резонансную частоту. Следовательно, подобранное по частоте акустическое воздействие может вызвать резонанс в гироскопе, что приведет к его неправильной работе и, как следствие, к выдаче ошибочных показаний о местоположении БПЛА. Эксперименты, проведенные исследователями из KAIST, показали, что 7 моделей гироскопов из 15 наиболее часто используемых в коммерческих малых БПЛА подвержены резонансу. По результатам дальнейших расчетов учеными были сделаны следующие выводы – звукового воздействия мощностью порядка 140 дБ на резонансной частоте гироскопа достаточно, чтобы нарушить работу этого прибора на расстоянии до 40 м от источника звукового сигнала.

Важно отметить, что акустическое воздействие на гироскопы, во-первых, будет эффективно только против малых БПЛА, во-вторых, такое воздействие не всегда приводит к значительной дестабилизации БПЛА. Это связано с тем, что в некоторых гироскопах звуковое колебание влияет только на канал ориентации в горизонтальной плоскости, который в ряде моделей БПЛА продублирован магнитометром для лучшей стабилизации полета. В этом случае эффективность технических средств противодействия БПЛА, основанных на способе акустического воздействия, существенно снижаются [62]. Кроме того, само формирование акустических помех на уровне 120-140 дБ, что соответствует болевому порогу или контузии человека, фактически невозможно в населенной местности, а также в составе комплексов, в которые входят люди-операторы. В связи с этим применение данного способа подавления на практике весьма затруднено.

4. Радиоэлектронное подавление радиолиний управления и передачи данных БПЛА

4.1. Проблемные вопросы радиоэлектронного подавления радиолиний управления и передачи данных БПЛА

Вопросы организации управления и связи БПЛА, а также помехозащищенности радиоканалов передачи данных достаточно глубоко рассмотрены в известных работах: В.С. Вербы [64-67], В.И. Меркулова [65-69], Н.М. Боева [70-76], В.И. Слюсаря [77-78], А.В. Ананьева [79-84], Д.Г. Пантенкова [85-88], Р.В. Киричека [89], Д.В. Самойленко, О.А. Финько [90-92, 148], С.В. Дворникова [93-95], А.А. Донченко [96, 97], Д.С. Чирова [97-99], В.В. Бородина, А.М. Петракова, В.А. Шевцова [100, 101], Л.Н. Казакова [145-147], а также в отдельных работах [102-107] других ученых. Нужно отметить, что в сравнении с задачей радиоэлектронного подавления навигационной системы БПЛА, задача подавления радиолиний «ПУ – БПЛА» не является принципиально новой и фактически сводится к известной задаче формирования на входе подавляемого приемника такого значения ОСШ, которое не позволяет обеспечить прием дан-

ных с требуемой степенью достоверности. Данная задача является классической в теории РЭП, а особенностью ее решения, применительно к БПЛА, является учет используемых в радиолиниях типов сигнально-кодовых конструкций, типов передаваемых данных (тип передаваемых данных определяет требуемый уровень достоверности приема), а также сигнальных, энергетических, пространственных и прочих параметров радиолиний.

При рассмотрении вопросов подавления КРУ и каналов передачи данных БПЛА необходимо учитывать, что подсистема управления и радиосвязи БПЛА представляет собой совокупность различных линий, в которых предаются данные принципиально различного типа, уровня важности, объема, уровня криптозащиты и т.д.

Для управления и обмена данными с БПЛА организуются следующие направления связи:

- направление «вверх» – организуется от ПУ к БПЛА и включает в себя:
  - направление «вверх» КРУ для передачи команд управления БПЛА, а также команд управления специальной аппаратурой и техническими средствами полезной нагрузки, размещенными на БПЛА;
- направление «вниз» – организуется от БПЛА к ПУ и включает в себя:
  - направление «вниз» КРУ для передачи телеметрической информации (ТМИ) о состоянии подсистем БПЛА, специальной аппаратуры и технических средств полезной нагрузки, а также квитанций о выполнении команд управления;
  - высокоскоростная линия передачи данных от специальной аппаратуры и технических средств полезной нагрузки, размещенных на БПЛА.

Вышеуказанные линии связи могут организовываться в различных частотных диапазонах, использовать различные режимы с ретрансляцией и без неё, использовать различные сигнально-кодовые конструкции, специально адаптированные под тип и важность передаваемых данных.

Наиболее критичным элементом для функционирования БПЛА является КРУ. Именно подавление КРУ по направлению «вверх» способно обеспечить максимальный эффект с точки зрения нарушения нормального функционирования БПЛА. Вместе с тем при решении данной задачи встречается ряд трудностей:

- вскрытие параметров линии КРУ «вверх» требует наблюдения за ПУ, при этом ПУ может находиться в существенном удалении от средств РЭП (до 30-50 км) и использовать для организации связи антенную систему с остронаправленной ДНА (порядка 5-10°) и с подавлением боковых лепестков, что резко снижает возможности средств РРТР в составе комплекса РЭП по вскрытию параметров КРУ БПЛА значимых для ее подавления;
- варианты организации КРУ на одних и тех же частотах в дуплексном режиме встречаются исключительно на простых малых БПЛА. Достаточно часто встречающимся вариантом организации КРУ для БПЛА специального назначения является формирование направлений

«вверх» и «вниз» не только на различных частотах, но даже в различных частотных диапазонах (L, C, S, Ku диапазоны), и с различными частотно-временными параметрами. В результате успешное вскрытие параметров КРУ «вниз», при подлете БПЛА к контролируемому рубежу, не позволяет сформировать целеуказания средствам РЭП для подавления КРУ в направлении «вверх»;

- в КРУ, как в наиболее важном элементе системы управления БПЛА, широко используются различные способы повышения помехозащищенности: ШПС, автоматическая перестройка частоты на наименее пораженные помехами каналы, использование режима ППРЧ, резервирование каналов, многократное дублирование команд управления и передаваемых ТМИ, использование антенн с направленными ДНА, высокий уровень криптозащиты передаваемых данных и т.д.

Однако первостепенными являются не эти трудности, а то, что даже успешное вскрытие и подавление КРУ не гарантирует, что БПЛА прекратит свой полет в направлении контролируемой зоны. Как правило при отсутствии внешнего управления, БПЛА переходит в автономный режим, при этом его действия в этом режиме полностью определяются предварительно заложенной программой автономного полета. При этом сутью программы может быть не «возврат к ПУ», а продолжение дальнейшего полета к контролируемому объекту и выполнение целевой задачи с использованием всех доступных способов навигации. Для БПЛА, используемых в незаконных или военных целях, именно эта программа реализуется чаще всего. Таким образом, подавление КРУ может снизить вероятность успешного выполнения БПЛА целевой задачи, но не гарантирует каких-либо однозначных действий по прекращению полета БПЛА в направлении контролируемого рубежа, активации «программы возвращения» или «программы посадки» и т.д. Именно отсутствие однозначной реакции БПЛА на успешное подавление КРУ является существенным недостатком комплексов противодействия БПЛА основанным исключительно на РЭП.

Следующей по важности радиолинией БПЛА, которая является уязвимой для средств РЭП, является линия «вниз» в направлении «БПЛА – ПУ», предназначенная для передачи данных от специальной аппаратуры и технических средств полезной нагрузки, размещенных на БПЛА. Дело в том, что довольно распространенным способом управления БПЛА остается режим ручного управления им со стороны оператора по визуальным данным от ОЭС видимого диапазона. Особенностью этой линии является следующее. Передаваемые от ОЭС на ПУ видеоданные имеют большой объем, требуют широкой полосы частот для передачи, и в связи с их высокими скоростями и необходимостью передачи в режиме реального времени, могут не подвергаться криптозащите даже на БПЛА специального и военного назначения. При этом сложность организации на БПЛА большеразмерных остронаправленных антенных систем, ведет к тому, что зачастую эти данные передаются либо через всенаправленную антенну, либо через антенну с широким главным лепестком ДНА (порядка 60-90°). Это позволяет относительно легко не только вскрывать сигнально-частотные параметры данной линии связи, но и получать доступ к передаваемым видеодан-

ным. Подавление такой линии потенциально бы позволило лишить оператора визуальной обратной связи, и принудить его управлять БПЛА, так сказать, «по приборам» т.е. только по данным ТМИ поступающим по КРУ «вниз», что резко бы снизило эффективность и эргономичность управления. Вместе с тем высокоэффективное подавление этой линии связи требует знания местоположения ПУ или промежуточного узла-ретранслятора, используемых для управления БПЛА. При этом высота полета БПЛА, а также возможность размещения ПУ или узлов-ретрансляторов на летно-подъёмных средствах, потенциально обеспечивают больший радиогоризонт и, как следствие, более высокую дальность организации связи прямой видимости, чем дальность действия наземных средств РЭП. В результате весьма вероятна ситуация, когда при наличии полной информации о сигнально-частотных параметрах линии «вниз» будет невозможно подавить ПУ и узлы-ретрансляторы, ввиду их пространственной недоступности для наземных средств РЭП.

Вышеуказанное относится к подавляющему числу БПЛА и является фундаментальными ограничениями, накладываемыми на эффективность существующих комплексов РЭП, ориентированных на противодействие БПЛА.

Далее будут более подробно рассмотрены различные технические аспекты проблематики подавления каналов управления и связи с БПЛА, при этом большее внимание будет уделено вопросам подавления каналов малых БПЛА, как наиболее опасных и сложных объектов для противодействия.

4.2. Особенности организации связи в командной радиолинии управления БПЛА

Командная радиолиния управления в направлениях «вверх» и «вниз» предназначена для передачи наиболее критических данных для процесса нормального управления полетом БПЛА: команд управления с ПУ и квитанций об их исполнении, программ полета, программ действий в автономном режиме, навигационных и специальных данных, обеспечивающих нормальное функционирование БПЛА, а также ТМИ о состоянии отдельных подсистем, остатке топлива и т.д. Указанные данные, как правило, имеют относительно малый объем и требуемую скорость передачи (порядка 2,4-200 кбит/с), однако, должны передаваться в масштабе реального времени.

Для больших и средних БПЛА специального и военного назначения, как правило КРУ организуется в режиме прямой видимости с наземным или воздушным ПУ, а при значительном удалении ПУ – ретрансляцией через узел-ретранслятор на летно-подъёмном средстве или через ССС. Для малых БПЛА как специального, так и коммерческого назначения КРУ организуется в режиме прямой видимости с наземным ПУ.

4.2.1. Специальные и военные БПЛА

Обобщая материалы работ [64-107] возможно сформировать следующие обобщенные ТТХ КРУ специальных и военных БПЛА, значимых для радиоэлектронного подавления.

При организации КРУ специальных и военных больших и средних БПЛА через ССС, как правило, используются ССС Irudum, Inmarsat, MOUS, WGS, при этом линии связи формируются в УКВ, L, X, Ku, Ka диапазонах. В УКВ диапазоне используются низкоскоростные каналы шириной по 25 кГц с QPSK сигналами. В L, Ku, X и Ka диапазонах производится «упаковка» КРУ в широкополосный общий спутниковый канал ССС (например, ССС Iridium, Inmarsat или WGS), на основе кодового (CDMA – Code Division Multiple Access) или частотно-временного (MF-TDMA – Multi-Frequency Time-Division Multiple Access) разделения абонентов с использованием BPSK, QPSK, 8PSK, 8QAM сигналов. Ширина главного лепестка ДНА спутниковой связи на БПЛА составляет порядка 10-35° [109].

Для управления специальными и военными малыми БПЛА (например, такими как RQ-7B Shadow 200, RQ-11B Raven, RQ-16T-Hawk и др.), как правило, организуется КРУ в режиме прямой видимости с наземным ПУ или с узлом-ретрансляции:

- каналы в L (1,4-1,85 ГГц), S (2,2-2,5 ГГц), C (4,4-5,85 ГГц), и Ku (15,15-15,35 / 14,4-14,83 ГГц) диапазонах – основные каналы КРУ;
- в УКВ диапазоне (220-400 МГц) – резервные каналы КРУ;
- спутниковый канал (как правило используется низкоорбитальная ССС Iridium обеспечивающая возможность использованиям небольших антенн) L-диапазона (1,616-1,6265 ГГц) – резервный канал КРУ, устанавливаемый опционально на отдельных БПЛА.

Ширина каналов:

- канал «вверх» в L, S, C и Ku диапазонах: в режиме фиксированной частоты – 300-700 кГц; в режиме ШПС – 0,7-28 МГц;
- канал «вниз» в L, S, C и Ku диапазонах: 3-20 МГц;
- каналы «вверх»/«вниз» в УКВ диапазоне: 25 кГц.

Скорости передачи данных в КРУ:

- до 20 кбит/с – в линии «вверх»; 200 кбит/с – в линии «вниз» (при передаче только ТМИ); 1,6-12 Мбит/с – в линии «вниз» (при передаче ТМИ совместно с данными от ОЭС БПЛА для визуального управления оператором) в L, S, C и Ku диапазонах;
- 2,4-16 кбит/с в линиях «вверх»/«вниз» в УКВ диапазоне;
- до 2,4 кбит/с в линиях «вверх»/«вниз» по спутниковой линии L диапазона (для ССС Iridium);

Мощности передатчиков:

- в L, C, S, Ku диапазоне в каналах «вверх»/«вниз»: 5-15 Вт;
- в УКВ диапазоне в каналах «вверх»/«вниз»: 15-25 Вт.

Используемые типы сигналов: BPSK, QPSK (DQPSK, SOQPSK), 2FSK, GMSK. Возможно использование режима ППРЧ в пределах разрешенной к использованию полосы частот в S, C и Ku диапазонах (например, встречаются варианты организации КРУ БПЛА с использованием режима ППРЧ по 10 каналам шириной по 4 МГц каждый в общей полосе 40 МГц). Тип помехоустойчивого кодирования: коды Рида-Соломона, сверточное кодирование, кодирование Витерби, турбо-кодирование, LDPC-кодирование. Скорости кода R=1/2, 2/3, 3/4.

Типы многостанционного доступа: «точка-точка», многостанционный доступ БПЛА в режимах частотного (FDMA – Frequency Division Multiple Access) и временного (TDMA – Time-Division Multiple Access) разделения абонентов.

На БПЛА, стоящих на вооружении стран НАТО, формат данных КРУ, порядок передачи и обработки команд определяется стандартами STANAG: 4586, 4660 и 7085.

Для криптографической защиты данных в КРУ специализированных и военных БПЛА используется шифрование в соответствии со стандартами: MIL-STD-188-181A, MIL-STD-188-183, NSA Type I, Triple DES, AES-128, AES-256.

На БПЛА используются либо всенаправленные антенны, либо направленные антенны с шириной ДНА порядка 60-90° и усилением 2-4 дБи. Наземные ПУ используют следящие за БПЛА поворотные антенны диаметром до 1,2 м с усилением до 40 дБи с остронаправленной ДНА до 3,5-5°.

Дальность связи:

- в направлении ПУ – БПЛА с использованием направленных антенн на ПУ: до 75 км;
- в направлении ПУ – БПЛА / ПУ – БПЛА с использованием ненаправленных антенн: до 15 км;
- в направлении БПЛА – ПУ с использованием направленных антенн на БПЛА и ПУ: до 55 км.

4.2.2. Коммерческие БПЛА

Обобщая материалы работ [64-108] возможно сформировать следующие обобщенные ТТХ КРУ малых коммерческих БПЛА, значимых для радиоэлектронного подавления.

Для коммерческих малых БПЛА, направления «вверх» / «вниз» КРУ организуются в фиксированных частотных диапазонах, которые, как правило, соответствуют использованию на БПЛА одной или нескольких коммерческих технологий связи:

- RC433: 433 МГц;
- сети 4G: 725-770, 790-830, 850-894 МГц;
- сети CDMA: 850-894 МГц:
- RC868: 868-916 МГц;
- GSM900: 890-915, 935-960 МГц;
- GSM1800: 1710-1880 МГц;
- сети 3G: 2110-2170 МГц;
- сети Wi-Fi на базовой частоте 2,4 ГГц: 2,4-2,5 ГГц;
- сети 4G: 2,5-2,7 ГГц;
- сети Wi-Fi на базовой частоте 5,2 ГГц: 4,9-5,5 ГГц;
- сети Wi-Fi на базовой частоте 5,8 ГГц: 5,5-6,1 ГГц.

Используемые типовые частоты, ширина типовых каналов, типы сигналов и помехоустойчивого кодирования, мощности передатчиков и ТТХ приемных средств определяются соответствующими стандартами на вышеуказанные технологии связи. Данные по наиболее распространённым стандартам Wi-Fi,

используемым для управления малыми коммерческими БПЛА, представлены в таблице 4.

Таблица 4 – Данные по наиболее распространенным стандартам Wi-Fi, используемым для управления коммерческими малыми БПЛА

Характеристика	Wi-Fi IEEE 802.11b	Wi-Fi IEEE 802.11g	Wi-Fi IEEE 802.11n
Диапазон частот, ГГц	S (2,4-2,483)	S (2,4-2,483)	S (2,4-2,483), C (5,725-5,875)
Ширина канала, МГц	22	22	20, 40
Мощность передатчика, дБм	до 20	до 20	до 20
Технология разделения каналов	FDMA	FDMA, OFDM	FDMA, OFDM
Используемые сигналы	DBPSK, DQPSK	BPSK, QPSK, 16QAM, 64QAM	BPSK, QPSK, 16QAM, 64QAM
Помехоустойчивое кодирование	код Баркера, комплементарные последовательности, сверточное кодирование		сверточное кодирование *R*=5/6
Скорость передачи данных, Мбит/с	до 11	до 54	до 100
Дополнительные технологии помехозащиты	Стандартом предусмотрена возможность использования DSSS и ППРЧ		Стандартом предусмотрена возможность использования HR-DSSS и MIMO
Шифрование (опционально)*	WEP, WPA, DES, AES-128, AES-256		

*Шифрование данных в коммерческих БПЛА может не использоваться.

Особенностью организации канала «вниз» КРУ в малых коммерческих БПЛА является, то, что фактически сам канал отсутствует, а роль ТМИ от БПЛА выполняют видеоданные, поступающие от ОЭС БПЛА и предназначенные для визуального управления со стороны оператора.

ТТХ каналообразующей аппаратуры различных КРУ малых коммерческих БПЛА представлены в таблице 5.

Таблица 5 – ТТХ каналообразующей аппаратуры различных КРУ малых коммерческих БПЛА [108]

Параметр	Значения параметров				
Наименование КРУ	3D Link	Skyhopper PRO	Picoradio OEM	SOLO7	J11
Производитель, страна	Geoscan, РФ	Mobilicom, Израиль	Airborne Innovation, Канада	DTC, Великобритания	Redess, Китай
Диапазон частот, ГГц	S (2,4-2,483), C (5,725-5,875)				
Дальность связи, км	20-60	5	н/д	н/д	10-20

Параметр	Значения параметров				
Наименование КРУ	3D Link	Skyhopper PRO	Picoradio OEM	SOLO7	J11
Скорость передачи данных, Мбит/с	0,023-64,9	1,6-6	0,78-28	0,144-31,668	1,5-6
Задержка передачи данных, мс	1-20	25	н/д	15-100	15-30
Мощность передатчика, дБм	25	н/д	27-30	20	30
Чувствительность приемника, дБм:	–78,6... −122	−101	–76... −101	–95... −104	–90... −97
Энергетический бюджет КРУ, дБ	103-147	н/д	103-131	н/д	120-127
Поддерживаемые полосы частот, МГц	4-20	4,5; 8,5	2; 4; 8	0,625; 1,25; 2,5; 6; 7; 8	2; 4; 8
Режим организации связи	Дуплекс	Дуплекс	Дуплекс	Симплекс	Дуплекс
Поддержка разнесенного приема	да	да	да	да	да
Отдельный канал для управления/телеметрии	да	да	да	нет	да
Используемые протоколы управления БПЛА в КРУ / ТМИ	MAVLink, проприетарные	MAVLink, проприетарные	нет	нет	MAVLink
Поддержка мультиплексирования в канале КРУ / ТМИ	да	да	нет	нет	н/д
Используемые сетевые топологии:					
«точка – точка»	да	да	да	да	да
«точка – многоточка»	да	да	да	нет	да
ретрансляция данных	да	да	да	нет	да
Средства повышения помехозащищенности	DSSS, подавители узкополосных и импульсных помех	н/д	н/д	н/д	н/д
Энергопотребление блока связи на БПЛА, Вт	6-7	н/д	4,8	4,5-7	8
Энергопотребление блока связи на ПУ, Вт	7	н/д	4,8	8	5
Габариты бортового блока, длинна × ширина × высота, мм	77×45×25	74×54×26	40×40×10 (без корпуса)	67×68×22	76×48×20
Масса бортового блока, г	89	105	17,6 (без корпуса)	135	88

Примечание: н/д – нет данных.

4.3. Особенности организации связи в радиолиниях передачи данных с БПЛА

При организации линий передачи данных «вниз» по направлению «БПЛА – ПУ» необходимо учитывать следующие особенности:

- специальная аппаратура и технические средства полезной нагрузки, размещенные на БПЛА, формируют потоки данных значительного объема (таблица 6), при этом, в большинстве случаев передачу этих данных необходимо вести в режиме времени близком к реальному (например, видеоданные от ОЭС БПЛА зачастую используются оператором для управления БПЛА в ручном режиме);

Таблица 6 – Приблизительные оценки интенсивности потоков данных, формируемых специальной аппаратурой и техническими средствами полезной нагрузки БПЛА

Технические средства полезной нагрузки	Кол-во источников данных на БПЛА	Интенсивность потока данных от одного источника без сжатия	Интенсивность потока данных от одного источника с учетом предварительного сжатия
ТВ-камера	1-4	10-150 Мбит/с	2-6 Мбит/с
Фото-камера	1-4	до 20 Мбит/с	до 4 Мбит/с
Тепловизионная аппаратура	1-4	до 0,5 Мбит/с	до 0,5 Мбит/с
Лазерная аппаратура	1	до 0,5 Мбит/с	до 0,5 Мбит/с
РЛС	1	5-200 Мбит/с	до 10 Мбит/с
РРТР аппаратура (с обработкой сигналов РЛС на борту)	1	до 5 Мбит/с	0,2-1 Мбит/с

- большой объем формируемых данных, а также ограниченность доступного частотного ресурса предопределяет необходимость использования различных способов и технологий оптимизации пропускной способности и повышения скорости линии передачи данных: использование технологии адаптивной смены сигнально-кодовых конструкций ACM (Adaptive Coding and Modulation); технологии спектрального уплотнения OFDM (Orthogonal Frequency-Division Multiplexing), технологий сжатия данных на борту. При этом небольшие габариты БПЛА препятствуют размещению на нем направленных антенных систем с относительно высоким коэффициентом усиления, однако возможно использование антенных систем MIMO (Multiple Input Multiple Output) на основе нескольких простых антенн;
- большой объем формируемых данных, необходимость их передачи в режиме реального времени, а также отсутствие высокопроизводительной аппаратуры шифрования на борту БПЛА, предопределяет использование либо низкого уровня криптозащиты, либо ее полное отсутствие.

4.3.1. Специальные и военные БПЛА

Обобщая материалы работ [64-107, 109] возможно сформировать следующие обобщенные ТТХ радиолиний передачи данных со специальных и военных БПЛА, значимых для их радиоэлектронного подавления.

Для передачи данных с больших и средних БПЛА специального и военного назначения через ССС, как правило, используются ССС WGS и Inmarsat, а также другие совместимые с ними по режимам организации связи широкополосные ССС. Линия связи «вниз» с ретрансляцией через ССС, как правило, формируется в Ka диапазоне (30-31 / 20,2-21,2 ГГц) в полосе частот 125 МГц, в которой требуемая полоса частот выделяется подканалами с шириной 2,6 МГц. Это позволяет гибко формировать требуемую пропускную способность линии, обеспечивая скорости передачи 10-137 Мбит/с. Ширина главного лепестка ДНА спутниковой связи на БПЛА составляет 10-35° [109].

Для высокоскоростного получения данных со специальных и военных малых БПЛА (например, таких как RQ-7B Shadow 200, RQ-11B Raven, RQ-16T-Hawk и др.), как правило, организуется высокоскоростная линия связи в режиме прямой видимости (без ретрансляции) с наземным ПУ в S (2,2-2,5 ГГц), C (4,4-5,85 ГГц), и Ku (15,15-15,35 / 14,4-14,83 ГГц) диапазонах. Ширина линии связи 3-40 МГц. Типовые скорости передачи данных 1,6-12 Мбит/с, при использовании режима частотного ортогонального уплотнения OFDM совместно с QAM сигналами скорость передачи данных повышается до 45 Мбит/с.

Используемые типы сигналов: BPSK, QPSK (DQPSK, SOQPSK), FSK, GMSK, QAM (16QAM, 64QAM). Тип помехоустойчивого кодирования: коды Рида-Соломона, сверточное кодирование, кодирование Витерби, турбо-кодирование, LDPC-кодирование, со скоростями кода R=1/2, 2/3, 3/4. Типы многостанционного доступа: «точка-точка», многостанционный доступ БПЛА в режимах частотного (FDMA – Frequency Division Multiple Access) и временного (TDMA – Time-Division Multiple Access) разделения абонентов.

Компрессия видеоданных, поступающих от ОЭС БПЛА: MPEG-2/4, H.264.

Стандарты «упаковки» передаваемой информации: DVB, DVB-S1/S2, DVB-T1/T2.

Для криптографической защиты передаваемых данных может использоваться шифрование по стандартам: NSA Type 1, AES-128, AES-256. При отсутствии на БПЛА средств высокоскоростного шифрования данные от БПЛА передаются без криптозащиты.

На БПЛА, стоящих на вооружении стран НАТО, формат данных полезной нагрузки, порядок их передачи и обработки определяется стандартами STANAG: 4545, 4559, 4575, 4607, 4609, 7023, 7085.

На БПЛА используются либо всенаправленные антенны, либо направленные антенны с шириной ДНА порядка 60-90° и усилением 2-4 дБи. Наземные ПУ используют следящие за БПЛА поворотные антенны диаметром до 1,2 м с усилением до 40 дБи с остронаправленной ДНА до 3,5-5°.

Мощности передатчиков БПЛА и ПУ составляют порядка 5-15 Вт.

Дальность связи:

- в направлении ПУ – БПЛА с использованием направленных антенн на ПУ: до 75 км;
- в направлении ПУ – БПЛА / ПУ – БПЛА с использованием неправленных антенн: до 15 км;
- в направлении БПЛА – ПУ с использованием направленных антенн на БПЛА и ПУ: до 55 км.

4.3.2. Коммерческие БПЛА

Обобщая материалы работ [64-108] возможно сформировать следующие обобщенные ТТХ радиолиний передачи данных с коммерческих малых БПЛА, значимых для их радиоэлектронного подавления.

Для коммерческих малых БПЛА, направления «вверх» / «вниз» КРУ организуются в фиксированных частотных диапазонах, которые, как правило, соответствуют использованию на БПЛА одной или нескольких коммерческих технологий связи:

- RC433: 433 МГц;
- сети 4G: 725-770, 790-830, 850-894 МГц;
- сети CDMA: 850-894 МГц:
- RC868: 868-916 МГц;
- GSM900: 890-915, 935-960 МГц;
- GSM1800: 1710-1880 МГц;
- сети 3G: 2110-2170 МГц;
- сети Wi-Fi на базовой частоте 2,4 ГГц: 2,4-2,5 ГГц;
- сети 4G: 2,5-2,7 ГГц;
- сети Wi-Fi на базовой частоте 5,2 ГГц: 4,9-5,5 ГГц;
- сети Wi-Fi на базовой частоте 5,8 ГГц: 5,5-6,1 ГГц.

Используемые типовые частоты, ширина типовых каналов, типы сигналов и помехоустойчивого кодирования, мощности передатчиков и ТТХ приемных средств определяются соответствующими стандартами на вышеуказанные технологии связи и соответствуют ТТХ, представленным выше для КРУ на основе технологии Wi-Fi (таблицы 4-5).

Основным типом данных, передаваемых по каналу «вниз» являются видеоданные, поступающие от ОЭС БПЛА и предназначенные для визуального управления со стороны оператора. Формат передаваемых видеоданных: MPEG-2/4, MPEG-TS, H.264.

Для передачи видеоданных, а также мультиплексирования видеоданных и ТМИ, помимо радиолиний на основе Wi-Fi могут использоваться радиолинии на основе стандартов DVB, предназначенных для цифрового телевизионного вещания: DVB-T1/T2 или DVB-S2 (таблица 7). Для передачи высокоскоростных потоков основным требованием является энергетическая эффективность, поэтому в условиях многолучевого распространения, в последнее время, предпочтение отдается технологии DVB-T2 (с использованием OFDM), как наиболее устойчивой к межсимвольной интерференции, потери от которой могут достигать 10 дБ. При этом значительный пик-фактор, свойственный радиосигналу

DVB-T2 с множеством ортогональных несущих, компенсируется умеренными требованиями к средней выходной мощности передающего устройства.

Таблица 7 – ТТХ радиолиний на основе стандартов DVB

Характеристика	DVB-T1	DVB-T2	DVB-S2
Диапазон частот, ГГц	S (2,4-2,483), C (5,725-5,875)		
Ширина канала, МГц	6; 7; 8	1,7; 5; 6; 7; 8; 10	36
Технология разделения/уплотнения каналов	FDMA, OFDM		FDMA
Используемые сигналы	QPSK, 16QAM, 64QAM	QPSK, 16QAM, 64QAM, 256QAM	QPSK, 8PSK, 16APSK, 32APSK
Помехоустойчивое кодирование	FEC, PC	FEC, LDCP-код, БЧХ	FEC, LDCP-код
Скорость кода	1/2, 2/3, 3/4, 5/6, 7/8	1/2, 3/5, 2/3, 3/4, 4/5, 5/6	1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 8/9, 9/10
Скорость передачи данных, Мбит/с	до 31,67	до 50,34	
Технологии помехозащиты	ACM	ACM	ACM (прием до –2,4 дБ)
Инкапсуляция данных	MPEG-TS	MPEG-4, GTS, PLP	MPEG-4, PLP

4.4. Особенности радиоэлектронного подавления радиолиний управления и передачи данных БПЛА

Эффективность подавления радиолиний управления и передачи данных БПЛА определяется следующими факторами:

- условиями распространения радиоволн на трассе радиолиний БПЛА – ПУ, а также на трассе радиоподавления;
- энергетической, временной и пространственной доступностью приемников средств связи на БПЛА и ПУ для средств РЭП, а также их чувствительностью;
- мощностью передатчиков средств связи БПЛА и ПУ, а также средств РЭП;
- типом антенных систем, взаимной ориентацией ДНА средств связи БПЛА и ПУ, а также средств РЭП;
- используемыми для передачи шириной полосы частот, типом сигнала, типом помехоустойчивого кодирования, скоростью кода.

Для подавления радиолиний управления и передачи данных БПЛА используются следующие типы помех.

1) Помехи, перекрывающие рабочий диапазон частот, предположительно используемый для организации связи с БПЛА. Данный тип помех используется при отражении массированного налета БПЛА, когда невозможно вскрыть параметры частных КРУ отдельных БПЛА и требуется перекрыть весь используемый диапазон частот, или же при невозможности средствами РРТР вскрыть частотные параметры линий связи.

К таким помехам относятся:

- заградительная шумовая помеха (белый шум высокой мощности) во всем диапазоне частот;
- узкополосная шумовая или гармоническая (одночастотное или модулированное гармоническое колебание) помеха, скользящая по диапазону частот.

2) Помехи, прицельные по частоте линий управления и связи БПЛА. Данный тип помех используется при подавлении одиночных БПЛА или группы БПЛА, управляемых по одной КРУ, когда средствами РРТР достоверно вскрыты частотные параметры линий связи. К таким помехам относятся:

- шумовая помеха, прицельная по частоте линии связи;
- гармоническая помеха, прицельная по частоте линии связи;
- узкополосная шумовая или гармоническая помеха, скользящая по используемому диапазону частот (при использовании линий связи с ШПС или ППРЧ);
- имитирующая помеха, прицельная по частоте линии связи и структуре передаваемых сигналов (имитирует структуру сигналов линии связи);
- имитирующая помеха, прицельная по частоте и структуре сигнала, а также по структуре и формату передаваемых данных (имитирует ложные данные, передаваемые по линии связи), с целью навязывания ложных режимов работы.

Эффективность подавления может быть повышена если средствами мониторинга вскрывается ожидаемая траектория полета БПЛА и средства РЭП могут формировать вышеуказанные помехи прицельно по направлению на БПЛА или его ПУ за счет изменения ориентации ДНА антенных систем.

В настоящее время широкое распространение получили шумовые помехи, прицельные по частотам линий связи БПЛА – ПУ. При этом, ввиду более высокой эффективности, перспективным является использование имитирующих помех, прицельных по структуре сигнала. Однако данный режим подавления более сложен в реализации и, по всей видимости, будет реализован в средствах РЭП следующего поколения.

При организации подавления линий управления и передачи данных БПЛА средства РЭП, как привило, придерживаются следующей логики функционирования.

1) При обнаружении факта налета БПЛА средства РРТР пытаются вскрыть частотные параметры линий радиосвязи «вверх» и «вниз». Если вскрытие частотных параметров данных линий невозможно, то средство РЭП переходит в режим излучения заградительных или скользящих помех по всему диапазону частот, потенциально используемому для организации связи с БПЛА по линям «вверх» / «вниз». В этот же режим средство РЭП переходит в случае если количество вскрытых линий связи превышает возможности средств РЭП по постановке помех, прицельных по частоте и по направлению.

2) Если произведено успешное вскрытие частотных параметров линий «вверх» / «вниз», то средства РРТР пытаются определить сигнально-структурные и пространственные параметры этих линий. Если вскрытие таких

параметров невозможно, то по ранее определённым частотным параметрам формируются шумовые или гармонические помехи, прицельные по частоте. Этот же тип помех формируется если успешное вскрытие сигнальных и структурных параметров радиолинии показывает, что данные радиолинии имеют высокостойкую криптографическую защиту.

3) Если функционал средства РЭП позволяет управлять ДНА, то постановка помех линии «вверх» осуществляется с учетом ориентации ДНА на БПЛА и его траекторного сопровождения. Если по результатам вскрытия пространственных параметров радиолиний определённо направление на ПУ, то постановка помех линии «вниз» осуществляется с учетом ориентированности ДНА средств РЭП на ПУ БПЛА.

4) Если по результатам вскрытия сигнально-структурных параметров радиолиний определенны тип и структура сигналов и ширина сигнала позволяет произвести его запись и воспроизведение [110], то имитационные структурно-прицельные помехи формируются путем циклического воспроизведения на частоте линии ранее записанного сигнала. Если определенны тип и структура сигналов, но ширина сигнала не позволяет произвести его запись, например, вследствие того, что используется сигналы ШПС или ППРЧ, то используется либо широкополосная шумовая помеха в полосе частот радиолинии, либо узкополосная шумовая или гармоническая помеха, скользящая по полосе частот радиолинии.

5) Если по результатам вскрытия сигнально-структурных параметров радиолиний определенны не только тип и структура сигналов, но также вскрыты формат и структура передаваемых данных, тип используемого протокола или кодека связи, то появляется возможность подмены управляющих команд БПЛА или передачи ложных данных путем формирования имитирующей помехи, прицельной по частоте и структуре сигнала, а также по структуре и формату передаваемых данных. Этот же тип помех может быть сформирован если в линии используется уязвимый или имеющий низкую криптографическую защищённость протокол шифрования. Наиболее распространенным примером такого подавления является вскрытие формата передаваемых видеоданных в канале «вниз», с записью и последующим циклическим воспроизведением ранее переданного видео, что фактически блокирует обратную связь для оператора.

Приблизительная оценка эффективности подавления линий управления и передачи данных может быть оценена путем использования двух основных, относительно простых, подходов:

- расчет помехозащищенности (по показателю BER (Bit Error Rite) – вероятности ошибочного приема бита P_b) используемой в радиолинии комбинации сигнала и помехоустойчивого кода при достигаемом значении ОСШ на входе приемника, с последующем сравнением ее с предельными требуемыми значениями $P_{b\,\text{тр}}$ для используемого протокола связи;
- расчет энергетического бюджета радиолинии, с последующем сравнением полученного значения с предельными значениями чувствительности приемника.

При использовании этих подходов предполагается, что помеха представляет собой аддитивный белый гауссовский шум (АБГШ) в полосе частот сигнала. Вопрос сведения сложных мультипликативных помех к эквивалентным аддитивным помехам, рассмотрен в работе [111].

Значение ОСШ q на входе приемника при постановке шумовой помехи средством РЭП в радиолинии равен (рис. 4) [112]:

$$q = \frac{P_{\text{с}} G_{\text{с}} F_{\text{с}}(\phi_{\text{СА}}) F_{\text{а}}(\phi_{\text{АС}})}{P_{\text{п}} G_{\text{п}} F_{\text{п}}(\phi_{\text{ПА}}) F_{\text{а}}(\phi_{\text{АП}})} \cdot \frac{D_{\text{п}}^2}{D_{\text{с}}^2} \cdot \frac{\Delta f_{\text{п}}}{\Delta f_{\text{с}}} \cdot \frac{1}{\gamma},$$

где: $P_{\text{С}}$ – мощность передатчика (ПРД) абонента-излучателя сигнала в радиолинию; $P_{\text{п}}$ – мощность ПРД помех средства РЭП; $G_{\text{с}}$ – коэффициент направленного действия (КНД) передающей антенны в радиолинии; $G_{\text{п}}$ – КНД передающей антенны средства РЭП; $D_{\text{п}}$ – расстояние от средства РЭП до приемника (ПРМ) абонента-получателя в радиолинии; $D_{\text{с}}$ – расстояние от ПРД сигнала до ПРМ в радиолинии; $F_{\text{п}}(\phi_{\text{ПА}})$ – функция, описывающая ориентацию оси ДНА средства РЭП относительно ДНА ПРМ абонента-получателя в радиолинии; $F_{\text{а}}(\phi_{\text{АП}})$ – функция, описывающая ориентацию ДНА ПРМ абонента-получателя радиолинии относительно направления на средство РЭП; $F_{\text{с}}(\phi_{\text{СА}})$ – функция, описывающая ориентацию ДНА ПРД абонента-излучателя сигнала в радиолинии относительно направления на абонента-получателя; $F_{\text{а}}(\phi_{\text{АС}})$ – функция, описывающая ориентацию ДНА ПРМ абонента-получателя относительно направления на абонента-излучателя в радиолинию; γ – коэффициент поляризации, учитывающий различие поляризации передающей антенны средства РЭП и приемной антенны абонента-получателя; $\Delta f_{\text{с}}$ – полоса пропускания приемника радиолинии; $\Delta f_{\text{п}}$ – ширина энергетического спектра помех, излучаемых средством РЭП.

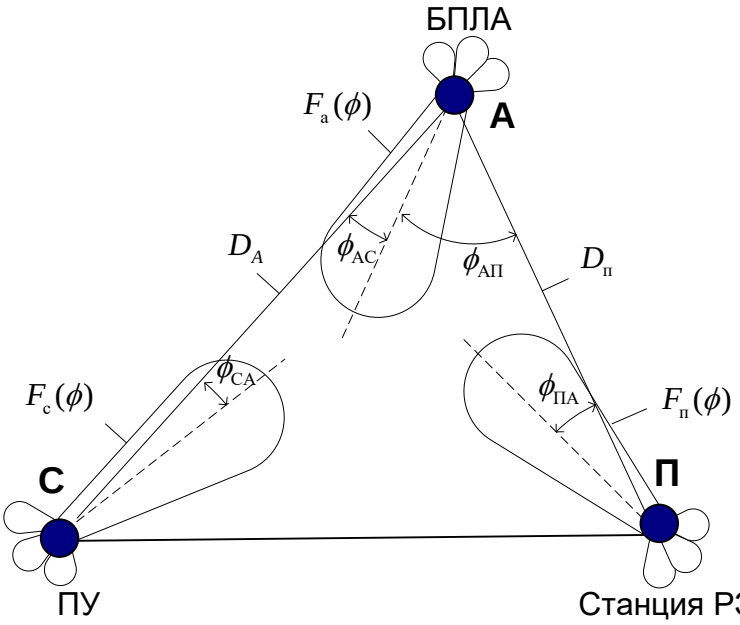


Рис. 4. Вариант взаимного положения в пространстве БПЛА, ПУ и станции РЭП [112]

Знание значения ОСШ на входе ПРМ и используемого типа сигнала позволяет определить значение вероятности ошибочного приема бита P_b. Сравнение значения P_b с требуемыми значениями $P_{b\,тр}$ для КРУ и канала передачи данных (таблица 8) позволяет сделать вывод о потенциальной эффективности подавления.

Таблица 8 – Требуемые значения достоверности передачи данных для КРУ и канала передачи данных

Параметры	КРУ «вверх»	КРУ «вниз»	Линия передачи данных «вниз»
Передаваемая информация	Команды управления	ТМИ	Данные от бортовых средств ОЭС, РЛС и т.д.
Протоколы передачи	IP/TCP, X.25, MAVlink, SLT.DSM, XBee, проприетарные протоколы		DVB, MPEG-TS, MPEG-2/4, H.264
Требуемая достоверность передачи данных, $P_{b\,тр}$	10^{-6}		10^{-3}

В теоретических работах [113-117] для учета различных особенностей приема BPSK, QPSK и M-QAM, сигналов обосновываются различные аналитические выражения для расчета вероятности ошибки на бит P_b, достаточные для инженерного применения, в зависимости от энергетических соотношений ОСШ с АБГШ. На основе этих выражений, например, в работах [118, 119] рассчитаны значения P_b для типовых сигнально-кодовых конструкций, используемых в линиях радиосвязи с БПЛА – рис. 7.

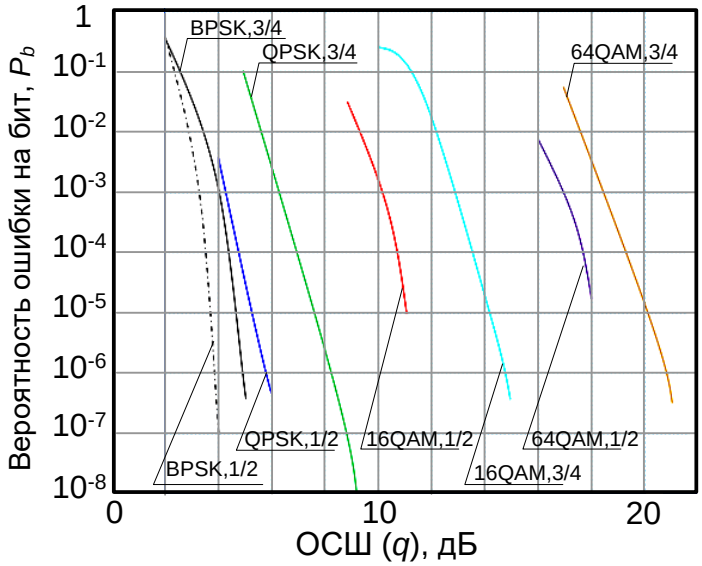


Рис. 7. Зависимость вероятности битовой ошибки P_b от ОСШ для типовых сигнально-кодовых конструкций, используемых в линиях радиосвязи с БПЛА [118, 119]

Для коррекции и экспериментальной проверки аналитических выражений оценки помехозащищенности $P_b(q)$, для наиболее распространенных сигналов, типов кодирования (таблица 4 и 7), а также условий применения БПЛА были

проведены экспериментальные исследования. Эксперименты проводилась по методике, представленной в работе [120]. При этом рассматривались нижеуказанные модели многолучевого распространения [120, 121].

1. Модель гауссовской линии – соответствует радиолинии с АБГШ, в котором многолучевость полностью отсутствует, то есть рассматривается единственный прямой луч между ПРД и ПРМ. Таким образом, данная модель описывает идеальные условия распространения на трассе «ПУ – БПЛА», которые, как правило, не встречаются на практике, но зачастую соответствует верхней границе оценки помехозащищенности P_b, полученной расчетно-теоретическим путем [113-117].

2. Модель райсовской линии - соответствует радиолинии с помехами (АБГШ, импульсные и гармонические помехи), моделирует наличие прямого луча и нескольких отраженных лучей с разными мощностью и задержками прихода в точку приема, статистические свойства которых описываются распределением вероятностей Райса. Данная модель соответствует условиям полета БПЛА в прямой радиовидимости ПУ, с учетом переотражения электромагнитных волн от поверхности Земли и других объектов.

3. Модель рэлеевской линии – отличается от райсовской отсутствием прямого луча, при этом статистические свойства отраженных лучей описываются распределением вероятностей Рэлея. Соответствует условиям полета БПЛА в отсутствие прямой радиовидимости ПУ на относительно низкой высоте в пересеченной местности или в высотной городской застройке.

Исследования линии радиосвязи ПУ – БПЛА проводились для QPSK, 16QAM, 64QAM сигналов. В качестве помехоустойчивого кода использовалось кодирование Витерби со скоростями R = 1/2, 2/3, 3/4, 5/6, 7/8. В качестве помехи рассматривалась шумовая помеха – АБГШ. При учете многолучевого распространения радиоволн использовались стандартные модели каналов RC20 и RL20 [121]. Влияние доплеровского сдвига частот не учитывалось. Результаты экспериментальной оценки помехозащищенности КРУ с QPSK, 16QAM, 64QAM сигналами, при типовой скорости кодирования R=3/4, представлены в виде среднего значения вероятности ошибки на бит P_b, который соответствует вероятности ошибочного приема бита после различных этапов декодирования (рис. 8 и 9) – на входе декодера Витерби ($P_{b\ in\ Vit}$) и на выходе этого декодера ($P_{b\ out\ Vit}$).

Анализ графиков на рис. 8 показал следующее. Значения показателей $P_{e\ out\ Vit}$ на выходе декодера Витерби в райсовской линии (полет БПЛА в прямой радиовидимости ПУ) соответствует ухудшению их на 1,5-5 дБ относительно гауссовой линии, что соответствует значению потерь за счет приема переотраженных сигналов. По мере роста ОСШ q увеличивается отклонение показателей $P_{b\ out\ Vit}$, что соответствует изменению структуры ошибок (наблюдается группирование ошибочно принятых бит) в радиолинии и на выходе декодера Витерби.

Аналогичный эффект характерен и для рэлеевской модели радиолинии (полет БПЛА в отсутствии радиовидимости ПУ в пересеченной местности или в городских условиях) – рис. 9. Наблюдается сдвиг значений $P_{b\ out\ Vit}$ на выходе

декодера Витерби на 10-20 дБ вправо, в рэлеевской линии относительно гауссовской, а также серии ошибочных битов (до 10 бит), разделенных интервалами безошибочного приема до нескольких десятков секунд. Данное исследование качественно и количественно соответствует результатам, полученным в работе [120].

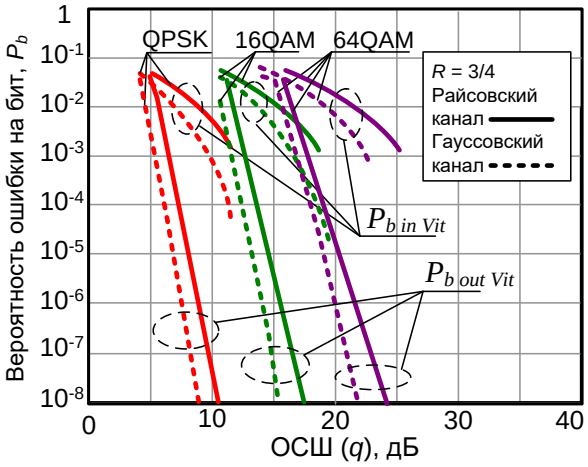


Рис. 8. Зависимость $P_b(q)$ на входе ($P_{b\ in\ Vit}$) и выходе кодера Витерби ($P_{b\ out\ Vit}$) для гауссовской и райсовской радиолиний

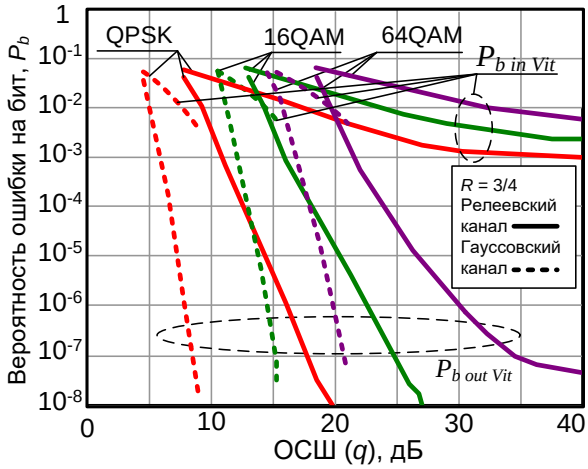


Рис. 9. Зависимость $P_b(q)$ на входе ($P_{b\ in\ Vit}$) и выходе кодера Витерби ($P_{b\ out\ Vit}$) для гауссовской и рэлеевской радиолиний

Оценка вклада помехоустойчивого кодирования в повышение помехозащищенности радиолиний связи с БПЛА проводилось путем оценки значения вероятности ошибки на бит на входе ($P_{b\ in\ Vit}$) и на выходе декодера Витерби ($P_{b\ out\ Vit}$). Данные значения для райсовской и рэлеевской радиолиний для кодовых скоростей R = 1/2, 2/3, 3/4, 5/6, 7/8 для сигнала 64QAM представлены на рис. 10.

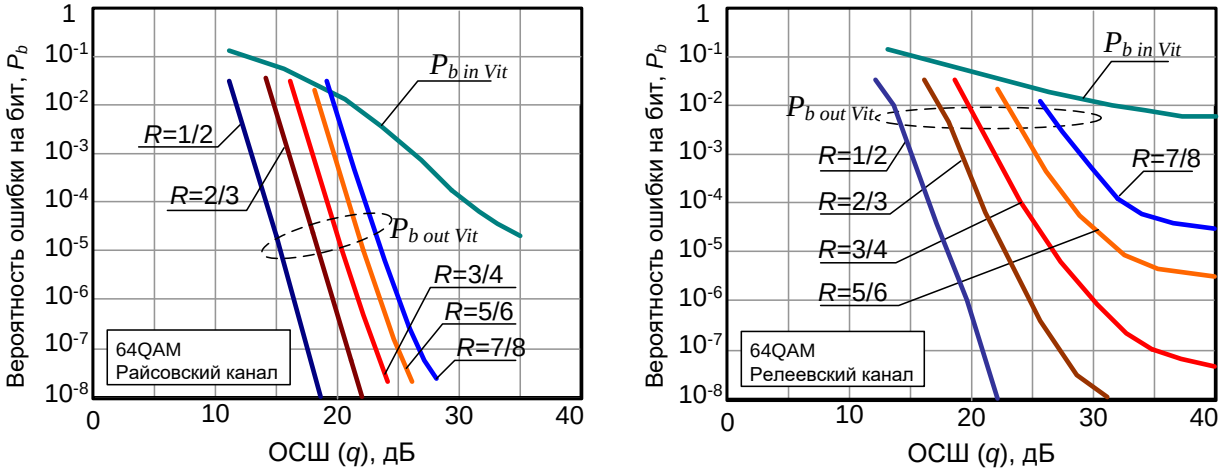


Рис. 10. Влияние значения скорости кода на помехоустойчивость линии радиосвязи

По результатам анализа можно сформировать приблизительные предельные значения ОСШ q (таблица 9), при которых достигается требуемый уровень

достоверности приема для типовых схем сигнально-кодовых конструкций, используемых в КРУ и в линии передачи данных. При ориентировании на эти данные следует иметь ввиду, что, как правило, разработчиками КРУ закладывается дополнительный запас на помехоустойчивость порядка 10 дБ. Указанные в таблице 9 данные является очень приблизительной и грубой оценкой, окончательная оценка требуемых энергетических затрат необходимых для нарушения функционирования КРУ и линии передачи данных средствами РЭП проводится после вскрытия сигнально-кодовых конструкций, используемых в радиолиниях «ПУ – БПЛА».

Значения ОШП в таблице 9 не учитывают возможности использования таких способов повышения помехозащищённости как расширение базы сигнала или использование режима ППРЧ. Вопросы воздействия помех на такие сложные типы сигналов как ШПС и ППРЧ рассмотрены в работах [122] и [123] соответственно.

Таблица 9 – Приблизительные значения ОСШ при которых достигается требуемый уровень достоверности приема в радиолиниях связи «ПУ – БПЛА» для типовых схем сигнально-кодовых конструкций

Условия полета	Тип радиолинии, тип передаваемых данных	Требуемая достоверность приема, $P_{b\,тр}$	Значение ОСШ при котором достигается требуемая достоверность приема, дБ									
			BPSK, 1/2	BPSK, 3/4	QPSK, 1/2	QPSK, 3/4	16QAM, 1/2	16QAM, 3/4	64QAM, 1/2	64QAM, 3/4	64QAM, 5/6	64QAM, 7/8
Полет БПЛА в прямой радиовидимости ПУ	КРУ «вверх», команды управления БПЛА	10^{-6}	6	7	8	9	14	16	17	22	24	25
	КРУ «вниз», ТМИ для ПУ, квитанции о выполнении команд											
	Радиолиния передачи данных «вниз», видеоданные от ОЭС*	10^{-3}	4	5	6	7	11	13	14	18	19	21
Полет БПЛА в отсутствии радиовидимости ПУ, в пересеченной местности или в городских условиях	КРУ «вверх», команды управления БПЛА	10^{-6}	11	13	16	17	21	23	20	30	46	н/д
	КРУ «вниз», ТМИ для ПУ, квитанции о выполнении команд											
	Радиолиния передачи данных «вниз», видеоданные от ОЭС*	10^{-3}	7	8	10	11	14	16	16	22	25	28

*В случае если ТМИ интегрированы в видеоданные и передаются в едином потоке, то рекомендуется ориентироваться на наиболее «худший» для средств РЭП вариант – подавление радиолинии «вниз» с $P_{b\,тр} = 10^{-3}$.

Для оценки помехозащищенности других сигнально-кодовых конструкций, которые не указаны в таблице 9, автор рекомендует обратиться к достаточно полному справочнику [124].

Достигаемое на входе ПРМ радиолинии значение ОСШ оценивается путем расчета энергетического бюджета радиолинии. Общая методика расчета энергетического бюджета радиолинии довольно подробно представлена в работах [124, 125] и, применительно к БПЛА, с учетом различных влияющих факторов, такой расчет проводился в статьях [71, 97, 107, 126].

Подводя итог оценке возможностей подавления линий КРУ и передачи данных, необходимо еще раз акцентировать внимание на то, что несмотря на достаточные возможности существующих средств РЭП по эффективному подавлению этих линий, такое подавление не гарантирует какой-либо определенной реакции БПЛА в виде прекращения полета БПЛА в направлении контролируемого рубежа, активации «программы возвращения» или «программы посадки» и т.д. Именно отсутствие однозначной реакции БПЛА на успешное подавление радиолиний является существенным недостатком комплексов противодействия БПЛА основанным исключительно на РЭП.

4.5. Особенности информационно-технического воздействия с целью вмешательства в процесс функционирования систем БПЛА или перехвата управления

Если по результатам анализа КРУ средствами РРТР удается определить не только тип и структуру сигналов, но также вскрыть формат и структуру передаваемых данных, тип используемого протокола управления или кодека связи, то появляется возможность подмены управляющих команд БПЛА или передачи ложных данных путем формирования имитирующей помехи, прицельной по частоте и структуре сигнала, а также по структуре и формату передаваемых данных. Фактически задача вскрытия формата и протокола передаваемых данных в КРУ относится уже не к задачам, которые решаются средствами РРТР, а к задачам средств форматной, потоковой и сетевой компьютерной разведки (КР). При этом формирование вышеуказанного типа помех соответствует уже не «чистому» РЭП, а, в большей степени, имитонавязыванию ложного управления [95] или информационно-техническому воздействию (ИТВ) на БПЛА реализуемого через его КРУ [91, 127-130, 148]. Одним из основных достоинств воздействия ИТВ на БПЛА является ее скрытность. Отсутствие явных признаков деструктивных воздействий на БПЛА, существенно затрудняет своевременное и адекватное принятие мер противодействия со стороны ПУ и операторов системы.

Доступ средств КР к форматам передаваемых данных КРУ возможен если в ней используется протокол шифрования с низкой криптоустойчивостью, либо протокол шифрования не используется вообще. Для БПЛА, в которых КРУ реализуется на основе коммерческих технологий Wi-Fi, WiMAX Mobile и LTE, средствами КР могут эксплуатироваться следующие уязвимости:

- подмена данных авторизации при установлении или поддержании соединения в КРУ;

- использование в Wi-Fi для шифрования передаваемых данных протоколов WEP (Wired Equivalent Privacy) и WPA (Wi-Fi Protected Access), которые имеют низкую криптографическую стойкость, при этом известны способы, позволяющие вскрыть ключевую информацию за считаное число минут [131, 132];
- использование в WiMAX Mobile для шифрования алгоритма DES (Data Encryption Standard) с ключами TEK (Traffic Encryption Key), которые имеют ограниченный срок действия, а также использование ложных сертификатов идентификации абонентских станций X.509 [131, 132];
- уязвимости процедур «attach», «detach» и «paging» для сетей LTE [133] и т.д.

После доступа средств КР к форматам передаваемых в КРУ данных, анализа их структуры и особенностей, появляется возможность сделать вывод о следующих аспектах управления БПЛА:

- используемые протоколы и форматы передачи данных в КРУ на канальном, сетевом и транспортном уровнях модели OSI (Open System Interconnect);
- используемый протокол управления БПЛА;
- текущая задача БПЛА, текущая последовательность выполняемых команд;
- данные о состоянии подсистем БПЛА (в составе ТМИ), данные от бортовых средств полезной нагрузки (прежде всего ОЭС);
- местоположение БПЛА по данным от бортовой навигационной системы;
- структура адресации, маршрутизации, а также приоритетности при передаче команд управления и данных полезной нагрузки в сети управления группой БПЛА;
- типы используемых на БПЛА и ПУ управляющей операционной системы (ОС), программного обеспечения (ПО), микроконтролеров (МК) управления радиосетью, отдельными бортовыми подсистемами и средствами полезной нагрузки БПЛА.

Вышеуказанные признаки формируют исходные данные для анализа уязвимостей одиночного или группы БПЛА как стандартной удаленной информационной системы (ИС) или, как сейчас их еще часто называют, киберфизической системы [149], каналом доступа к которой является КРУ. Основные уязвимости БПЛА как удаленной ИС рассмотрены в работе [130]. На основе уязвимостей системы «ПУ – БПЛА» как стандартной ИС могут быть предложены следующие ИТВ:

- ИТВ, основанные на нарушении доступности БПЛА или ПУ:
    - ИТВ, направленные на нарушение синхронизации и правил вхождения в связь;
    - ИТВ, направленные на снижение эффективности протоколов канального или сетевого уровней радиосети [134-138];
    - ИТВ типа DOS или DDOS-атаки на входные порты ИС, с целью переполнения входного буфера [132];

- ИТВ на нарушение нормального функционирования ПО МК, управляющих средствами связи;

- ИТВ, основанные на нарушении конфиденциальности и целостности связи между БПЛА или ПУ:
  - внедрение в КРУ ложного ПУ с целью перехвата управления БПЛА и навязывания ему новых режимов полета;
  - отправка на БПЛА некорректных или разнонаправленных команд, которые переводят его в аэродинамически-неустойчивый режим полета;
  - отправка на БПЛА команд «снижение» или «отключение питания двигателей», а также других команд, однозначно ведущих к немедленному прекращению полета БПЛА;
  - отправка на БПЛА команд отключения бортовой аппаратуры полезной нагрузки;
  - внедрение в КРУ ложного «виртуального» БПЛА, предоставляющего ПУ такую ложную ТМИ, которая вынуждает ПУ формировать заведомо некорректные команды управления БПЛА, переводящие последний в аэродинамически-неустойчивый режим полета;
- ИТВ основанные на нарушении целостности и доступности ОС или ПО на БПЛА или ПУ:
  - использование стандартных уязвимостей управляющих ОС или ПО для формирования ИТВ на них с целью блокирования нормального режима их функционирования;
  - скрытый перевод аппаратных средств БПЛА в режим повышенного расхода энергии или в аэродинамически-неустойчивый режим полета;
  - внедрение в управляющие ОС или ПО компьютерных вирусов, которые создают условия для нарушения функционирования ОС и ПО или для перехвата управления БПЛА;
  - внедрение в БПЛА программных или аппаратных закладок, реализующих несанкционированные режимы работы или подключение к другому «несанкционированному ПУ» и исполнение его команд с более высоким приоритетом.

В целом при формировании ИТВ на БПЛА, последний рассматривается как стандартная ИС. В этом смысле таргетированная атака на ОС и ПО БПЛА фактически не отличается атаки какой-либо другой удаленной ИС. Основные типы ИТВ характерных для ИС рассмотрены в работе [139]. Примеры таргетированных ИТВ на БПЛА представлены в работах [140-144]. При этом, особенностью ИТВ на БПЛА является то, что формируемые ИТВ должны приводить к максимально быстрому прекращению полета БПЛА к контролируемому рубежу с минимальным ущербом.

Рассматривая вопрос организации ИТВ на БПЛА, необходимо отметь, что несмотря на распространение в популярных СМИ большого числа сообщений об успешном «взломе» БПЛА и перехвате управления ими, создание такой си-

стемы представляется весьма нетривиальной научно-технической задачей. Организация ИТВ на БПЛА требует интеграции средств РРТР и КР в единый комплекс разведки сигнальных, форматных, потоковых и сетевых параметров КРУ, обеспечивающих автоматическое вскрытие и получения данных об ОС и ПО, используемых на БПЛА и на ПУ, в весьма сжатые сроки (в лучшем случае – порядка нескольких десятков секунд, пока БПЛА движется к контролируемому рубежу), основываясь на весьма ограниченном числе перехваченных пакетов из относительно низкоскоростной линии КРУ. Формирование ИТВ потребует интегрирования в единый комплекс средств РЭП и ИТВ, которые бы на основе данных о сигнальных, форматных, потоковых и сетевых параметрах КРУ, БПЛА и ПУ автоматически выбирали сценарии наиболее оптимальных ИТВ и затем в режиме реального времени формировали таргетированные атаки на элементы системы «БПЛА – ПУ», с целью скорейшего прекращения полета БПЛА. Действующие полнофункциональные системы, решающие подобные задачи в режиме реального времени в отношении БПЛА, или хотя бы их проекты, к настоящему времени автору неизвестны.

Вместе с тем, в отдельных проектах систем РЭП для противодействия БПЛА встречаются технические решения, направленные на определение факта использования одного из наиболее распространенных протоколов управления коммерческими малыми БПЛА (MAVlink, SLT.DSM, XBee и др.) и формирование в рамках этого конкретного протокола ложных команд управления БПЛА: «посадки», «снижения» и т.д.

Более реализуемым при решении задачи противодействия малым коммерческим БПЛА выглядит способ разработки специальных программных закладок, внедряемых в управляющую ОС или ПО БПЛА при их сертификации, например, для продажи и применения на территории России. При этом данная программная закладка должна предусматривать прием по стандартным радиоканалам (например, Wi-Fi) и обработку с наивысшем приоритетом специализированных команд запрета полета, которые могут транслироваться «виртуальными ПУ» размещаемыми на рубежах контролируемых зон. Такая мера позволит на 90% однозначно закрыть проблему противодействия коммерческим малым БПЛА в зонах, где их полет запрещен, причем без разработки дорогостоящих средств РЭП с потенциально сомнительной эффективностью.

Заключение

В статье представлены результаты систематизации и анализа различных способов и средств противодействия БПЛА, основанных на радиоэлектронном подавлении систем навигации и радиосвязи БПЛА. В основу систематизации положено более 140 открытых источников, анализ которых позволил вскрыть основные особенности БПЛА, как объекта подавления, а также провести многоаспектный подробный анализ современных комплексов РЭП и их эффективности при работе по воздушным целям такого типа.

Элементом новизны работы являются выявленные общие особенности радиоэлектронного подавления БПЛА, а также системные недостатки используемых технологических решений в существующих комплексах РЭП, а также

применяемых способов подавления, приводящие к снижению их эффективности при применении против БПЛА.

Материал статьи может использоваться для формирования исходных данных для моделирования и исследования эффективности комплексов РЭП при их противодействии БПЛА. Также, данная статья может быть полезна конструкторам, проектирующим системы противодействия БПЛА, а также специалистам при оценке параметров группы БПЛА, гарантированно вскрывающих и преодолевающих зону РЭП противника при решении своих целевых задач.

Автор выражает благодарность доктору технических наук доценту Т.Р. Газизову и кандидату технических наук А.В. Ананьеву за ценные советы и критические замечания, которые в значительной степени способствовали повышению качества статьи на этапе ее подготовки к публикации.

Литература

1. Michel A. H. Counter-drone systems. – Center for the Study of the Drone at Bard College, 2018. – 23 с.

2. Countering rogue drones. – FICCI Committee on Drones, EY, 2018. – 31 с.

3. de Visser E., Cohen M. S., LeGoullon M., Sert O., Freedy A., Freedy E., Weltman G., Parasuraman R. A Design Methodology for Controlling, Monitoring, and Allocating Unmanned Vehicles // Third International Conference on Human Centered Processes (HCP-2008). – 2008. – С. 1-5.

4. Sheu B. H., Chiu C. C., Lu W. T., Huang C. I., Chen W. P. Sheu B. H. et al. Development of UAV Tracing and Coordinate Detection Method Using a Dual-Axis Rotary Platform for an Anti-UAV System // Applied Sciences. 2019. Т. 9. № 13. С. 2583.

5. Kratky M., Minarik V. The non-destructive methods of fight against UAVs // 2017 International Conference on Military Technologies (ICMT). – IEEE, 2017. – С. 690-694.

6. Kim B. H., Khan D., Choi W., Kim M. Y. Real-time counter-UAV system for long distance small drones using double pan-tilt scan laser radar // Preceding SPIE 11005, Laser Radar Technology and Applications XXIV, 110050C (2 May 2019). – 2019. DOI: 10.1117/12.2520110.

7. Gaspar J., Ferreira R., Sebastião P., Souto N. Capture of UAVs Through GPS Spoofing // 2018 Global Wireless Summit (GWS). – IEEE, 2018. – С. 21-26.

8. Müller W., Reinert F., Pallmer D. Open architecture of a counter UAV system // Preceding SPIE 10651, Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation 2018, 1065106 (9 May 2018). – 2018. DOI: 10.1117/12.2305606.

9. Hartmann K., Giles K. UAV exploitation: A new domain for cyber power // 8th International Conference on Cyber Conflict (CyCon). – IEEE, 2016. – С. 205-221.

10. Макаренко С. И., Тимошенко А. В., Васильченко А. С. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 1. Беспилотный летательный аппарат как объект обнаружения и поражения //

Системы управления, связи и безопасности. 2020. № 1. С. 109-146. DOI: 10.24411/2410-9916-2020-10105.

11. Макаренко С. И., Тимошенко А. В. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 2. Огневое поражение и физический перехват // Системы управления, связи и безопасности. 2020. № 1. С. 147-197. DOI: 10.24411/2410-9916-2020-10106.

12. Макаренко С. И. Робототехнические комплексы военного назначения – современное состояние и перспективы развития // Системы управления, связи и безопасности. 2016. № 2. С. 73-132. DOI: 10.24411/2410-9916-2016-10204.

13. Макаренко С. И., Иванов М. С. Сетецентрическая война - принципы, технологии, примеры и перспективы. Монография. – СПб.: Наукоемкие технологии, 2018. – 898 с.

14. Еремин Г. В., Гаврилов А. Д., Назарчук И. И. Малоразмерные беспилотники – новая проблема для ПВО // Отвага [Электронный ресурс]. 29.01.2015. № 6 (14). – URL: http://otvaga2004.ru/armiya-i-vpk/armiya-i-vpk-vzglyad/malorazmernye-bespilotniki/ (дата доступа 16.10.2019).

15. Изделия и комплексы противодействия беспилотным летательным аппаратам [Доклад]. – СПб.: АО «НИИ «Вектор», 2018. – 51 с.

16. Репеллент-1. Комплекс радиоэлектронной борьбы с малоразмерными БЛА // НИИ РЭБ [Электронный ресурс], 2019. – URL: http://www.ntc-reb.ru/repelent.html (дата обращения 14.04.2020).

17. Ловушка для дрона: как вывести из строя беспилотник // Государственная корпорация «Ростех» [Электронный ресурс], 2019. – URL: https://rostec.ru/news/lovushka-dlya-drona-kak-vyvesti-iz-stroya-bespilotnik/?sphrase_id=115590 (дата обращения 14.04.2020).

18. Комплекс радиоэлектронной борьбы с БПЛА «Шиповник-АЭРО» // RuFor.org [Электронный ресурс], 18.06.2015. – URL: https://rufor.org/showthread.php?t=29323 (дата обращения 14.04.2020).

19. Станция постановки помех Р-330Ж «Житель» // Военное обозрение [Электронный ресурс], 26.07.2016. – URL: https://topwar.ru/98467-stanciya-postanovki-pomeh-r-330zh-zhitel.html (дата обращения 14.04.2020).

20. Бойко А. Системы обнаружения и нейтрализации беспилотников // RoboTrends [Электронный ресурс], 2019. – URL: http://robotrends.ru/robopedia/sistemy-obnaruzheniya-i-nyaytralizacii-bespilotnikov (дата обращения 14.04.2020).

21. Демьянович М. А. Использование беспилотных летательных аппаратов в преступных целях: методы противодействия и борьбы // Правопорядок: история, теория, практика. 2019. № 2 (21). С. 108-112.

22. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. – СПб.: Наукоемкие технологии, 2017. – 546 с.

23. Оружие и технологии России. Энциклопедия. XXI век. Системы управления, связи и радиоэлектронной борьбы / Под общ. ред. С. Иванова. – М.: Изд. дом «Оружие и технологии», 2006. – 695 с.

24. Ясечко М. Н., Очкуренко А. В., Ковальчук А. А., Максюта Д. В. Современные радиотехнические средства борьбы с беспилотными летательными аппаратами в зоне проведения АТО // Збірник наукових праць Харківського університету Повітряних Сил. 2015. № 3 (44). С. 54-57.

25. Аниськов Р. В., Архипова Е. В., Гордеев А. А., Пугачев А. Н. К вопросу борьбы с незаконным использованием беспилотных летательных аппаратов коммерческого типа // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2017. № 9-10 (111-112). С. 71-75.

26. Бойко А. Blighter AUDS // RoboTrends [Электронный ресурс], 2015. – URL: http://robotrends.ru/pub/1542/bespilotnik-v-polete-ostanovit-blighter-auds (дата обращения 14.04.2020).

27. Федоров Е. Война с дронами. Саудовский голиаф против хуситов // Военное обозрение [Электронный ресурс]. 28.09.2019. – URL: https://topwar.ru/162842-vojna-s-dronami-saudovskij-goliaf-protiv-husitov.html (дата обращения 14.04.2020).

28. Какие существуют дроны и на каких частотах они работают? // Podavitel.ru [Электронный ресурс], 2020. – URL: http://www.podavitel.ru/na-kakikh-chastotakh-rabotayut-kvadrokoptery-i-drony.html (дата обращения 14.04.2020).

29. Подавитель сотовой связи Monster 16CH // n-sb.ru [Электронный ресурс], 2020. – URL: http://sankt-peterburg.n-sb.ru/podaviteli-gsm-signala.php (дата обращения 14.04.2020).

30. Частоты передачи данных // Podavitel.ru [Электронный ресурс], 2020. – URL: http://www.podavitel.ru/chastoty-peredachi-dannykh.html (дата обращения 14.04.2020).

31. Бочмага Д. А., Шимон Н. С., Калач А. В., Калач Е. В., Урусова Т. Е. Проблемы противодействия БПЛА в учреждениях ФСИН России // Пожарная безопасность: проблемы и перспективы. 2018. Т. 1. № 9. С. 89-91.

32. Охота на беспилотник: как военные борются с гражданской угрозой с воздуха // Военное.рф [Электронный ресурс], 11.11.2018. – URL: https://военное.рф/2018/%D0%91%D0%BF%D0%BB%D0%B029/ (дата доступа 20.12.2019).

33. Веремеенко К. К., Кошелев Б.В., Соловьев Ю. А. Анализ состояния разработок интегрированных инерциально-спутниковых навигационных систем // Новости навигации. 2010. № 4. С. 32-41.

34. Семенова Л. Л. Современные методы навигации беспилотных летательных аппаратов // Наука и образование сегодня. 2018. № 4 (27). С. 6-8.

35. Щербинин В. В., Свиязов А. В., Смирнов С. В., Кветкин Г. А. Автономный навигационный комплекс для роботизированных наземных и летательных аппаратов // Известия Южного федерального университета. Технические науки. 2014. № 3 (152). С. 234-243.

36. ГЛОНАСС. Принципы построения и функционирования / Под ред. А.И. Перова, В.Н. Харисова. – М.: Радиотехника, 2010. – 800 с.

37. Яценков В. С. Основы спутниковой навигации. Системы GPS NAVSTAR и ГЛОНАСС. – М.: Горячая линия – Телеком, 2005. – 272 с.

38. Филиппов А. А., Бажин Д. А., Хлобыстов А. Н. Повышение эффективности управления беспилотного летательного аппарата в условиях помех // Информационно-управляющие системы. 2014. № 6 (73). С. 45-50 – URL: https://cyberleninka.ru/article/n/povyshenie-effektivnosti-upravleniya-bespilotnogo-letatelnogo-apparata-v-usloviyah-pomeh (дата обращения: 16.04.2020).

39. Гришин В. А. Системы технического зрения в решении задач управления беспилотными летательными аппаратами // Датчики и системы. 2009. № 2. С. 46-52.

40. Югай Е. Б. Способ и система навигации пассажирского дрона в горной местности // Патент на изобретение RU 2681278 C1, 05.03.2019.

41. Корнеев М. А., Максимов А. Н., Максимов Н. А. Методы выделения точек привязки для визуальной навигации беспилотных летательных аппаратов // Труды МАИ. 2012. № 58. С. 6. – URL: https://mai.ru/upload/iblock/086/metody-vydeleniya-tochek-privyazki-dlya-vizualnoy-navigatsii-bespilotnykh-letatelnykh-apparatov.pdf (дата обращения 14.04.2020).

42. Степанов Д. Н., Тищенко И. П. Задача моделирования полета беспилотного летательного аппарата на основе системы технического зрения // Программные системы: теория и приложения. 2011. № 4. С. 33-43. – URL: https://cyberleninka.ru/article/n/zadacha-modelirovaniya-poleta-bespilotnogo-letatelnogo-apparata-na-osnove-sistemy-tehnicheskogo-zreniya (дата обращения: 14.04.2020).

43. Дятлов А. П., Дятлов П. А., Кульбикаян Б. Х. Радиоэлектронная борьба со спутниковыми радионавигационными системами. Монография. – М.: Радио и связь, 2004. – 226 с.

44. Камнев Е. А. Радиоподавление помехозащищенной навигационной аппаратуры потребителей спутниковых радионавигационных систем в интересах объектово-территориальной защиты. Дис. … канд. техн. наук по спец. 05.12.14 «Радиолокация и радионавигация». – М.: МАИ (НИУ), 2018. – 160 с.

45. Жук А. П., Орел Д. В. Об оценке помехозащищенности спутниковых радионавигационных систем // Инфокоммуникационные технологии. 2012. Т. 10. № 2. С. 83-88.

46. Казаков А. Е., Водяных А. А. Пути повышения помехозащищенности навигационной аппаратуры потребителей спутниковых навигационных систем // Системи обробки інформації. 2007. № 1 (59). С. 48-51.

47. Кащеев А. А., Кошелев В. И. Оценка эффективности подавления сигналов спутниковых радионавигационных систем преднамеренными помехами // Журнал радиоэлектроники. 2012. № 7. С. 1. – URL: http://jre.cplire.ru/koi/jul12/3/text.pdf (дата обращения: 14.04.2020).

48. Юдин В. Н., Камнев Е. А. Принципы создания противонавигационного поля радиопомех // Труды МАИ. 2015. № 83. С. 28. – URL:

https://mai.ru/upload/iblock/8cb/yudin_kamnev_rus.pdfhttps://mai.ru/upload/iblock/8cb/yudin_kamnev_rus.pdf (дата обращения: 14.04.2020).

49. Абукраа А. С., Вилькоцкий М. А., Лыньков Л. М. Влияние на помехоустойчивость и точность абонентских приемников спутниковых навигаторов близкорасположенных экранов с учетом условий распространения радиоволн на реальной местности // Доклады БГУИР. 2017. № 3 (105). С. 85-92.

50. Тяпкин В. Н., Дмитриев Д. Д., Мошкина Т .Г. Потенциальная помехоустойчивость навигационной аппаратуры потребителей спутниковых радионавигационных систем // Вестник Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева. 2012. № 3. (43). С. 113-119.

51. Дмитриев Д. Д. Исследование помехоустойчивости аппаратуры радионавигации // Современные проблемы развития науки, техники и образования. – Красноярск: ИПК СФУ, 2009. – С. 202-209.

52. Тяпкин В. Н., Гарин Е. Н. Методы определения навигационных параметров подвижных средств с использованием спутниковой радионавигационной системы ГЛОНАСС. Монография. – Красноярск: Сибирский федеральный университет, 2012. – 260 с.

53. Пантенков Д. Г. Результаты математического моделирования помехоустойчивости спутниковых радионавигационных систем при воздействии преднамеренных помех // Успехи современной радиоэлектроники. 2020. № 2. С. 57-68.

54. Журавлев А. В., Безмага В. М., Красов Е. М., Смолин А. В., Шуваев В. А., Маркин В. Г. Устройство для пространственной селекции сигналов навигационных космических аппаратов с использованием пеленгования источников радиопомех // Патент RU 2 619 800 C1 от 18.05.2017.

55. Гэн К., Чулин Н. А. Интегрированная навигационная система для беспилотных летательных аппаратов с возможностью обнаружения и изоляции неисправностей // Машиностроение и компьютерные технологии. 2016. № 12. С. 182-206.

56. Беркович С. Б., Грибунин В. Г., Котов Н. И., Мартынюк Г. А., Махаев А. Ю., Смирнов Д. В., Шолохов А. В., Лапшина А. А. Оценка эффективности вариантов построения навигационных систем робототехнических комплексов // Известия Тульского государственного университета. Технические науки. 2016. № 11-3. С. 19-38.

57. Доронин Д. В., Донченко А. А., Шевцов С. Н. Функционирование математической модели ошибок бесплатформенной инерциальной навигационной системы при одновременной навигации, динамическом построении и обработки данных многоструктурных систем управления в рамках разработки алгоритмов интегрированной системы навигации летательного аппарата с использованием GPS/ГЛОНАСС технологий // Известия Самарского научного центра Российской академии наук. 2012. Т. 14. № 4 (5). С. 1363-1367.

58. Марюхненко В. С., Ерохин В. В. Структурный синтез навигационного обеспечения триадной интегрированной системы навигации на основе

инерциальных и спутниковых технологий // Научный вестник Московского государственного технического университета гражданской авиации. 2017. Т. 20. № 4. С. 69-77. DOI: 10.26467/2079-0619-2017-20-4-69-77.

59. Рубцов В. Д., Заикин А. А. Сравнительный анализ эффективности различных вариантов комплексной обработки информации в аппаратуре потребителей спутниковых радионавигационных систем и инерциальной навигационной системе // Научный вестник Московского государственного технического университета гражданской авиации. 2010. № 159. С. 128-132.

60. Усов О. С., Хорошко А. Ю., Кванин Л. В. Лазерный высотомер для беспилотных летательных аппаратов вертолетного типа средней и большой дальности (ЛВ-50) // Секрет производства («ноу-хау») № 218.016.804d от 28.08.2018. – URL: https://edrid.ru/rid/218.016.804d.html (дата обращения: 17.04.2020).

61. Фокин Г. А. Позиционирование в условиях отсутствия прямой видимости с использованием цифровых моделей местности // T-Comm: Телекоммуникации и транспорт. 2019. Том 13. № 11. С. 4-13. DOI: 10.24411/2072-8735-2018-10319.

62. Егурнов В. О., Ильин В. В., Некрасов М. И., Сосунов В. Г. Анализ способов противодействия беспилотным летательным аппаратам для обеспечения безопасности защищаемых объектов // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2018. № 1-2 (115-116). С. 51-58.

63. Vaas L. Sound: Yet another way to smack down drones // Naked Security by Sophos [Электронный ресурс]. 06.08.2015. – URL: nakedsecurity.sophos.com/2015/08/06/sound-yet-another-way-to-smack-down-drones/ (дата обращения: 10.04.2020).

64. Верба В. С. Авиационные комплексы радиолокационного дозора и наведения. Принципы построения, проблемы разработки и особенности функционирования. Монография. – М.: Радиотехника, 2014. – 528 с.

65. Верба В. С., Меркулов В. И. Теоретические и прикладные проблемы разработки систем радиоуправления нового поколения // Радиотехника. 2014. № 5. С. 39-44.

66. Верба В. С., Меркулов В. И., Самодов И. О. Управление беспилотными летательными аппаратами в составе локальной сети // Информационно-измерительные и управляющие системы. 2014. Т. 12. № 3. С. 7-12.

67. Верба В. С., Меркулов В. И., Миляков Д. А. Проблемы управления большими плотными группами беспилотных летательных аппаратов // Информационно-измерительные и управляющие системы. 2018. Т. 16. № 6. С. 3-13.

68. Меркулов В. Н., Дрогалин В. В., Канащенков А. Н., Лепин В. Н., Самарин О. Ф., Соловьев А. А. Авиационные системы радиоуправления. Том 1. Принципы построения систем радиоуправлсния. Основы синтеза и анализа / Под ред. А.И. Канащенкова и В.И. Меркулова. – М.: Радиотехника, 2003. – 192 с.

69. Белов С. Г., Крайлюк А. Д., Меркулов В. И., Чернов В. С. Информационные системы беспилотных комплексов стратегической и

оперативной воздушной разведки США // Успехи современной радиоэлектроники. 2020. № 1. С. 28-42.

70. Боев Н. М. Анализ командно-телеметрической радиолинии связи с беспилотными летательными аппаратами // Вестник Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева. 2012. № 2 (42). С. 86-91.

71. Боев Н. М., Шаршавин П. В., Нигруца И. В. Построение систем связи беспилотных летательных аппаратов для передачи информации на большие расстояния // Известия ЮФУ. Технические науки. 2014. № 3 (152). С. 147-158.

72. Боев Н. М., Лебедев Ю. А. Управление энергетической эффективностью совмещенных каналов передачи данных единой системы связи // Вестник Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева. 2013. № 1 (47). С. 11-15.

73. Боев Н. М. Способы повышения энергетической и спектральной эффективности цифровых систем связи беспилотных летательных аппаратов // Труды Московского физико-технического института. 2014. Т. 6. № 2 (22). С. 162-166.

74. Боев Н. М. Разработка и проектирование бортового антенно-фидерного оборудования малых беспилотных летательных аппаратов // Решетневские чтения. 2011. Т. 1. С. 162-163.

75. Батурин Т. Н., Боев Н. М. Разработка и проектирование бортового усилителя мощности радиосигнала УКВ-диапазона для беспилотного летательного аппарата // Решетневские чтения. 2012. Т. 1. С. 141-142.

76. Лебедев Ю. А., Боев Н. М. Разработка и проектирование малогабаритной системы связи малых беспилотных летательных аппаратов // Решетневские чтения. 2012. Т. 1. С. 155-156.

77. Слюсар В. И. Передача данных с борта БПЛА: Стандарты НАТО // Электроника: Наука, технология, бизнес. 2010. № 3 (101). С. 80-87.

78. Слюсар В. И. Радиолинии связи с БПЛА. Примеры реализации // Электроника: Наука, технология, бизнес. 2010. № 5 (103). С. 56-61.

79. Ананьев А. В., Стафеев М. А., Макеев Е. В. Апробация способа организации связи с использованием беспилотных летательных аппаратов // Труды МАИ. 2019. № 105. С. 14.

80. Ананьев А. В., Катруша А. Н. Контурная антенна ДКМВ-диапазона для беспилотных летательных аппаратов // Антенны. 2017. № 8 (240). С. 45-52.

81. Ананьев А. В., Ерзин И. Х., Щербаков А. А., Филатов С. В. Аэромобильная сеть связи - эффективная система ретрансляции объединенной автоматизированной цифровой системы связи // Военная мысль. 2017. № 4. С. 26-34.

82. Ананьев А. В., Катруша А. Н. Сравнительная оценка возможностей радиосвязи с беспилотными летательными аппаратами в диапазонах КВ и УКВ для полузакрытых и закрытых трасс распространения радиоволн // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 10. С. 4-9.

83. Ананьев А. В., Стафеев М. А., Филатов С. В. Оценка эффективности систем связи и боевого управления на базе беспилотных летательных аппаратов

межвидовой группировки войск // Воздушно-космические силы. Теория и практика. 2017. № 3 (3). С. 75-84.

84. Ананьев А. В., Змий Б. Ф., Кащенко Г. А. Модернизация бортовых приемо-передающих систем беспилотных летательных аппаратов на основе эволюционного подхода // Радиотехника. 2016. № 8. С. 46-49.

85. Пантенков Д. Г., Ломакин А. А. Оценка устойчивости спутникового канала управления беспилотными летательными аппаратами при воздействии преднамеренных помех // Радиотехника. 2019. Т. 83. № 11 (17). С. 43-50.

86. Долженков Н. Н., Пантенков Д. Г., Литвиненко В. П., Ломакин А. А., Егоров А. Т., Гриценко А. А. Интегрированный комплекс дальней радиосвязи для повышения эффективности решения целевых задач беспилотными летательными аппаратами // Вестник Воронежского государственного технического университета. 2019. Т. 15. № 3. С. 102-108. DOI: 10.25987/VSTU.2019.15.3.015.

87. Долженков Н. Н., Пантенков Д. Г., Егоров А. Т., Ломакин А. А., Литвиненко В. П., Великоиваненко В. И., Лю-Кэ-Сю Е. Ю. Технические характеристики комплекса средств спутниковой радиосвязи с беспилотными летательными аппаратами // Вестник Воронежского государственного технического университета. 2019. Т. 15. № 3. С. 74-82. DOI: 10.25987/VSTU.2019.15.3.011.

88. Пантенков Д. Г., Гусаков Н. В., Егоров А. Т., Ломакин А. А., Литвиненко В. П., Великоиваненко В. И., Лю-Кэ-Сю Е. Ю. Техническая реализация высокоскоростного информационного канала радиосвязи с беспилотного летательного аппарата на наземный пункт управления // Вестник Воронежского государственного технического университета. 2019. Т. 15. № 3. С. 52-71. DOI: 10.25987/VSTU.2019.15.5.007.

89. Киричек Р. В. Разработка и исследование комплекса моделей и методов для летающих сенсорных сетей. Диссертация на соискание ученой степени доктора технических наук по специальности 05.12.13. – СПб.: СПбГУТ им. проф. М.А. Бонч-Бруевича, 2018. – 276 с.

90. Самойленко Д. В., Финько О. А., Еремеев М. А. Распределённая обработка и защита информации в группировке комплексов с беспилотными летательными аппаратами // Теория и техника радиосвязи. 2017. № 4. С. 93-100.

91. Самойленко Д. В., Финько О. А. Обеспечение целостности информации в группе беспилотных летательных аппаратов в условиях деструктивных воздействий нарушителя // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2017. № 5-6 (107-108). С. 20-27.

92. Самойленко Д. В., Финько О. А. Помехоустойчивая передача данных в радиоканалах робототехнических комплексов на основе полиномиальных классов вычетов // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8. № 3. С. 49-55.

93. Дворников С. В., Дворников С. С., Морозов Е. В. Модель взаимодействия радиотехнических систем беспилотных аппаратов // Вопросы радиоэлектроники. Серия: Техника телевидения. 2020. № 1. С. 84-90.

94. Дворников С. В., Погорелов А. А., Дворников С. С., Иванов Р. В. Предложения по восстановлению сигналов в каналах управления беспилотных летательных аппаратов // Вопросы радиоэлектроники. Серия: Техника телевидения. 2020. № 1. С. 91-97.

95. Дворников С. В. Методика оценки имитоустойчивости каналов управления роботизированных устройств // Радиопромышленность. 2016. № 2. С. 64-69.

96. Донченко А. А., Нехорошев Г. В., Штефан В. И. Технология построения высокоскоростных энергоскрытных каналов передачи команд управления, видео и телеметрии группировки робототехнических комплексов специального назначения // Роботизация вооружённых сил Российской Федерации. Сборник статей конференции. – Анапа: Военный инновационный технополис «ЭРА», 2019. – С. 174-179.

97. Донченко А. А., Чиров Д. С. Обоснование требований к системе связи беспилотных летательных аппаратов средней и большой дальности // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 12. С. 12-16.

98. Чиров Д. С., Лобов Е. М. Выбор сигнально-кодовой конструкции для командно-телеметрической линии радиосвязи с беспилотными летательными аппаратами средней и большой дальности // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 10. С. 21-28.

99. Чертова О. Г., Чиров Д. С. Построение опорной сети связи на базе малоразмерных беспилотных летательных аппаратов с отсутствием наземной инфраструктуры // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 3. С. 60-71. DOI: 10.24411/2409-5419-2018-10269.

100. Бородин В. В., Петраков А. М., Шевцов В. А. Анализ алгоритмов маршрутизации в сети связи группировки беспилотных летательных аппаратов // Труды МАИ. 2016. № 87. С. 16.

101. Бородин В. В., Петраков А. М., Шевцов В. А. Анализ эффективности передачи данных в сети связи группировки беспилотных летательных аппаратов // Труды МАИ. 2015. № 81. С. 27.

102. Назаров Л. Е., Игошин Е. В., Зудилин А. С., Щеглов М. А. Разработка, реализация и испытания сигнально-кодовых конструкций для высокоскоростной радиолинии связи с БПЛА // Успехи современной радиоэлектроники. 2014. № 8. С. 68-74.

103. Паршин Ю. Н., Кудряшов В. И. Анализ пропускной способности канала передачи информации от беспилотного летательного аппарата при неточной канальной матрице // Вестник Рязанского государственного радиотехнического университета. 2015. № 52. С. 22-27.

104. Сивов А. Ю. Алешин М. Г. Обоснование основных параметров антенной системы ретранслятора связи на беспилотном летательном аппарате // Техника радиосвязи. 2011. № 16. С. 43-54.

105. Крыжевич Л. С., Сизов А. С. Обзор состояния проблемы передачи растровых изображений с беспилотных летательных средств // Известия Юго-Западного государственного университета. 2012. № 6 (45). С. 54-60.

106. Макаров И. В. Оценка пропускной способности системы связи беспилотного летательного аппарата для решения задач управления // Радиотехника. 2013. № 4. С. 40-45.

107. Фокин Г. А. Обзор моделей радиоканала связи с беспилотными летательными аппаратами // Труды учебных заведений связи. 2018. Т. 4. № 4. С. 85-101. DOI: 10.31854/1813-324X-20184-4-85-101.

108. Смородинов А. А. Как выбрать широкополосный модем для беспилотного летательного аппарата (БЛА) или робототехники // Habr.com [Электронный ресурс]. 22.03.2019. – URL: https://habr.com/ru/post/444898/ (дата обращения 14.04.2020).

109. Михайлов Р.Л. Описательные модели систем спутниковой связи как космического эшелона телекоммуникационных систем специального назначения. Монография. – СПб.: Наукоемкие технологии, 2019. – 150 с.

110. Добыкин В. Д., Куприянов А. И., Пономарев В. Г., Шустов Л. Н. Радиоэлектронная борьба. Цифровое запоминание и воспроизведение радиосигналов и электромагнитных волн. – М.: Вузовская книга, 2009. – 360 с.

111. Харкевич А. А. Борьба с помехами. 5-е изд. – М.: Либроком, 2018. – 280 с.

112. Палий А. И. Радиоэлектронная борьба. – М.: Военное издательство, 1989. – 350 с.

113. Комашинский В. И. Максимов А. В. Системы подвижной радиосвязи с пакетной передачей информации: основы моделирования. – М.: Горячая линия – Телеком, 2007. – 176 с.

114. Борисов В. А., Калмыков В. В., Ковальчук Я. М., Себекин Ю. Н., Сенин А. И., Федоров И. Б., Цикин И. А. Радиотехнические системы передачи информации: Учебное пособие для вузов / под ред. В.В. Калмыкова. – М.: Радио и связь, 1990. – 304 с.

115. Маслов П. В. Сравнительный анализ методов цифровой модуляции // Молодежный научно-технический вестник. 2013. № 2. С. 46.

116. Песков С. Н., Ищенко А. Е. Расчет вероятности ошибки в цифровых каналах связи // Телеспутник. 2010. № 11. С. 70-75.

117. Иванов Ю. А., Невструев И. А. Структура и помехоустойчивость систем беспроводного доступа с OFDM // Электротехнические и информационные комплексы и системы. 2009. Т. 5. № 3. С. 25-29.

118. Пантенков Д. Г., Гусаков Н. В., Соколов В. М., Великоиваненко В. И., Константинов В. С. Комплекс методик оценки эффективности решения частных целевых задач военного времени космическим аппаратом многоцелевой космической системы // Актуальные вопросы проектирования космических систем и комплексов. Сборник научных трудов аспирантов и соискателей ученых степеней. Выпуск 15. – Химки: НПО им. С.А. Лавочкина, 2014. – С.107-150.

119. Пантенков Д. Г., Гусаков Н. В., Соколов В. М., Великоиваненко В. И., Ломакин А. А. Комплекс методик оценки эффективности решения частных целевых задач мирного времени космическим аппаратом многоцелевой космической системы // Актуальные вопросы проектирования космических

систем и комплексов. Сборник научных трудов аспирантов и соискателей ученых степеней. Выпуск 15. – Химки: НПО им. С.А. Лавочкина, 2014. – С. 89-106.

120. Красносельский И. Н., Канев С. А. Исследование помехоустойчивости системы DVB-T на модели канала с многолучевым распространением // Электросвязь. 2010. № 7. С. 28-30.

121. European Standard (Telecommunications series) ETSI EN 300 744 V1.6.1. – Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television. 2009. – URL: http://www.etsi.org (дата доступа 12.04.2019).

122. Варакин Л. Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с.

123. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. СПб.: – Свое издательство, 2013. – 166 с.

124. JSC-CR-10-004. Communications Receiver Performance Degradation Handbook. – Annapolis: Joint Spectrum Center, 2010. – 306 с.

125. Ерохин Г. А., Мандель В. И., Нестёркин Ю. А., Струков А. П. Методика расчета энергетического запаса радиолинии "космический аппарат - станция" // Ракетно-космическое приборостроение и информационные системы. 2018. Т. 5. № 1. С. 65-74.

126. Полынкин А. В., Ле Х. Т. Исследование характеристик радиоканала связи с беспилотными летательными аппаратами // Известия Тульского государственного университета. Технические науки. 2013. № 7-2. С. 98-107.

127. Зикратов И. А., Зикратова Т. В., Лебедев И. С., Гуртов А. В. Построение модели доверия и репутации к объектам мультиагентных робототехнических систем с децентрализованным управлением // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 3 (91). С. 30-38.

128. Зикратов И. А., Зикратова Т. В., Лебедев И. С. Доверительная модель информационной безопасности мультиагентных робототехнических систем с децентрализованным управлением // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 2 (90). С. 47-52.

129. Викснин И. И., Мариненков Е. Д. Противодействие скрытому деструктивному воздействию в роях беспилотных летательных аппаратов // International Journal of Open Information Technologies. 2018. Т. 6. № 12. С. 1-11.

130. Винокуров А. В. Анализ уязвимостей комплексов с беспилотными летательными аппаратами и классификация угроз безопасности циркулирующей в них информации // I-Methods. 2016. № 1. С. 5-9.

131. Макаренко С. И. Вычислительные системы, сети и телекоммуникации: учебное пособие. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2008. – 352 с.

132. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.

133. Нефёдова М. Множественные уязвимости в 4G LTE позволяют следить за абонентами и подделывать данные // Хакер [Электронные ресурс]. 07.03.2018. – URL: https://xakep.ru/2018/03/07/lteinspector/ (дата доступа 20.12.2019).

134. Перегудов М. А., Семченко И. А. Оценка эффективности случайного множественного доступа к среде типа ALOHA при голосовых соединениях, передаче служебных команд, текстовых сообщений и мультимедийных файлов в условиях деструктивных воздействий // Труды СПИИРАН. 2019. Т. 18. № 4. С. 887-911. DOI: 10.15622/sp.2019.18.4.887-911.

135. Перегудов М. А., Стешковой А. С., Бойко А. А. Вероятностная модель процедуры случайного множественного доступа к среде типа CSMA/CA // Труды СПИИРАН. 2018. № 4 (59). С. 92-114. DOI: 10.15622/sp.59.4.

136. Перегудов М. А., Бойко А. А. Модель процедуры случайного множественного доступа к среде типа S-Aloha // Информационно-управляющие системы. 2014. № 6 (73). С. 75-81.

137. Макаренко С. И. Оценка качества обслуживания пакетной радиосети в нестационарном режиме в условиях воздействия внешних дестабилизирующих факторов // Журнал радиоэлектроники. 2012. № 6. С. 2. – URL: http://jre.cplire.ru/jre/jun12/9/text.pdf (дата доступа 20.04.2020).

138. Макаренко С. И. Подавление пакетных радиосетей со случайным множественным доступом за счет дестабилизации их состояния // Журнал радиоэлектроники. 2011. № 9. С. 2. – URL: http://jre.cplire.ru/jre/sep11/4/text.pdf (дата доступа 20.04.2020).

139. Макаренко С. И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. 2016. № 3. С. 292-376. DOI: 10.24411/2410-9916-2016-10311.

140. Холмогоров В. Угнать дрон. Методы перехвата управления коптерами // Хакер [Электронный ресурс]. 24.06.2019. – URL: https://xakep.ru/2019/06/24/dron-interception/ (дата доступа 20.04.2020).

141. Khan A. Hacking the Drones // Open Web Application Security Project [Электронный ресурс]. 2016. – URL: https://owasp.org/www-chapter-london/assets/slides/OWASP201604_Drones.pdf (дата доступа 20.04.2020).

142. Rodday N. Hacking a Professional Drone // Black Hat Asia 2016 [Электронный ресурс]. 2016. – URL: https://www.blackhat.com/docs/asia-16/materials/asia-16-Rodday-Hacking-A-Professional-Drone.pdf (дата доступа 20.04.2020).

143. Petrovsky O. Attack on the drones: security vulnerabilities of unmanned aerial vehicles // 25th Virus Bulletin International Conference [Электронный ресурс]. 2015. – URL: https://www.virusbulletin.com/conference/vb2015/abstracts/attack-drones-security-vulnerabilities-unmanned-aerial-vehicles (дата доступа 20.04.2020).

144. Here’s how easy it is to hack a drone and crash it // Futurity [Электронный ресурс]. 08.06.2016. – URL: https://www.futurity.org/drones-hackers-security-1179402-2/ (дата доступа 20.04.2020).

145. Казаков Л. Н., Исмаилов А., Кукушкин Д. С. Оценка эффективности применения OFDM-технологий в высокоскоростных системах авиационной связи // Системы синхронизации, формирования и обработки сигналов. 2013. Т. 4. № 3. С. 146-149.

146. Казаков Л. Н., Селянская Е. А., Соловьев Д. М., Ботов В. А. Организация энергетически скрытных радиоканалов для передачи данных и команд управления беспилотными летательными аппаратами // Системы синхронизации, формирования и обработки сигналов. 2017. Т. 8. № 4. С. 91-93.

147. Казаков Л. Н., Царев А. Б., Соловьев Н. В., Махов М. И. Разработка OCDM системы для организации информационного обмена группы БПЛА // Системы синхронизации, формирования и обработки сигналов. 2018. Т. 9. № 4. С. 51-56.

148. Самойленко Д. В. Повышение информационной живучести группировки робототехнических комплексов в условиях деструктивных воздействий злоумышленника // Автоматизация процессов управления. 2018. № 2 (52). С. 4-13.

149. Wang H., Zhao H., Zhang J., Ma D., Li J., Wei J. Survey on unmanned aerial vehicle networks: A cyber physical system perspective // IEEE Communications Surveys & Tutorials. 2019. Т. 22. № 2. С. 1027-1070. DOI: 10.1109/COMST.2019.2962207.

References

1. Michel A. H. *Counter-drone systems*. Center for the Study of the Drone at Bard College, 2018. 23 p.

2. *Countering rogue drones*. FICCI Committee on Drones, EY, 2018. 31 p.

3. de Visser E., Cohen M. S., LeGoullon M., Sert O., Freedy A., Freedy E., Weltman G., Parasuraman R. A Design Methodology for Controlling, Monitoring, and Allocating Unmanned Vehicles. *Third International Conference on Human Centered Processes (HCP-2008)*, 2008, pp. 1-5.

4. Sheu B. H., Chiu C. C., Lu W. T., Huang C. I., Chen W. P. Sheu B. H. et al. Development of UAV Tracing and Coordinate Detection Method Using a Dual-Axis Rotary Platform for an Anti-UAV System. *Applied Sciences*, 2019, vol. 9, no. 13, pp. 2583.

5. Kratky M., Minarik V. The non-destructive methods of fight against UAVs. *2017 International Conference on Military Technologies (ICMT)*. IEEE, 2017, pp. 690-694.

6. Kim B. H., Khan D., Choi W., Kim M. Y. Real-time counter-UAV system for long distance small drones using double pan-tilt scan laser radar. *Preceding SPIE 11005, Laser Radar Technology and Applications XXIV, 110050C (2 May 2019)*, 2019. DOI: 10.1117/12.2520110.

7. Gaspar J., Ferreira R., Sebastião P., Souto N. Capture of UAVs Through GPS Spoofing. *2018 Global Wireless Summit (GWS)*, IEEE, 2018, pp. 21-26.

8. Müller W., Reinert F., Pallmer D. Open architecture of a counter UAV system. *Preceding SPIE 10651, Open Architecture/Open Business Model Net-Centric*

Systems and Defense Transformation 2018, 1065106 (9 May 2018). 2018. DOI: 10.1117/12.2305606.

9. Hartmann K., Giles K. UAV exploitation: A new domain for cyber power. *8th International Conference on Cyber Conflict (CyCon)*. IEEE, 2016. pp. 205-221.

10. Makarenko S. I., Timoshenko A. V., Vasilchenko A. S. Counter Unmanned Aerial Vehicles. Part 1. Unmanned aerial vehicle as an object of detection and destruction. *Systems of Control, Communication and Security*, 2020, no. 1, pp. 109-146 (in Russian). DOI: 10.24411/2410-9916-2020-10105.

11. Makarenko S. I., Timoshenko A. V. Counter Unmanned Aerial Vehicles. Part 2. Rocket and Artillery Fire, Physical Interception. *Systems of Control, Communication and Security*, 2020, no. 1, pp. 147-197 (in Russian). DOI: 10.24411/2410-9916-2020-10106.

12. Makarenko S. I. Military Robots - the Current State and Prospects of Improvement. *Systems of Control, Communication and Security*, 2016, no. 2, pp. 73-132 (in Russian). DOI: 10.24411/2410-9916-2016-10204.

13. Makarenko S. I., Ivanov M. S. *Setecentricheskaya vojna - principy, tekhnologii, primery i perspektivy. Monografiya* [*Network-centric warfare - principles, technologies, examples and perspectives. Monograph*]. Saint Petersburg, Naukoemkie Tekhnologii Publ., 2018. – 898 p. (in Russian).

14. Eremin G. V., Gavrilov A. D., Nazarchuk I. I. Malorazmernye bespilotniki – novaya problema dlya PVO [Small-sized drones – a new problem for air defense]. *Otvaga* [*Courage*], 2015, no. 6 (14). Available at: http://otvaga2004.ru/armiya-i-vpk/armiya-i-vpk-vzglyad/malorazmernye-bespilotniki/ (accessed 16 October 2019) (in Russian).

15. *Izdeliya i kompleksy protivodejstviya bespilotnym letatel'nym apparatam* [*Products and systems for countering unmanned aerial vehicles*]. Saint Petersburg, "Vector" research Institute, 2018. 51 p. (in Russian).

16. Repellent-1. Kompleks radiojelektronnoj bor'by s malorazmernymi BLA [Repellent-1. Complex of electronic warfare with small-sized UAVs]. *Scientific and technical center of electronic warfare*, 2019. Available at: http://www.ntc-reb.ru/repelent.html (accessed 14 May 2020) (in Russian).

17. Lovushka dlja drona: kak vyvesti iz stroja bespilotnik [A drone trap: how to disable a drone]. *Rostec State Corporation*, 2019. Available at: https://rostec.ru/news/lovushka-dlya-drona-kak-vyvesti-iz-stroya-bespilotnik/?sphrase_id=115590 (accessed 14 May 2020) (in Russian).

18. Kompleks radiojelektronnoj bor'by s BPLA "Shipovnik-AJeRO" [Complex of electronic warfare with UAV "Rosehip-AERO"]. *RuFor.org*, 18.06.2015. Available at: https://rufor.org/showthread.php?t=29323 (accessed 14 May 2020) (in Russian).

19. Stancija postanovki pomeh R-330Zh "Zhitel" [Jamming station R-330ZH "Resident"]. *Voennoe obozrenie*, 26.07.2016. Available at: https://topwar.ru/98467-stanciya-postanovki-pomeh-r-330zh-zhitel.html (accessed 14 May 2020) (in Russian).

20. Boyko A. Sistemy obnaruzhenija i nejtralizacii bespilotnikov [UAV detection and neutralization systems]. *RoboTrends*, 2019. Available at:

http://robotrends.ru/robopedia/sistemy-obnaruzheniya-i-nyaytralizacii-bespilotnikov (accessed 14 May 2020).

21. Demyanovich M. A. Use of unmanned aerial vehicles in criminal intents: methods of counteraction and fight. *Legal order: history, theory, practice*, 2019, no. 2 (21), pp. 108-112 (in Russian).

22. Makarenko S. I. *Informatsionnoe protivoborstvo i radioelektronnaia borba v setetsentricheskikh voinakh nachala XXI veka. Monografiia* [Information warfare and electronic warfare to network-centric wars of the early XXI century. Monograph]. Saint Petersburg, Naukoemkie Tekhnologii Publ., 2017. 546 p. (in Russian).

23. Ivanov S. *Oruzhie i tekhnologii Rossii. Entsiklopediia. XXI vek. Sistemy upravleniia, sviazi i radioelektronnoi bor'by* [Weapons and Technology of Russia. The Encyclopedia. XXI Century. Control Systems, Communications and Electronic Warfare]. Moscow, "Weapons and Technology" Publ., 2006, 695 p. (in Russian).

24. Modern electronic means of dealing with unmanned aircraft in the zone of the ATO. *Scientific Works of Kharkiv National Air Force University*, 2015, no. 3 (44), pp. 54-57 (in Russian).

25. Aniskov R. V., Arkhipova E. V., Gordeev A. A., Pugachev A. N. To the issue of combating illegal use of drones commercial type. *Enginery Problems. Series 16. Anti-Terrorist Engineering Means*, 2017, vol. 111-112, no. 9-10, pp. 71-75 (in Russian).

26. Boyko A. Blighter AUDS. *RoboTrends*, 2015. Available at: http://robotrends.ru/pub/1542/bespilotnik-v-polete-ostanovit-blighter-auds (accessed 14 May 2020) (in Russian).

27. Fedorov E. Vojna s dronami. Saudovskij goliaf protiv husitov [War with drones. Saudi Goliath against the Houthis]. *Voennoe obozrenie*, 28.09.2019. Available at: https://topwar.ru/162842-vojna-s-dronami-saudovskij-goliaf-protiv-husitov.html (accessed 14 May 2020) (in Russian).

28. Kakie sushhestvujut drony i na kakih chastotah oni rabotajut? [What kind of drones are there and at what frequencies do they work?]. *Podavitel.ru*, 2020. Available at: http://www.podavitel.ru/na-kakikh-chastotakh-rabotayut-kvadrokoptery-i-drony.html (accessed 14 May 2020) (in Russian).

29. Podavitel' sotovoj svjazi Monster 16CH [Monster 16CH cellular suppressor]. *n-sb.ru*, 2020. Available at: http://sankt-peterburg.n-sb.ru/podaviteli-gsm-signala.php (accessed 14 May 2020) (in Russian).

30. Chastoty peredachi dannyh [Data transmission frequencies]. Podavitel.ru, 2020. Available at: http://www.podavitel.ru/chastoty-peredachi-dannykh.html (accessed 14 May 2020) (in Russian).

31. Bochmaga D. A., Shimon N. S., Kalach A. V., Kalach E. V., Urusova T. E. Problems of counteraction of the UAV in institutions of FSIN of Russia. *Pozharnaya bezopasnost: problemy i perspektivy*, 2018, vol. 1, no. 9, pp. 89-91 (in Russian).

32. Ohota na bespilotnik: kak voennye borjutsja s grazhdanskoj ugrozoj s vozduha [Hunting for a drone: how the military is fighting the civil threat from the air]. *Voennoe.rf*, 11.11.2018. Available at:

https://voennoe.rf/2018/%D0%91%D0%BF%D0%BB%D0%B029/ (accessed 20 December 2019) (in Russian).

33. Veremeenko K. K., Koshelev B. V., Solovyev Yu. A. The analysis of development of the integrated inertial & satellite navigation systems. *Novosti Navigacii*, 2010, no. 4, pp. 32-41 (in Russian).

34. Semenova L. L. Sovremennye metody navigacii bespilotnyh letatel'nyh apparatov [Modern methods of navigation of unmanned aerial vehicles]. *Science and education today*, 2018, no. 4 (27), pp. 6-8 (in Russian).

35. Scherbinin V. V., Sviyazov A. V., Smirnov S. V., Kvetkin G. A. Autonomous navigation complex for ground and flying robotic vehicles. *Izvestiya SFedU. Engineering Sciences*, 2014, no. 3 (152), pp. 234-243 (in Russian).

36. GLONASS. *Principy postroenija i funkcionirovanija* [*GLONASS. Principles of construction and operation*]. Edit. by A.I. Perova, V.N. Harisova. Moscow, Radiotehnika Publ., 2010. 800 p. (in Russian).

37. Jacenkov V. S. *Osnovy sputnikovoj navigacii. Sistemy GPS NAVSTAR i GLONASS* [*Basics of satellite navigation. GPS NAVSTAR and GLONASS systems*]. Moscow, Goriachaia Liniia - Telecom Publ., 2005, 272 p. (in Russian).

38. Filippov A. A., Bazhin D. A., Khlobystov A. N. Improving Drone Aircraft Control Efficiency under Interference. *Informatsionno-upravliaiushchie sistemy*, 2014, vol. 73, no. 6, pp. 45-50 (in Russian).

39. Grishin V. A. Computer vision systems in unmanned aerial vehicle flight control. *Datchiki & Systemi*, 2009, no. 2, pp. 46-52 (in Russian).

40. Jugaj E. B. Sposob i sistema navigacii passazhirskogo drona v gornoj mestnosti [Method and system for navigation of a passenger drone in a mountainous area]. Patent RU 2681278 C1, 05.03.2019. (in Russian).

41. Korneev M. A., Maksimov A. N., Maksimov N. A. Metody vydelenija tochek privjazki dlja vizual'noj navigacii bespilotnyh letatel'nyh apparatov [Methods for selecting anchor points for visual navigation of unmanned aerial vehicles]. *Trudy MAI*, 2012, no. 58, pp. 6. Available at: https://mai.ru/upload/iblock/086/metody-vydeleniya-tochek-privyazki-dlya-vizualnoy-navigatsii-bespilotnykh-letatelnykh-apparatov.pdf (accessed 14 May 2020) (in Russian).

42. Stepanov D. N., Tishchenko I. P. The problem of modeling the flight unmanned aerial vehicle based on vision systems. *Program Systems: Theory and Applications*, 2011, no. 4, pp. 33-43. Available at: https://cyberleninka.ru/article/n/zadacha-modelirovaniya-poleta-bespilotnogo-letatelnogo-apparata-na-osnove-sistemy-tehnicheskogo-zreniya (accessed 14 May 2020) (in Russian).

43. Diatlov A. P., Diatlov P. A., Kulbikaian B. Kh. *Radioelektronnaia bor'ba so sputnikovymi radionavigatsionnymi sistemami. Monografiia* [Electronic warfare satellite radio navigation systems. Monograph]. Moscow, Radio i Sviaz Publ., 2004. 226 p. (in Russian).

44. Kamnev E. A. *Radiopodavlenie pomehozashhishhennoj navigacionnoj apparatury potrebitelej sputnikovyh radionavigacionnyh sistem v interesah ob#ektovo-territorial'noj zashhity* [*Radio suppression of noise-protected navigation equipment of consumers of satellite radio navigation systems in the interests of*

object-territorial protection. Thesis of PhD]. Moscow, Moscow Aviation Institute, 2018. 160 p. (in Russian).

45. Zhuk A. P., Orel D. V. About the noise immunity evaluation of satellite radio navigation systems. *Infokommunikacionnye tehnologii*, 2012, vol. 10, no. 2, pp. 83-88 (in Russian).

46. Kazakov A. E., Vodjanyh A. A. Puti povyshenija pomehozashhishhennosti navigacionnoj apparatury potrebitelej sputnikovyh navigacionnyh system [Ways to increase the noise immunity of navigation equipment of consumers of satellite navigation systems]. *Information Processing Systems*, 2007, vol. 59, no. 1, pp. 48-51 (in Russian).

48. Kascheev A. A., Koshelev V. I. Estimation of efficiency of the supression of signals of satellite radio navigational systems by intentional hindrance. *Radio Electronics Journal*, 2012, no. 6, pp. 2. Available at: http://jre.cplire.ru/jre/jun12/9/text.pdf (accessed 14 April 2020) (in Russian).

48. Judin V. N., Kamnev E. A. Principy sozdanija protivonavigacionnogo polja radiopomeh [Principles of creating an anti navigation field of radio interference]. *Trudy MAI*, 2015, no. 83, pp. 28. Available at: https://mai.ru/upload/iblock/8cb/yudin_kamnev_rus.pdfhttps://mai.ru/upload/iblock/8cb/yudin_kamnev_rus.pdf (accessed 14 May 2020) (in Russian).

49. Abukraa A. S., Vilkotsky M. A., Lynkov L. M. Influence of the screens with regular conditions on the immunity and accuracy of subscriber receivers of satellite navigators according to the conditions of radiowaves distribution on the real location. *Doklady BGUIR*, 2017, vol. 105, no. 3, pp. 85-92 (in Russian).

50. Tyapkin V. N., Dmitriev D. D., Moshkina T. G. Potential interference immunity of navigation equipment of customers of satellite radio navigational systems. *Vestnik SibGAU*, 2012, vol. 43, no. 3, pp. 113-119 (in Russian).

51. Dmitriev D. D. Issledovanie pomehoustojchivosti apparatury radionavigacii [Investigation of radio navigation equipment noise immunity]. *Sovremennye problemy razvitija nauki, tehniki i obrazovanija* [*Modern problems of science, technology and education development*]. Krasnoyarsk, Institute of advanced training of Siberian Federal University, 2009. pp. 202-209 (in Russian).

52. Tjapkin V. N., Garin E. N. *Metody opredelenija navigacionnyh parametrov podvizhnyh sredstv s ispol'zovaniem sputnikovoj radionavigacionnoj sistemy GLONASS. Monografija* [*Methods for determining the navigation parameters of mobile vehicles using the GLONASS satellite radio navigation system. Monograph*]. Krasnoyarsk, Siberian Federal University, 2012. 260 p.

53. Pantenkov D. G. Results of mathematical modeling of noise immunity of satellite radio navigation systems under the influence of intentional interference. *Uspekhi sovremennoi radioelektroniki*, 2020, no. 2, pp. 57-68 (in Russian).

54. Zhuravlev A. V., Bezmaga V. M., Krasov E. M., Smolin A. V., Shuvaev V. A., Markin V. G. Ustrojstvo dlja prostranstvennoj selekcii signalov navigacionnyh kosmicheskih apparatov s ispol'zovaniem pelengovanija istochnikov radiopomeh [Device for spatial selection of navigation spacecraft signals using direction finding of radio interference sources]. Patent RU 2 619 800 C1, 18.05.2017. (in Russian).

55. Gen K., Chulin N. A. An Integrated Unmanned Aerial Vehicle Navigation System Capable of Fault Detection and Isolation. *Mechanical Engineering and Computer Science*, 2016, no. 12, pp. 182-206 (in Russian).

56. Berkovich S. B., Gribunin V. G., Kotov N. I., Martynyuk G. A., Mahaev A. U., Smirnov D. V., Sholokhov A. V., Lapshina A. A. Solution of efficiency evaluation problem of creation of navigation systems of robotic complexes. *Izvestiya Tula State University*, 2016, no. 11-3, pp. 19-38 (in Russian).

57. Doronin D. V., Donchenko A. A., Shevtsov S. N. Mistakes mathematical model functioning of platformless inertial navigation system at simultaneous navigation, dynamic creation and data processing of multistructural control systems within the development of aircraft integrated navigation system algorithms with use the GPS/GLONASS technologies. *Izvestia of Samara Scientific Center of the Russian Academy of Sciences*, 2012, vol. 14, no. 4 (5), pp. 1363-1367 (in Russian).

58. Maryukhnenko V. S., Erokhin V. V. Structural synthesis of navigation support of triad integrated navigation system on the basis of inertial and satellite technologies. *Scientific Bulletin of the Moscow State Technical University of Civil Aviation*, 2017, vol. 20, no. 4, pp. 69-77 (in Russian). DOI: 10.26467/2079-0619-2017-20-4-69-77.

59. Roubtsov V. D., Zaikin A. A. The comparative analysis of efficiency various variants complex processing of iformation in equipments of consumers satellite radionavigating systems and inertial navigating system. *Scientific Bulletin of the Moscow State Technical University of Civil Aviation*, 2010, no. 159, pp. 128-132 (in Russian).

60. Usov O. S., Horoshko A. Ju., Kvanin L. V. Lazernyj vysotomer dlja bespilotnyh letatel'nyh apparatov vertoletnogo tipa srednej i bol'shoj dal'nosti (LV-50) [Laser altimeter for medium-and long-range helicopter-type unmanned aerial vehicles (LV-50)]. Know-how no. 218.016.804d, 28.08.2018 (in Russian).

61. Fokin G. A. Location estimation in non-line-of-sight conditions using digital terrain model. *T-Comm*, 2019, vol. 13, no. 11, pp. 4-13. (in Russian). DOI: 10.24411/2072-8735-2018-10319.

62. Egurnov V. O., Ilyin V. V., Nekrasov M. I., Sosunov V. G. Unmanned aerial vehicles countermeasures to ensure the protected sites safety analysis. *Enginery Problems. Series16. Anti-Terrorist Engineering Means*, 2018, no. 1-2 (115-116), pp. 51-58 (in Russian).

63. Vaas L. Sound: Yet another way to smack down drones. *Naked Security by Sophos*, 06.08.2015. Available at: nakedsecurity.sophos.com/2015/08/06/sound-yet-another-way-to-smack-down-drones/ (accessed 14 May 2020).

64. Verba V. S. *Aviatsionnye kompleksy radiolokatsionnogo dozora i navedeniia. Printsipy postroeniia, problemy razrabotki i osobennosti funktsionirovaniia. Monografiia* [Aircraft radar patrol and guidance. Principles, problems of development and peculiarities of functioning. Monograph]. Moscow, Radiotekhnika Publ., 2014. 528 p. (in Russian).

65. Verba V. S., Merkulov V. I. Heoretical and practical problems of designing next generation of radio guidance systems. *Radiotehnika*, 2014, no. 5, pp. 39-44 (in Russian).

66. Verba V. S., Merkulov V. I., Samodov I. O. The control of unmanned aerial vehicle in the structure of the local network. *Journal Information-measuring and Control Systems*, 2014, vol. 12, no. 3, pp. 7-12 (in Russian).

67. Verba V. S., Merkulov V. I., Milyakov D. A. Problems of management of large density groups of unmilled flying apparatuses. *Journal Information-measuring and Control Systems*, 2018, vol. 16, no. 6, pp. 3-13 (in Russian).

68. Merkulov V. N., Drogalin V. V., Kanashchenkov A. N., Lepin V. N., Samarin O. F., Solov'ev A. A. *Aviatsionnye sistemy radioupravleniia. Tom 1. Printsipy postroeniia sistem radioupravlsniia. Osnovy sinteza i analiza* [Aviation radio system. Volume 1. Principles of systems radioupravlenie. Fundamentals of synthesis and analysis]. Moscow, Radiotekhnika Publ., 2003. 192 p. (in Russian).

69. Belov S. G., Krylyuk A. D., Merkulov V. I., Chernov V. S. Information systems of unmanned strategic and operational air reconnaissance complexes of USA. *Uspekhi sovremennoi radioelektroniki*, 2020, no. 1, pp. 28-42 (in Russian).

70. Boev N. M. Analysis of UAV radio control and telemetry systems. *Vestnik SibGAU*, 2012, vol. 42, no. 2, pp. 86-91 (in Russian).

71. Boev N. M., Sharshavin P. V., Nigruca I. V. UAVs communication systems for long-distance information transmittion. *Izvestiya SFedU. Engineering Sciences*, 2014, vol. 152, no. 3, pp. 147-158 (in Russian).

72. Boev N. M., Lebedev Yu. A. Energy efficiency managment of communication channels. *Vestnik SibGAU*, 2013, vol. 47, no. 1, pp. 11-15 (in Russian).

73. Boev N. M. Sposoby povyshenija jenergeticheskoj i spektral'noj jeffektivnosti cifrovyh sistem svjazi bespilotnyh letatel'nyh apparatov [Ways to improve the energy and spectral efficiency of digital communication systems for unmanned aerial vehicles]. *Proceedings of Moscow Institute of Physics and Technology*, 2014, vol. 6, no. 2 (22), pp. 162-166 (in Russian).

74. Boev N. M. Razrabotka i proektirovanie bortovogo antenno-fidernogo oborudovanija malyh bespilotnyh letatel'nyh apparatov [Development and design of onboard antenna-feeder equipment for small unmanned aerial vehicles]. *Reshetnevskie chtenija*, 2011, vol. 1, pp. 162-163 (in Russian).

75. Baturin T. N., Boev N. M. Razrabotka i proektirovanie bortovogo usilitelja moshhnosti radiosignala UKV-diapazona dlja bespilotnogo letatel'nogo apparata [Development and design of an on-Board VHF radio signal power amplifier for an unmanned aerial vehicle]. *Reshetnevskie chtenija*, 2012, vol. 1, pp. 141-142 (in Russian).

76. Lebedev Ju. A., Boev N. M. Razrabotka i proektirovanie malogabaritnoj sistemy svjazi malyh bespilotnyh letatel'nyh apparatov [Development and design of a small communication system for small unmanned aerial vehicles]. *Reshetnevskie chtenija*, 2012, vol. 1, pp. 155-156 (in Russian).

77. Slusar V. I. Peredacha dannyh s borta BPLA: Standarty NATO [The data transfer from UAV Board: NATO Standards]. *Elektronika: nauka, tekhnologiia, biznes*, 2010, vol. 101, no. 3, pp. 80-87 (in Russian).

78. Slusar V. I. Radiolinii svjazi s BPLA. Primery realizacii [Radio lines of communication with the UAV. Examples of implementation]. *Elektronika: nauka, tekhnologiia, biznes*, 2010, vol. 103, no. 5, pp. 56-61 (in Russian).

79. Ananev A. V., Stafeev M. A., Makeev E. V. Developing communication organization method employing short-range unmanned flying vehicles. *Trudy MAI*, 2019, no. 105, pp. 14 (in Russian).

80. Ananyev A. V., Katrusha A .N., Gorovoj A. V., Ivanov E. A. Development of the standing wave ratio automatic tuning device of a contour magnet antenna of an unmanned aerial vehicle. *Antenny*, 2017, vol. 240, no. 8, pp. 45-52 (in Russian).

81. Ananev A. V., Erzin I. H., Shherbakov A. A., Filatov S. V. Ajeromobil'naja set' svjazi - jeffektivnaja sistema retransljacii obedinennoj avtomatizirovannoj cifrovoj sistemy svjazi [Aeromobile communication network-an effective relay system for the unified automated digital communication system]. *Military Thought*, 2017, no. 4, pp. 26-34 (in Russian).

82. Ananev A. V., Katrusha A. N. Comparative estimation radiocommunication possibilities with unmanned aerial vehicles in HF and VHF ranges for half-closed and closed path of radio-wave propagation. *T-Comm*, 2017, vol. 11, no.10, pp. 4-9 (in Russian).

83. Ananev A. V., Stafeev M. A., Filatov S. B. Communication and data interchange systems efficiency evaluation on the basis of interspecific forces grouping unmanned aerial vehicles. *Aerospace forces. Theory and practice*, 2017, vol. 3, no. 3, pp. 75-84 (in Russian).

84. Ananev A. V., Zmij B. F., Kaschenko G. A. Upgrade onboard transceiver systems of unmanned aerial vehicles on the basis of the evolutional approach. *Radiotekhnika*, 2016, no. 8, pp. 46-49 (in Russian).

85. Pantenkov D. G., Lomakin A. A. Assessment of stability of the satellite channel of control of unmanned aerial vehicles at influence of intentional interference. *Radiotekhnika*, 2019, vol. 83, no. 11 (17), pp. 43-50 (in Russian).

86. Dolzhenkov N. N., Pantenkov D. G., Litvinenko V. P., Lomakin A. A., Egorov A. T., Gritsenko A. A. Integrated complex of the long-distance radiocommunication for increase efficiency of the solution of target tasks by unmanned vehicle. *Bulletin of Voronezh state technical University*, 2019, vol. 15, no. 3, pp. 102-108 (in Russian). DOI: 10.25987/VSTU.2019.15.3.015.

87. Dolzhenkov N. N., Pantenkov D. G., Egorov A. T., Lomakin A. A., Litvinenko V. P., Velikoivanenko V. I., Lu-Ke-Syu E. Yu. Technical characteristics of the means for satellite radiocommunication with unmanned aerial vehicles. *Bulletin of Voronezh state technical University*, 2019, vol. 15, no. 3, pp. 74-82 (in Russian). DOI: 10.25987/VSTU.2019.15.3.011.

88. Pantenkov D. G., Gusakov N. V., Egorov A. T., Lomakin A. A., Litvinenko V. P., Velikoivanenko V. I., Lu-Ke-Syu E. Yu. Technical implementation of high-speed data radio channel from an unmanned aerial vehicle to ground control station. *Bulletin of Voronezh state technical University*, 2019, vol. 15, no. 3, pp. 52-71 (in Russian). DOI: 10.25987/VSTU.2019.15.5.007.

89. Kirichek R. V. *Razrabotka i issledovanie kompleksa modelej i metodov dlja letajushhih sensornyh setej. Dissertacija na soiskanie uchenoj stepeni doktora*

tehnicheskih nauk [*Development and research of a set of models and methods for flying sensor networks. Thesis of Dr. Sc.*]. Saint Petersburg, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, 2018. 276 p. (in Russian).

90. Samoylenko D. V., Finko O. A., Eremeev M. A. Distributed processing and data protection in the group of complexes with unmanned aerial vehicles. *Radio Communication Theory and Equipment*, 2017, no. 4, pp. 93-100 (in Russian).

91. Samoylenko D. V., Finko O. A. Providing integrity information group unmanned aerial vehicles under destructive impact pursue. *Enginery Problems. Series16. Anti-Terrorist Engineering Means*, 2017, no. 5-6 (107-108), pp. 20-27 (in Russian).

92. Samoylenko D. V., Finko O. A. Noise immunity of data transmission in a radio channel robotic complexes based on polynomial residue classes. *H&ES Research*, 2016, vol. 8, no. 3, pp. 49-55 (in Russian).

93. Dvornikov S. V., Dvornikov S. S., Morozov E. V. Model of radiotechnical systems of unmanned apparatus under conflict. *Questions of radio-electronics, the TV equipment series*, 2020, no. 1, pp. 84-90 (in Russian).

94. Dvornikov S. V., Pogorelov A. A., Dvornikov S. S., Ivanov R. V. Proposals for restoring signals in control channels of unmanned aerial vehicles. *Questions of radio-electronics, the TV equipment series*, 2020, no. 1, pp. 91-97 (in Russian).

95. Dvornikov S. V Procedure of evaluation of imitation stability of robotic devices control channels. *Radio industry*, 2016, no. 2, pp. 64-69 (in Russian).

96. Donchenko A. A., Nehoroshev G. V., Shtefan V. I. Tehnologija postroenija vysokoskorostnyh jenergoskrytnyh kanalov peredachi komand upravlenija, video i telemetrii gruppirovki robototehnicheskih kompleksov special'nogo naznachenija [Technology for building high-speed energy-secretive channels for transmitting control commands, video and telemetry for grouping special-purpose robotic systems]. *Robotizacija vooruzhjonnyh sil Rossijskoj Federacii* [*Robotization of the armed forces of the Russian Federation*]. Anapa, Military innovation Technopolis "ERA", 2019, pp. 174-179 (in Russian).

97. Donchenko A. A., Chirov D. C. Rationale requirements for the communication system of UAVS medium and long range, *T-Comm*, 2015, vol. 9, no. 12, pp. 12-16 (in Russian).

98. Chirov D. S., Lobov E. M. Choice of signal-code constructure for the command-telemetry radio communication line with medium andlong range unmanned aerial vehicles. 2017, *T-Comm*, vol. 11, no.10, pp. 21-28 (in Russian).

99. Chertova O. G., Chirov D. S. Building a core communication network which is based on small size unmanned aircraft vehicle without ground infrasrtuvture. *H&ES Research*, 2019, vol. 11, no. 3, pp. 60-71 (in Russian). DOI: 10.24411/2409-5419-2018-10269.

100. Borodin V. V., Petrakov A. M., Shevtsov V. A. The analysis of algorithms of routing in a communication network groups of unmanned aerial vehicles. *Trudy MAI*, 2016, no. 87, pp. 16 (in Russian).

101. Borodin V. V., Petrakov A. M., Shevcov V. A. Analiz jeffektivnosti peredachi dannyh v seti svjazi gruppirovki bespilotnyh letatel'nyh apparatov

[Analysis of the effectiveness of data transmission in the communication network of the unmanned aerial vehicle grouping]. *Trudy MAI*, 2015, no. 81, pp. 27 (in Russian).

102. Nazarov L. E., Igoshin E. V., Zudilin A. S., Sheglov M. A. Development, realization and experiments of coding for unmanned aerial vehicle system high-rate telemetry channel. *Uspekhi sovremennoi radioelektroniki*, 2014, no. 8, pp. 68-74 (in Russian).

103. Parshin Y. N., Kudryashov V. I. Analysis of data transmission channel capacity from unmanned aerial vehicle with imprecise channel matrix. *Vestnik of Ryazan state radioengineering university*, 2015, no. 52, pp. 22-27 (in Russian).

104. Sivov A. Ju. Aleshin M. G. Obosnovanie osnovnyh parametrov antennoj sistemy retransljatora svjazi na bespilotnom letatel'nom apparate [Justification of the main parameters of the antenna system of the communication repeater on an unmanned aerial vehicle]. *Radio communication technology*, 2011, no. 16, pp. 43-54 (in Russian).

105. Kryzhevich L. S., Sizov A. S. Current issues of transfer bitmap from unmanned aerial vehicles. *Proceedings of the South-West State University*, 2012, no. 6 (45), pp. 54-60 (in Russian).

106. Makarov I. V. Estimation of communication system's capacity for the unmanned aerial vehicle control. *Radiotekhnika*, 2013, no. 4, pp. 40-45 (in Russian).

107. Fokin G. A. Survey of Radio Communication Channel Models for Unmanned Aerial Vehicles. *Proceedings of Telecommunication Universities*, 2018, vol. 4, no. 4, pp. 85-101 (in Russian). DOI: 10.31854/1813324X-2018-4-3-85-101.

108. Smorodinov A. A. Kak vybrat' shirokopolosnyj modem dlja bespilotnogo letatel'nogo apparata (BLA) ili robototehniki [How to choose a broadband modem for an unmanned aerial vehicle (UAV) or robotics]. *Habr.com*, 22.03.2019. Available at: https://mai.ru/upload/iblock/8cb/yudin_kamnev_rus.pdfhttps://mai.ru/upload/iblock/8cb/yudin_kamnev_rus.pdf (accessed 14 May 2020) (in Russian).

109. Mihajlov R.L. *Opisatelnye modeli sistem sputnikovoj svjazi kak kosmicheskogo jeshelona telekommunikacionnyh sistem specialnogo naznachenija. Monografija* [*Descriptive models of satellite communication systems as a space echelon of special-purpose telecommunications systems. Monograph*]. Saint Petersburg, Naukoemkie Tehnologii Publ., 2019. 150 p. (in Russian).

110. Dobykin V. D., Kuprijanov A. I., Ponomarev V. G., Shustov L. N. *Radiojelektronnaja bor'ba. Cifrovoe zapominanie i vosproizvedenie radiosignalov i jelektromagnitnyh voln* [*Electronic warfare. Digital storage and reproduction of radio signals and electromagnetic waves*]. Moscow, Vuzovskaja Kniga Publ., 2009. 360 p. (in Russian).

111. Harkevich A. A. *Borba s pomehami* [*The anti-interference*]. Moscow, Librokom Publ., 2018. 280 p. (in Russian).

112. Paliy A. I. *Radioelektronnaia bor'ba* [Electronic warfare]. Moscow, Voenizdat Publ., 1989. 350 p. (in Russian).

113. Komashinskij V. I. Maksimov A. V. *Sistemy podvizhnoj radiosvjazi s paketnoj peredachej informacii: osnovy modelirovanija* [*Mobile radio communication systems with packet data transmission: modeling basics*]. Moscow, Gorjachaja linija – Telekom Publ., 2007. 176 p. (in Russian).

114. Borisov V. A., Kalmykov V. V., Kovalchuk Ja. M., Sebekin Ju. N., Senin A. I., Fedorov I. B., Cikin I. A. *Radiotehnicheskie sistemy peredachi informacii* [*Radio engineering systems for transmitting information*]. Moscow, Radio i Svjaz Publ., 1990. 304 p. (in Russian).

115. Maslov P. V. Sravnitelnyj analiz metodov cifrovoj moduljacii [Comparative analysis of digital modulation methods]. *Molodezhnyy nauchno-tekhnicheskiy vestnik*, 2013, no. 2, pp. 46 (in Russian).

116. Peskov S. N., Ishhenko A. E. Raschet verojatnosti oshibki v cifrovyh kanalah svjazi [Calculating the probability of error in digital communication channels]. *Telesputnik*, 2010, no. 11, pp. 70-75 (in Russian).

117. Ivanov U. A., Nevstruev I. A. Structure and noise immunity of OFDM wireless access systems. *Electrotechnical Systems and Complexes*, 2009, vol. 5, no. 3, pp. 25-29 (in Russian).

118. Pantenkov D. G., Gusakov N. V., Sokolov V. M., Velikoivanenko V. I., Konstantinov V. S. Kompleks metodik ocenki jeffektivnosti reshenija chastnyh celevyh zadach voennogo vremeni kosmicheskim apparatom mnogocelevoj kosmicheskoj sistemy [A set of methods for evaluating the effectiveness of solving specific wartime targets by a multi-purpose space system spacecraft]. *Aktual'nye voprosy proektirovanija kosmicheskih sistem i kompleksov* [*Current issues of designing space systems and complexes*]. Khimki, S. A. Lavochkin scientific and production Association, 2014, no. 15, pp. 107-150 (in Russian).

119. Pantenkov D. G., Gusakov N. V., Sokolov V. M., Velikoivanenko V. I., Konstantinov V. S. Kompleks metodik ocenki jeffektivnosti reshenija chastnyh celevyh zadach mirnogo vremeni kosmicheskim apparatom mnogocelevoj kosmicheskoj sistemy [A set of methods for evaluating the effectiveness of solving specific peacetime targets by a multi-purpose space system spacecraft]. *Aktual'nye voprosy proektirovanija kosmicheskih sistem i kompleksov* [*Current issues of designing space systems and complexes*]. Khimki, S. A. Lavochkin scientific and production Association, 2014, no. 15, pp. 89-106 (in Russian).

120. Krasnosselsky I. N., Kanev S. A. Analyzing DVB-T system's interference immunity in a multipath fading channel as a model. *Electrosvyaz*, 2010, no. 7, pp. 28-30 (in Russian).

121. European Standard (Telecommunications series) ETSI EN 300 744 V1.6.1. – Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television. 2009. Available at: http://www.etsi.org (accessed 14 May 2019).

122. Varakin L E. *Sistemy svjazi s shumopodobnymi signalami* [*Communication systems with noise-like signals*]. Moscow, Radio i Svjaz Publ., 1985. 384 p.

123. Makarenko S. I., Ivanov M. S., Popov S. A. *Pomekhozashchishchennost' sistem sviazi s psevdosluchainoi perestroikoi rabochei chastity. **Monografija*** [Interference Resistance Communication Systems with Frequency-Hopping Spread Spectrum. Treatise]. Saint Petersburg, Svoe Izdatelstvo Pabl., 2013, 166 p. (in Russian).

124. JSC-CR-10-004. Communications Receiver Performance Degradation Handbook. Annapolis, Joint Spectrum Center, 2010. 306 p.

125. Erokhin G. A., Mandel V. I., Nesterkin Yu. A., Strukov A. P. The Calculation Methodology for the Energetic Reserve of the Radio Link Spacecraft-Station. *Rocket-Space Device Engineering and Information Systems*, 2018, vol. 5, no. 1, pp. 65-74 (in Russian).

126. Polynkin A. V., Le H. T. Analysis of characteristics of UAV communication link. *Izvestiya Tula State University*, 2013, no. 7-2, pp. 98-107 (in Russian).

127. Zikratov I. A., Zikratova T. V., Lebedev I. S., Gurtov A. V. Trust and reputation model design for objects of multi-agent robotics systems with decentralized control. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2014, no. 3 (91), pp. 30-38 (in Russian).

128. Zikratov I. A., Zikratova T. V., Lebedev I. S. Trust model for information security of multi-agent robotic systems with a decentralized management. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2014, no. 2 (90), pp. 47-52 (in Russian).

129. Viksnin I. I., Marinenkov E. D. Counteraction to the Hidden Destructive Impact in Swarms of Unmanned Aerial Vehicles. *International Journal of Open Information Technologies*, 2018, vol. 6, no. 12, pp. 1-11 (in Russian).

130. Vinokurov A. V. Vulnerability analysis complexes with unmanned aerial vehicles and classification of security threats circulating information in them. *I-Methods*, 2016, no. 1, pp. 5-9 (in Russian).

131. Makarenko S. I. *Computer systems, networks and telecommunication*. Stavropol, Sholokhov Moscow State University for the Humanities (Stavropol Branch) Publ., 2008, 352 p. (in Russian).

132. Makarenko S. I. *Information security*. Stavropol, Sholokhov Moscow State University for the Humanities (Stavropol Branch) Publ., 2009, 372 p. (in Russian).

133. Nefjodova M. Mnozhestvennye ujazvimosti v 4G LTE pozvoljajut sledit' za abonentami i poddelyvat' dannye [Multiple vulnerabilities in 4G LTE allow you to monitor subscribers and fake data]. *Haker*, 07.03.2018. Available at: https://xakep.ru/2018/03/07/lteinspector/ (accessed 20 December 2019) (in Russian).

134. Peregudov M. A., Semchenko I. A. Evaluation of Efficiency of Random Multiple Access to Aloha Type Environment with Voice Connections, Transfer of Service Commands, Text Messages and Multimedia Files in Destructive Impact Conditions. *SPIIRAS Proceedings*, 2019, vol. 18, no. 4, pp. 887-911 (in Russian). DOI: 10.15622/sp.2019.18.4.887-911.

135. Peregudov Maksim Anatol'evich, Steshkovoy Anatoliy Sergeevich, Boyko Aleksey Aleksandrovich Probabilistic random multiple access procedure model to the CSMA/CA type medium. *SPIIRAS Proceedings*, 2018, vol. 59, no. 4, pp. 92-114 (in Russian). DOI: 10.15622/sp.59.4.

136. Peregudov M. A., Boyko A. A. Model Procedure of Random Multiple Access to the Environment Type S-ALOHA. *Informatsionno-upravliaiushchie sistemy*, 2014, vol. 73, no. 6, pp. 75-81 (in Russian).

137. Makarenko S. I. Estimation of quality of service in radio network with package transmitting in unstationary mode under influence of external destructive factors. *Radio Electronics Journal*, 2012, no. 6, pp. 2. Available at: http://jre.cplire.ru/jre/jun12/9/text.pdf (accessed 20 April 2020) (in Russian).

138. Makarenko S. I. The countermeasures of the radio networks with the random multiple access by changing the radionet state to non-stable. *Radio Electronics Journal*, 2011, no. 9. Available at: http://jre.cplire.ru/jre/sep11/4/text.pdf (accessed 20 April 2020) (in Russian).

139. Makarenko S. I. Information Weapon in Technical Area – Terminology, Classification and Examples. *Systems of Control, Communication and Security*, 2016, no. 3, pp. 292-376 (in Russian). DOI: 10.24411/2410-9916-2016-10311.

140. Holmogorov V. Ugnat dron. Metody perehvata upravlenija kopterami [Hijack a drone. Methods for intercepting copter control]. *Haker*, 24.06.2019. Available at: https://xakep.ru/2019/06/24/dron-interception/ (accessed 20 April 2020) (in Russian).

141. Khan A. Hacking the Drones. *Open Web Application Security Project*, 2016. Available at: https://owasp.org/www-chapter-london/assets/slides/OWASP201604_Drones.pdf (accessed 20 April 2020).

142. Rodday N. Hacking a Professional Drone. *Black Hat Asia 2016*, 2016. Available at: https://www.blackhat.com/docs/asia-16/materials/asia-16-Rodday-Hacking-A-Professional-Drone.pdf (accessed 20 April 2020).

143. Petrovsky O. Attack on the drones: security vulnerabilities of unmanned aerial vehicles. *25th Virus Bulletin International Conference*, 2015. Available at: https://www.virusbulletin.com/conference/vb2015/abstracts/attack-drones-security-vulnerabilities-unmanned-aerial-vehicles (accessed 20 April 2020).

144. Here's how easy it is to hack a drone and crash it. Futurity, 08.06.2016. Available at: https://www.futurity.org/drones-hackers-security-1179402-2/ (accessed 20 April 2020).

145. Kazakov L. N., Ismailov A., Kukushkin D. S. Ocenka jeffektivnosti primenenija OFDM-tehnologij v vysokoskorostnyh sistemah aviacionnoj svjazi [Evaluating the effectiveness of OFDM technologies in high-speed aviation communication systems]. *Sistemy sinhronizacii, formirovanija i obrabotki signalov*, 2013, vol. 4, no. 3, pp. 146-149 (in Russian).

146. Kazakov L. N., Seljanskaja E. A., Solovev D. M., Botov V. A. Organizacija jenergeticheski skrytnyh radiokanalov dlja peredachi dannyh i komand upravlenija bespilotnymi letatel'nymi apparatami [Organization of energy-secretive radio channels for transmitting data and commands for controlling unmanned aerial vehicles]. *Sistemy sinhronizacii, formirovanija i obrabotki signalov*, 2017, vol. 8, no. 4, pp. 91-93 (in Russian).

147. Kazakov L. N., Carev A. B., Solovev N. V., Mahov M. I. Razrabotka OCDM sistemy dlja organizacii informacionnogo obmena gruppy BPLA [Development of an OCDM system for organizing information exchange of a group of UAVs]. *Sistemy sinhronizacii, formirovanija i obrabotki signalov*, 2018, vol. 9, no. 4, pp. 51-56 (in Russian).

148. Samoylenko D. V. Increasing of information survivability of the group of robotic engineering complexes under destructive attack of the violator. *Automation of Control Processes*, 2018, vol. 52, no. 2, pp. 4-13 (in Russian).

149. Wang H., Zhao H., Zhang J., Ma D., Li J., Wei J. Survey on unmanned aerial vehicle networks: A cyber physical system perspective. *IEEE Communications Surveys & Tutorials*, 2019, vol. 22, no. 2, pp. 1027-1070. DOI: 10.1109/COMST.2019.2962207.

Статья поступила 20 мая 2020 г.

Информация об авторе

Макаренко Сергей Иванович – доктор технических наук, доцент. Ведущий научный сотрудник. Санкт-Петербургский институт информатики и автоматизации РАН. Профессор кафедры информационной безопасности. Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина). Профессор кафедры информационных и вычислительных систем. Петербургский государственный университет путей сообщения императора Александра I. Область научных интересов: сети и системы связи; радиоэлектронная борьба; информационное противоборство. E-mail: mak-serg@yandex.ru

Адрес: Россия, 197376, Санкт-Петербург, ул. Профессора Попова, 5.

Counter Unmanned Aerial Vehicles. Part 3. Electronic Warfare against Navigation and Radio Connection Subsystems of Unmanned Aerial Vehicles

S. I. Makarenko

Relevance. *There have been reports of unauthorized use of unmanned aerial vehicles (UAVs) in highly controlled areas (airports, military installations, against critical industrial infrastructure) in the media since the mid-2000s. Nowadays, small UAVs are widely used for unauthorized surveillance of important objects, conducting terrorist attacks and sabotage, carrying prohibited goods (weapons, drugs), as well as for military purposes. For this reason, the problem of countering UAVs, and especially small UAVs, has become extremely relevant. Analysis of publications in this area has shown a small number of serious studies on this topic. There are often too optimistic conclusions about the effectiveness of existing electronic warfare (EW) systems for countering all types of UAVs in many papers. However, the problem of countering UAVs, and especially small UAVs, is highly complex, multi-faceted, and has not been solved yet.* ***The goal of this paper*** *is to systematize and analyze various ways and means of countering UAVs, as well as to form general directions for effective solution of the problem. The material is presented in the paper focuses on the analysis of the capabilities of EW-systems to disrupt normal functioning navigation and radio connection subsystems of UAVs.* ***Results****. The results of systematization and analysis of various methods and means of countering UAVs, which are based on EW, are presented in the article. This systematization is based on more than 140 open sources. The analysis of the sources show the main features of the UAV as an object of electronic jamming, and made possible a detailed multi-aspect analysis of modern EW-systems, their effectiveness and disadvantage. Suggestions for improving the effectiveness of the EW-systems what are used against UAVs are also summarized in this paper.* ***Elements of the novelty of the*** *paper are the general features of the electronic jamming to UAVs, as well as systemic disadvantage in technological solutions of the EW-systems, which*

lead to a decrease in their combat effectiveness when they are used against UAVs. ***Practical significance****. The material of the paper can be used to generate initial data for modeling and studying the combat effectiveness of the EW-systems when countering UAVs. This article can be useful for designers who design countering UAV systems as well.*

Keywords*: unmanned aerial vehicle, UAV, air defense, air defense system, counter unmanned aerial vehicles, C-UAV, C-UAS, anti-UAV defense system, counter-drone systems, anti-drone technologies, counter-UAVs technologies, electronic warfare, electronic warfare system, electronic jamming*.

Information about Author

Sergey Ivanovich Makarenko – Dr. habil. of Engineering Sciences, Docent. Leading Researcher. St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences. Professor of Information Security Department. Saint Petersburg Electrotechnical University 'LETI'. Professor of Department of Information and Computer Systems. Emperor Alexander I Saint Petersburg State Transport University Field of research: stability of network against the purposeful destabilizing factors; electronic warfare; information struggle. E-mail: mak-serg@yandex.ru

Address: Russia, 197376, Saint Petersburg, Professor Popov Street, 5.