Алматинский университет энергетики и связи имени Гумарбека Даукеева

УДК 681.2:621.37:004.056.5(043) На правах рукописи

ҚАДЫРЖАН АРУЖАН БУЛАТОВНА

Разработка новых средств защиты информации в зоне прямой радиовидимости

8D07104 – «Приборостроение»

Диссертация на соискание
ученой степени доктора философии (PhD)

Научный руководитель:
доктор PhD, профессор
Жауыт Әлғазы

Зарубежный научный консультант:
к.т.н, профессор
Головин Владислав Викторович
(Севастополь, РФ)

Республика Казахстан
Алматы, 2026

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящей диссертации применяются следующие обозначения и сокращения:

РК – Республика Казахстан;

МНВО – Министерство науки и высшего образования;

ОПК – оборонно-промышленный комплекс;

БПЛА – беспилотный летательный аппарат;

РЭБ – радиоэлектронная борьба;

АЦП – аналого-цифровой преобразователь;

ПВО – противовоздушная оборона.

ВВЕДЕНИЕ

Общая характеристика работы. В диссертационной работе представлены результаты разработки новых подходов к защите информации при передаче команд группам БПЛА в ходе прямой радиовидимости.

Актуальность темы исследования. Актуальность работы определяется сложившимися тенденциями в области использования роботизированных вооружений и боевой техники. Имеет место существенный рост концентрации БПЛА вблизи линии боевого соприкосновения (ЛБС), а также возрастание значения радиоэлектронной борьбы (РЭБ), в том числе ведущейся непосредственно вблизи ЛБС. Актуальным становится защищенное использование БПЛА при управлении с достаточно короткого расстояния (порядка нескольких километров), что обеспечивается, в частности, при помощи передачи команд по оптоволоконной линии связи. Наблюдается также устойчивый переход к использованию БПЛА в групповом режиме, причем здесь также более чем велико значение защиты информации от оператора к группе. Тем самым актуальной становится разработка новых методов защиты информации в зоне прямой радиовидимости (по порядку величины это отвечает удаленности линии горизонта, т.е. около 4 км.), которые позволяли бы отказаться как от использования шифросистем, так и от использования протяжённых оптоволоконных линий связи.

Связь темы с конкурсами на грантовое финансирование по научным и (или) научно-техническим проектам:

Исследования выполнялись в соответствие с утвержденным планом исследований, МНВО РК и в рамках научного проекта AP23490107 «Разработка теоретико-информационных методов описания преобразователей волновых сигналов на основе использования конечных алгебраических структур».

Объектами исследования являются системы защиты информации, предназначенные для передачи команд от оператора к группе БПЛА в зоне прямой радиовидимости.

Предметом исследования являются теоретические основы управления группами беспилотных аппаратов, в том числе, оборонного назначения.

Цель исследования:

Разработка системы защиты информации, предназначенной для передачи команд от оператора к группе БПЛА в зоне прямой радиовидимости, и ее отработка на физически реализованных электронных схемах.

Для достижения поставленной цели необходимо решение следующих задач:

- разработать теоретические основы организации защищенного канала передачи команд от оператора к группе БПЛА, связанных между собой

оптоволоконными линиями передачи данных, предназначенного для использования в зоне прямой радиовидимости;

- разработать метод измерения мгновенных значений частоты, амплитуды и фазы квазигармонического колебания, предназначенный для использования в системе защиты информации, передаваемой от оператора группе БПЛА;

- разработать и реализовать электронные схемы, доказывающие работоспособность и практическую полезность предложенного метода защиты информации;

- разработать новый метод обфускации данных на основе операции дискретного логарифмирования в квази-мерсенновских полях Галуа.

Способ достижения цели:

Использованы методы математического моделирования, методы разработки и отладки электронных схем, методы тестирования и доказательства работоспособности электронных схем.

Результаты исследования:

- Разработана теория, обеспечивающая создание защищенного канала передачи команд от оператора к группе БПЛА, связанных между собой оптоволоконными линиями передачи данных, предназначенного для использования в зоне прямой радиовидимости.

- Разработан и апробирован метод измерения мгновенных значений частоты, амплитуды и фазы квазигармонического колебания, основанный на использовании фазовых портретов, предназначенный для использования в системе защиты информации, передаваемой от оператора группе БПЛА.

- Разработаны электронные схемы, доказывающие работоспособность и практическую полезность предложенного метода защиты информации.

- Разработан новый метод обфускации данных на основе операции дискретного логарифмирования в квази-мерсенновских полях Галуа и осуществлена проверка его базовых электронных компонент.

Научная новизна диссертационного исследования состоит в том, что:

- разработана теория, обеспечивающая создание защищенного канала передачи команд от оператора к группе БПЛА, связанных между собой оптоволоконными линиями передачи данных, предназначенного для использования в зоне прямой радиовидимости;

- разработан и апробирован метод измерения мгновенных значений частоты, амплитуды и фазы квазигармонического колебания, основанный на использовании фазовых портретов, предназначенный для использования в системе защиты информации, передаваемой от оператора группе БПЛА;

- разработаны и реализованы электронные схемы, доказывающие работоспособность и практическую полезность предложенного метода защиты информации;

- разработан метод вычисления дискретных логарифмов в квазимерсенновских полях Галуа, в максимальной степени учитывающий особенности таких полей и продемонстрировано, что на этой основе может быть реализован новый метод обфускации данных.

Основные положения, выносимые на защиту:

1. Защита информации, передаваемой от оператора к группе БПЛА в зоне прямой радиовидимости, обеспечивается за счет использования оптоволоконных линий связи между элементами группы и идентификации местоположения оператора радиотехническими методами.
2. Идентификация положения источника радиосигнала осуществима радиотехническими методами за счет использования схемы, реализующей измерение мгновенных значений частоты, амплитуды и фазы квазигармонического сигнала методом фазовых портретов.
3. Новый метод вычисления дискретных логарифмов, разработанный целенаправленно для квазимерсенновских полей Галуа, позволяет реализовать новый метод обфускации данных.

Значимость исследования в национальном и международном масштабах состоит в том, что результаты выполненных работ являются основой для создания нового типа системы защиты информации (национальный масштаб), а также в том, что разработан и апробирован новый метод измерения мгновенных значений частоты, амплитуды и фазы квазигармонического сигнала методом фазовых портретов (международный масштаб).

Научные и технологические нужды (экономическая и индустриальная заинтересованность).

В условиях нарастающей геополитической турбулентности РК нуждается, в том числе, в существенной модернизации боевой техники, стоящей на вооружении казахстанских Вооруженных Сил и иных силовых структур.

Качественные изменения в характере боевых действий требуют создания принципиально новых подходов обеспечению защиты информации, передаваемой от оператора к роботизированным вооружениям различного назначения.

Личный вклад автора заключается в самостоятельном планировании и выполнении экспериментальной части исследования, а также интерпретации и обработке полученных данных, разработке алгоритмов и математических моделей. Автор также работал совместно с научными консультантами над постановкой задач и обсуждением результатов исследования.

Апробация работы.

Основные результаты и выводы, полученные в ходе исследования, а также предложения и рекомендации, основанные на этих результатах, были

доложены и обсуждены на международных конференциях, а также опубликованы в научных журналах. Все эти публикации полностью отражают результаты данного исследования, связанного с темой диссертации.

Публикации. Результаты исследований отражены в следующих научных работах, в том числе:

Результаты исследований отражены в следующих научных работах, в том числе:

По теме диссертации опубликовано 7 печатных работ. Из них 1 – в журнале, входящем в 1-й квартиль по базе данных Scopus (Скопус), 3 – в журналах, входящих во 2-й квартиль по базе данных Scopus (Скопус), 1 – в журнале, входящем в 3-й квартиль по базе данных Scopus (Скопус), 1 – в журнале, входящем в 4-й квартиль по базе данных Scopus (Скопус), 1 – в журналах рекомендованном КОКСОН. В каждую опубликованную статью докторантом был внесен достойный вклад, в них отражены выносимые на защиту положения, результаты, полученные докторантом в ходе проведенных исследований:

1. Shaltykova, D., Kadyrzhan, A., Vitulyova, Y., & Suleimenov, I. (2026). The Provision of Physical Protection of Information During the Transmission of Commands to a Group of UAVs Using Fiber Optic Communication Within the Group. *Drones*, *10*(1), 24. https://doi.org/10.3390/drones10010024

- реализация конкретной схемы защиты информации в соответствии с предложенным подходом.

2. Suleimenov, I., Kadyrzhan, A., Vitulyova, Y. et al. The use of fiber optics for securing information during command transmission to UAV groups. International Journal of Information Technology. (2025). https://doi.org/10.1007/s41870-025-02719-2. - 1

- реализация конкретной схемы защиты информации в соответствии с предложенным подходом.

3. Ermukhambetova, Bayana & Mun, Grigoriy & Kabdushev, Sherniyaz & Kadyrzhan, Aruzhan* & Kadyrzhan, Kaisarali & Vitulyova, Yelizaveta & Suleimenov, I. (2023). New approaches to the development of information security systems for unmanned vehicles. Indonesian Journal of Electrical Engineering and Computer Science. 31. 810. 10.11591/ijeecs.v31.i2.pp810-819. – 1

- реализация конкретной схемы защиты информации в соответствии с предложенным подходом.

4. Vitulyova, Yelizaveta & Kadyrzhan, Kaisarali & Kadyrzhan, Aruzhan* & Shaltykova, Dina & Suleimenov, I. (2024). Reducing the description of arbitrary wave field converters to tensor form. International Journal of Information Technology. 10.1007/s41870-024-01863-5. – 2

- обоснование связи предложенного метода с общими проблемами защиты информации

5. Vitulyova, Yelizaveta & Kadyrzhan, Kaisarali & Kadyrzhan, Aruzhan* & Suleimenov, I. (2024). Application of focusing systems to the protection of information during data transmission in the zone of direct radio visibility. International Journal of Electronics and Telecommunications. 699-705. 10.24425/ijet.2024.149599. – 1

- реализация конкретной схемы защиты информации в соответствии с предложенным методом.

6. Kadyrzhan, A.; Matrassulova, D.; Vitulyova, Y.; Suleimenov, I. Discrete Cartesian Coordinate Transformations: Using Algebraic Extension Methods. Appl. Sci. 2025, 15, 1464. https://doi.org/10.3390/app15031464 - 3.

- реализация конкретных примеров использования предложенной в работе методики

7. Кадыржан, А., Витулёва, Е., Қадыржан, Қ., Сулейменов, И., & Жауыт, Ә. (2025). ПЕРСПЕКТИВЫ РАЗВИТИЯ БЕСПИЛОТНЫХ РОБОТИЗИРОВАННЫХ СИСТЕМ ВОЕННОГО И ГРАЖДАНСКОГО НАЗНАЧЕНИЯ. Вестник КазАТК, 137(2), 544–553. https://doi.org/10.52167/1609-1817-2025-137-2-544-553 - 1

- написание части статьи, относящейся к использованию метаматериалов в радиочастотном диапазоне.

Охранный документ РК

Имеется 1 патент на изобретение «Способ реализации беспилотного аппарата-носителя боеприпаса воздушного базирования».

Была подана заявка на изобретение «Способ защиты информации в зоне прямой радиовидимости». На данный момент имеется положительный результат формальной экспертизы.

Объем и структура диссертации. Диссертационная работа состоит из введения, 4 глав, заключения и списка использованных источников из 220 наименований; содержит 136 страниц основного компьютерного текста, включая 40 рисунков, 10 таблиц и 186 формул.

Глава 1. Обзор литературы

1.1. Трансформации характера использования роботизированных вооружений на современном этапе

Современные вооруженные конфликты выявили целый ряд факторов, важных с точки зрения развития беспилотных аппаратов и характера их применения.

В частности, уже не требует дальнейших доказательств тезис, впервые сформулированный в работе [1]: «роботизированная (постиндустриальная) война есть война стоимостей». Действительно, беспилотные летательные аппараты (БПЛА) качественно изменили характер ведения боевых действий [2], что, впрочем, прогнозировалось на основании анализа характера боестолкновений в современных вооруженных конфликтах, а также на основании анализа литературы, посвященной развитию БПЛА [3-5] и характеру их перспективного боевого применения [6-7].

Как подчеркивается, в [2], вооруженный конфликт в Нагорном Карабахе (Арцахе) осенью 2020 г., стал первым, на протяжении которого основные задачи, традиционно решаемые пилотируемой авиацией (т.е. целеуказание, нанесение ударов по живой силе, позициям и технике противоборствующей стороны и т.д.), были возложены на БПЛА.

Как отмечается в [2], дело не сводится к замене одного вида авиатехники на другой. Это – решающий поворот, являющийся частью революции в военном деле, которая намечалась уже давно [8].

Существенно, что задачи, решаемые беспилотной авиацией в ходе боестолкновений 2022-2025 гг., по сравнению с более ранними конфликтами, качественно трансформировались. Точнее [2] были реализованы способы и приемы их боевого применения, которые ранее рассматривались преимущественно в теории [9]. Типичным примером [2] является групповое использование БПЛА-«камикадзе», в частности, «Герань-2», тогда как в предшествующих военных конфликтах БПЛА данного типа, как правило, наносили одиночные удары.

Еще более показательным является тот факт, что ни одно тактическое (артиллерийское, мотострелковое) формирование не применяется противоборствующими сторонами без использования БПЛА в качестве разведывательных или разведывательно-ударных средств [2].

В таких условиях, как и подчеркивалось в [1], на первый план выходят стоимостные показатели БПЛА, способных уничтожать, в том числе, тяжелую бронетехнику противника. В частности, как вытекает даже из поверхностного анализа сообщений СМИ, командованию боевых подразделений оказалось необходимо кардинально изменить характер применения танков, в особенности таких как «Абрамс», стоимость которых по данным открытых источников информации составляет около 6 млн. долл. США, тогда как стоимость БПЛА типа «Герань-2» - 375 тыс. долл. США (в ценах 2023 г.).

Таким образом, есть все основания утверждать, что прогнозы, отраженные в работе [1], оказались более чем состоятельными. Успех в роботизированной войне все в большей степени определяется экономическими и организационными факторами, так как при стремительном [10,11] развитии беспилотных и безэкипажных вооружений (в том числе, используемых в военно-морском флоте [12]) все большее значение имеют затраты на организацию производства их новых разновидностей.

Наглядным примером в рассматриваемом отношении является мнение бывшего высокопоставленного военного руководителя, отраженное в статье, публикованной CNN (цитируется по [13]). В данной статье, в том числе, сделан акцент на стоимости вооружений и боевой техники: «Пожалуй, приоритетом номер один здесь является овладение целым арсеналом (относительно) дешевых, современных и высокоэффективных беспилотных летательных аппаратов и других технологических средств».

Можно провести аналогию между точкой зрения, отстаиваемой авторами таких работ как [1] и предсказаниями таких видных военных теоретиков прошлого как генерал Д. Дуэ, выдвинувшему неординарную для своего времени концепцию боевого применения авиации [14]: Авиация практически сразу с момента возникновения существенно трансформировала характер войны, включая появление новых родов войск, способов ведения боевых действий и т.д. История военных конфликтов, имевших место во второй половине XX и в начале XXI века, однозначно свидетельствует, что успех операций, проводимых наземными войсками, равно, как и исход войны в целом во многом зависит от исхода борьбы за господство в воздухе.

Следовательно, принимая во внимание результаты [1], есть все основания для проведения анализа текущего состояния развития роботизированных вооружений с тем, чтобы выполнить прогноз, позволяющий определить, какие именно системы такого типа окажутся наиболее востребованными в обозримой перспективе и реализовать соответствующие разработки.

Для анализа характера развития роботизированных вооружений, в том числе, в ближайшей и среднесрочной перспективе, нами используется метод перекрестного анализа открытых источников информации, а также методы прикладной философии техники [15,16], общей теории инноваций [17,18], а также методы теории научных революций [19,20]. Данные методы, построенные на диалектике, действительно позволяют прогнозировать перспективные направления развития технических систем, так как создание тех или иных технических решений часто является откликом на те или иные противоречия.

Отметим также, что в настоящее время, как подчеркивалось, в частности, в [2], де-факто уже произошла вполне определенная революция в военном деле. По объективным причинам она повлечет за собой и существенные трансформации оборонно-промышленных комплексов

различных стран мира. Именно это и позволяет использовать теорию научных революций [19,20] в качестве прогностического инструмента.

Уместно также подчеркнуть, что роль прикладной философии в вопросах военно-технического строительства становится все более очевидной. В частности, даже в статье [13], цитированной выше, в качестве одной из трех приоритетных задач указана следующая: «Внедрение новой философии подготовки и ведения боевых действий, учитывающей ограничения в средствах и способах их применения».

Сформулируем основные тезисы, отражающие характер развития роботизированных вооружений, а далее перейдем к их обоснованию.

Критически важным, особенно для Республики Казахстан, является:

1. Устранение диспропорций между развитием беспилотных летательных, наземных и морских роботизированных систем (дронов), что позволяет прогнозировать (при условии выработки адекватной концепции развития ОПК РК) достаточно активное развитие наземных дронов различного назначения (включая гражданское).

2. Формирование комбинированных групп беспилотных аппаратов, что, прежде всего, предполагает отработку взаимодействия между летательными, наземными и морскими аппаратами в различных комбинациях. Это, в свою очередь, создает предпосылки для максимально широкого использования искусственного интеллекта для достижения данной цели (отметим, что последний вопрос также активно обсуждается в текущей литературе [21-23], причем затрагивается также и социально-политический аспект [24,25]). Несколько забегая вперед, отметим, что нами предложена система защиты информации, передаваемой от оператора именно к группе БПЛА, что создает вполне дополнительные предпосылки для последующего сопряжения ИИ и групп БПЛА. Эта же система защиты информации делает возможным создание комбинированных групп роботизированных вооружений, соответствующие примеры рассматриваются в данной работе.

3. Существенное снижение стоимости не только самого производства, но и организации производства (включая затраты на проведение научно-исследовательских и опытно-конструкторских работ), перспективных роботизированных вооружений при максимальном импортозамещении. Это, в свою очередь, предполагает сопряжение производства перспективных вооружений с производством продукции гражданского назначения (в идеале – продукции двойного назначения).

Первый из сформулированных выше тезисов подтверждается непосредственным анализом текущей литературы по данному вопросу, где констатируется выраженное отставание в развитии наземных робототехнических вооружений [26,27]. В частности, в [26] отмечается: «К сожалению, разработки роботизированных образцов вооружения и военной техники (ВВТ) в России ведут при отсутствии достаточного внимания и необходимой поддержки со стороны государства. Отдельные работы по

роботизации ВВТ проводили только в рамках единичных проектов.». Подчеркнем, что данный вывод касается далеко не только РФ.

Существование указанных выше диспропорций допустимо интерпретировать на основе базовых положений теории научных революций, восходящих к классической монографии Т. Куна [28]. Одним из ключевых понятий данной теории является понятие «парадигмы», которое, впрочем, не имеет однозначной трактовки и в самой монографии [28]. Для целей данной работы наиболее удобен следующий вариант: «Под парадигмами я подразумеваю признанные всеми научные достижения, которые в течение определенного времени дают научному сообществу модель постановки проблем и их решений».

Разумеется, со времен выхода в свет монографии [28] точка зрения Т. Куна неоднократно критиковалась, известны многочисленные попытки ее модернизации и переосмысления. В частности, в начале XXI века была выдвинута концепция «четвертой парадигмы» [29], во многом ориентированной на концепции Big Data и Data Mining. Однако, по отношению к развитию техники наблюдения Т. Куна по-прежнему остаются актуальными, и именно они позволяют интерпретировать существование рассматриваемых диспропорций. Развитие определенной группы технических решений «подчиняет» себе все более многочисленные исследовательские группы, нацеленные на получение значимых результатов, что наглядно продемонстрировано также в работе [19]. Ситуация усугубляется также и экономическими факторами. Так, не может вызывать сомнений, что массовое производство БПЛА военного назначения, в особенности FPV-дронов, стало возможным только потому, что их аналоги гражданского назначения оказались широко востребованы на рынке [30-32].

Сделанный вывод подтверждает и характер разрабатываемых наземных, морских и летательных беспилотных аппаратов. Нельзя не заметить, что концептуально многие БПЛА по своей конструкции копируют пилотируемые самолеты (наличие фюзеляжа, крыльев и т.д.). Аналогичный вывод допустимо сделать и по отношению к морским дронам, причем именно их анализ и позволяет максимально наглядно продемонстрировать существование выраженных диспропорций в развитии роботизированных вооружений, равно как и справедливость выводов, сделанных в работе [19].

1.2. Диспропорции в развитии роботизированных вооружений

Морские дроны, используемые в различных операциях в акватории Черного моря, представляют собой безэкипажные катера или аналоги торпед [33]. Как подчеркивается в цитированной работе, первое применение морских дронов первого поколения относится к событию от 29 октября 2022 года. Эти дроны де-факто представляли собой некую разновидность каноэ, снабженную двигателем от гидроцикла, и управляемую средствами спутникового интернета «Starlink» [33].

Разумеется, морские дроны продемонстрировали многие преимущества, сходные с теми, которые продемонстрировали БПЛА. Как отмечается в [33], такие системы обеспечили альтернативный, асимметричный ответ в условиях отсутствия боеспособного флота. Они показали, в том числе, достаточно высокую эффективность ведения боевых действий на море, а также при нанесении ударов на береговую инфраструктуру.

Такие системы развиваются достаточно быстро. Рисунок 1.1 [33] иллюстрирует разнообразие морских дронов, используемых в ходе конфликта.

Можно видеть, что характер конструкции и характер боевого применения МБРК показывает их выраженное сходство с прототипами, управляемыми экипажами. Именно этот факт говорит о сохранении вполне определенной парадигмы, определяемой в том числе, инерцией коллективного инженерного сознания (термин используется в смысле [19]).

В качестве иллюстрации допустимо рассмотреть схему одного из МБРК, реконструированную по фотографии, представленной в [34], рисунок 1.2. Видно, что данная разработка полностью ориентирована на достаточно стандартную схему плавсредств, хотя она также выявляет складывающуюся тенденцию на максимальное упрощение и удешевление конструкции, которая по объективным причинам в наиболее полной мере проявляется именно в соответствующей военно-технической практике.

Рисунок 1.1 – Типы морских дронов, стоящих на вооружении специализированного подразделения, сформированного 24 августа 2023 г. [33]

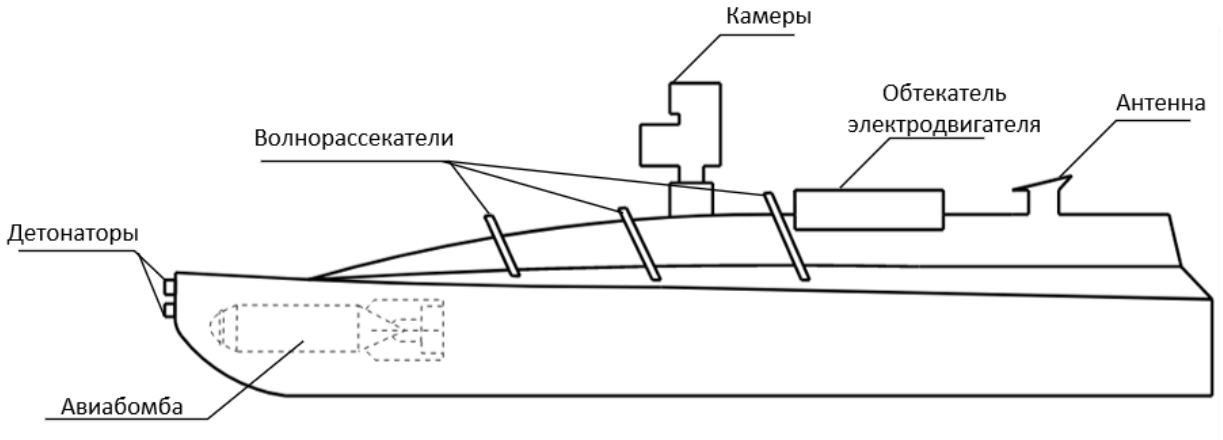


Рисунок 1.2 – Реконструированная схема одного из МБРК (по фотографии [34])

В еще большей степени рассматриваемый фактор проявляется при проектировании беспилотных наземных аппаратов. Инженерная мысль отчетливо отталкивается от аналогии с автомобильным колесным или гусеничным транспортом. Так, роботы, предназначенные для перемещения по земной поверхности, как правило, снабжаются четырьмя или более колесами [35] или являются аналогами существующего гусеничного транспорта [36,37] (рассмотрение шагающих роботов [38] с точки зрения перспектив боевого применения вряд ли представляет интерес).

Пример типовой схемы гусеничных роботов, рассматриваемых в текущей литературе, представлен на рисунке 1.3.

Для наглядности на рисунке 1.4 представлена фотография роботизированную транспортную платформу THeMIS UGV эстонского производства, используемой в военных целях [39].

Нельзя не видеть, что концептуально данная платформа полностью соответствует типовым представлениям о проектировании боевой гусеничной техники.

Еще более наглядно данный вывод подтверждается анализом патентной литературы [40-44]. Для примера на рисунке 1.3 представлена упрощенная схема изделия, отраженного в патенте [44].

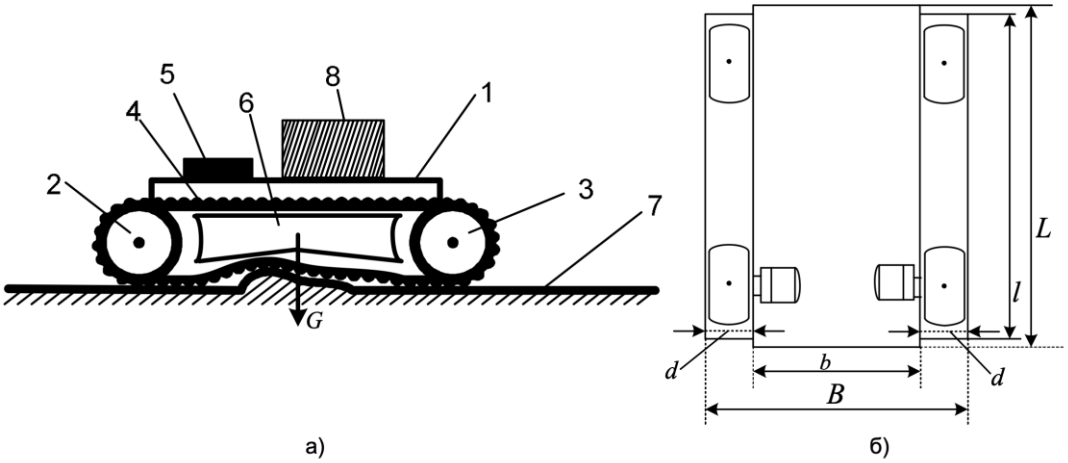


Рисунок 1.3 – Схема гусеничного робота [44]: а – вид сбоку; б – вид сверху; 1 – корпус; 2 – ведущее колесо; 3 – ведомое колесо; 4 – эластичная гусеница; 5 – система управления; 6 – направляющая; 7 – контактная поверхность; 8 – полезная нагрузка

Рисунок 1.4 – Фотография роботизированной транспортной платформы THeMIS UGV эстонского производства [39]

Можно видеть, что инженерная мысль противоборствующих сторон развивается достаточно близкими путями. В частности, фотография (рисунок 1.4) демонстрирует аппарат, весьма близкий к тому, что отражен в российской патентной литературе (рисунок 1.5, [44]).

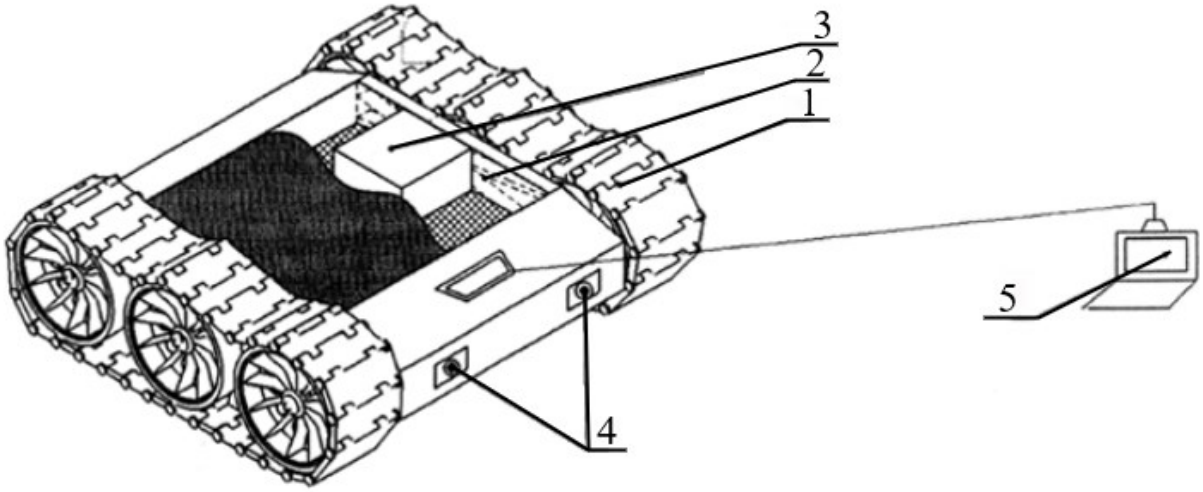


Рисунок 1.5 – Пример гусеничного робототехнического комплекса, отраженного в патентной литературе [44]: 1 – гусеницы; 2 – транспортный модуль; 3 – грузы; 4 – видеокамеры; 5 – пульт дистанционного управления

Таким образом, нельзя не видеть, что типовые конструкции наземного колесного или гусеничного транспорта изначально разрабатывалась в предположении, что им управляет человек и именно это и определило характер их развития. Действительно, транспортное средство, которым управляет человек, должно предусматривать хотя бы минимальный комфорт для водителя, во всяком случае, на уровне, сохраняющем его работоспособность, что в силу инерции мышления заставляет многих разработчиков придерживаться вполне определенной концепции.

При переходе к наземным роботизированным системам указанное выше требование автоматически снимается.

Следовательно, можно перейти к аппаратам, которые заведомо не ориентированы даже на минимальный комфорт водителя. Такие аппараты в настоящее время разрабатываются в Республике Казахстан, в частности, в [45] предложен одноосный робот для разминирования.

1.3. Особенности разработки беспилотных аппаратов группового применения

Массовое применение БПЛА уже изменило содержание термина «господство в воздухе». Соображения, основанные на методах общей теории инноваций, дополняемые доказательством возможности создания наземных дронов различного назначения, позволяют сделать вывод о том, что революция, о которой говорилось в [2], только набирает темп, причем все большее значение будут иметь группы аппаратов различного назначения, в том числе и комбинированные. Соответствующие тенденции также уже прослеживаются. В частности, тактика применения дронов уже во многом ориентируется на истощение средств защиты противника, в частности, по боезапасу за счет использования атакующей группы. Так, в работе [2], в

которой анализируется опыт применения морских дронов против объектов в охраняемой морской акватории, подчеркивается, что наилучшая тактика их применения предполагает атаку группы из 6-7 дронов, причем успешное выполнение задачи предполагает проникновение только 2-3 дронов через систему защиты гавани [2].

Использование групп беспилотных аппаратов делает актуальным их сопряжение с системами искусственного интеллекта. Это, в том числе, означает, что центр тяжести (наукоемкая составляющая) в разработках все более явно будет переносится с конструкции физических компонент группы (в перспективе – боевой нейронной сети [1]) на интеллектуальную составляющую (программное обеспечение), которое не может не включать в себя системы защиты информации.

Указанные факторы делают все более актуальным создание алгоритмов управления группами БПЛА. Кроме того, можно указать целый ряд задач, для решения которых целесообразно использовать именно группы беспилотных летательных аппаратов. Например, это относится к беспилотным аппаратам, используемым для дистанционного зондирования [46,47]. При решении задач такого рода использование одного БПЛА (или нескольких БПЛА, каждый из которых управляется отдельным оператором) заведомо обладает низкой эффективностью [48], особенно когда осуществляется мониторинг значительных площадей. Действительно, формирование роя БПЛА, образующего единое целое за счёт обмена информацией, существенно повышает эффективность управления, так как оно может осуществляться единственным оператором [49].

Сходным образом, использование групп БПЛА оправдано для мониторинга дикой природы на больших территориях, например, для слежения за дикими животными [50], а также для мониторинга качества воздуха [51,52]. Это позволяет получать подробную информацию о состоянии экосистемах и влиянии на них человеческой деятельности [53], поскольку БПЛА могут оснащаться самым различным дополнительным оборудованием, в частности, датчиками, предназначенным для контроля качества воздуха [54]. Подчеркнем, что для рассматриваемой цели в последней работе использовался именно рой БПЛА.

Не вызывает также сомнений, что группы БПЛА будет также все более активно использоваться в военном деле. Точнее, следует ожидать, что будет иметь место переход от использования БПЛА существующих типов [55,56], управляемых отдельным оператором, к использованию роя БПЛА, который представляет собой единую систему. Такая тенденция уже прослеживается вполне отчетливо. Так в работе [57] рассматривалась возможность использования групп БПЛА для создания мобильной сети, охватывающей большую площадь, и применяемой для обеспечения связи между небольшими военными подразделениями. Более того, имеются сведения о том, что группы БПЛА, используемые в военных целях, уже оснащаются искусственным

интеллектом [58], т.е. решается задача, неотделимая от создания группового управления роем БПЛА.

Задача группового управления роботами различного назначения рассматривается в литературе весьма продолжительное время [59-61]. В том числе, это относится и к аппаратам, перемещающимся в 3-D среде [62,63]. Для ее решения используются различные методы, в частности, построенные на самоорганизации (Self-adaptive collective motion) групп БПЛА [64], на машинном обучении [65], на использовании теории графов [66]. Известны работы, в которых рассматривается модернизированный алгоритм Ольфати-Сабера, использующий виртуального лидера, которого отслеживают все БПЛА, формирующие группу [67]. В работе [68] для управления роем БПЛА предложено использовать алгоритмы, построенные с использованием искусственного интеллекта в сочетании с IoS. На данной основе в цитированной работе имитируется самоорганизующаяся сеть ZigBee.

Однако, децентрализованный алгоритм управления роботами, который принимает во внимание только информации о позициях других элементов системы, но не о направлениях их движения, имеют существенные ограничения [68]. Отчасти это затруднение преодолено в работе [69].

Алгоритмы управления системой из нескольких БПЛА, рассматриваемые в работе [70], также ориентируются на распределенное управление, ориентированное на так называемый консенсус «лидер-последователь», обеспечивающий перемещение всего роя как системного целого в соответствии с заранее заданной траекторией. В работе [71], где рой дронов рассматривается с позиций сетевых систем управления (Networked Control Systems, NCS), подчеркивается роль бортовых вычислительных систем для управления роем БПЛА как системным целым. В работе [72] была решена задача о сопряжении искусственной нейронной сети с роем БПЛА, которая, в том числе, предусматривает сохранение заданного расстояния между элементами роя, а также сохранять строй группы. Известны работы, в которых управление роями БПЛА ориентируется на нечеткую логику [73,74]. Отметим, что работы в данном направлении ведутся, в том числе, и российскими авторами [75,76], причем внимание уделяется также алгоритмам, построенным на аналогиях с миром живой природы [77,78].

Переход к использованию роев БПЛА представляет интерес, в том числе, и с точки зрения защиты информации, в том числе, при передаче данных в зоне прямой радиовидимости. Именно этот вопрос представляет наибольший интерес с точки зрения преследуемых нами целей. Отметим, что такая постановка вопроса во многом совпадает с существующими тенденциями [79]. Например, в литературе обсуждается вопрос о применении беспилотных систем в качестве ретрансляторов [80,81].

Подчеркнем также, что в настоящее время в связи с совершенствованием методов радиоэлектронной борьбы все более актуальными становятся физические методы защиты информации, например, ориентированные на использование невоспроизводимых рядов данных [82-84]. Нет необходимости

подчеркивать, что методы криптографии, которые, в том числе, могут быть использованы бортовыми шифросистемами, продолжают активно совершенствоваться [85-88], в том числе, с применением современных нейросетевых методов [89,90]. Они, однако, были и остаются более чем уязвимыми по отношению к человеческому фактору. Кроме того, использование сложных бортовых шифросистем неизбежно влечет за собой увеличение производительности бортовых вычислительных систем, а, следовательно и их стоимости.

В качестве предельного случая реализации альтернативного подхода может рассматриваться случай, когда дрон управляется по оптоволокну [91,92], что заведомо исключает сторонние воздействия при помощи радиосигналов. Отметим, что FPV-дроны с управлением по оптоволокну в настоящее время активно применяются в ходе боестолкновений вблизи линии боевого соприкосновения в текущем конфликте на территории бывшего СССР. Подчеркнем также, что использование оптоволокна заведомо предполагает передачу сигнала на сравнительно небольшие расстояния. Следовательно, сам факт использования такого метода свидетельствует о целесообразности разработки и других методов, предполагающих передачу сигналов в зоне прямой радиовидимости. При передаче управляющих команд в зоне прямой радиовидимости для защиты информации может быть также использован метод [93,94], предполагающий идентификацию местоположения источника сигнала (подробнее он будет рассматриваться в следующих параграфах данной главы). Команды принимаются к исполнению при условии, что координаты источника совпадают с заложенными в память БПЛА и игнорируются в противоположном случае. Нельзя не видеть, что метод, предложенный в [93,94], применим именно для роев БПЛА, что отвечает современным тенденциям, ориентированным на переход к использованию роев дронов.

Данный метод, однако, не является единственно возможным. В нашей работе [95] отмечалось, что методика физической защиты информации допускает существенное усовершенствование за счет обмена информацией между, составляющими рой, по оптоволоконным линиям связи. В этом случае протяженность физических линий передачи данных, обеспечивающих защиту информации, может быть существенно уменьшена по сравнению, например, со случаем, когда управление дроном осуществляется по оптоволокну, которое связывает БПЛА и оператора. Метод, рассмотренный в цитированной работе, аналогичен методу, рассмотренному в [96]: пара бортовых приемников регистрирует разность времени Δt распространения радиосигнала от источника (оператора) до каждого из приемников, составляющих пару. Измерение Δt позволяет идентифицировать гиперболу (или гиперболоид, если рассматривается трехмерная задача), на которой располагается источник сигнала. Использование еще одной пары приемников (или двух таких пар для трехмерной задачи) позволяет идентифицировать координаты оператора как точку пересечения гипербол (гиперболоидов).

При переходе в диапазон длинных волн, что допустимо с точки зрения характера использования роев (групп) БПЛА в зоне прямой радиовидимости, измерение Δt может проводится на основании регистрации сдвига фазы между гармоническими колебаниями. Такие колебания допустимо использовать для управления БПЛА, так как реальное число исполняемых команд невелико и, следовательно, пропускная способность канала связи, по которому осуществляется их передача, может быть сделана низкой (вплоть до десятков бит в секунду). Соответственно, передача команд может осуществляться с использованием максимально простого сигнала, представляющего собой радиоимпульсы, отвечающие двоичному коду.

Применение такого подхода, однако, сталкивается с определенными трудностями, в том случае, когда сигнал перестает быть гармоническим (что может быть связано, например, с попытками радиотехнического воздействия, осуществляемыми противоборствующей стороной). Следовательно, при использовании рассматриваемого метода защиты информации требуется также учесть возможность отклонения сигнала от гармонического. Данную задачу, в принципе, позволяют решить такие методы как Expectation-Maximization [97], Synchro-Reassigning Transform [98], улучшающий традиционные методы анализа временно-частотного спектра, такие как вейвлет-преобразование и преобразование Габора, или Optimal Time-Frequency Distribution [99], использующий адаптивное временно-частотное разложение, и обеспечивающий лучшую точность по сравнению с классическими методами, такими как преобразование Вигнера-Вилля или Чой-Вильямса, и т.д. Однако при переходе к диапазону длинных волн использование таких методов не является оптимальным, особенно в том случае, когда необходимо только идентифицировать отклонение сигнала от гармонического.

Дополнительно отметим, что многие БПЛА, реально используемые на линии боевого соприкосновения, по степени сложности конструкции ненамного отличаются от систем, создаваемых в авиамодельных кружках, и далеко не случайно волонтёрская поддержка часто выражается в разработке/закупке/переоборудовании БПЛА силами малых коллективов, в том числе, сформированных на добровольной основе.

С точки зрения теории инноваций и экономике это, прежде всего, означает, что трансформации ОПК, обусловленные текущей революцией в военном деле, вполне могут задействовать потенциал малого и среднего бизнеса. Как вытекает из самых общих положений экономической теории, это позволит существенно повысить эффективность внедрения новых разработок, главным образом, скорость внедрения. Этот фактор является весьма важным, в том числе, и с точки зрения разработки наземных роботизированных вооружений, в том числе нелетальных.

1.4. Метод защиты информации, основанный на определении местоположения оператора

Излучение радиодиапазона представляет собой такие же электромагнитные волны, что и свет. Однако, различие в длине волны приводит к качественным различиям. В частности, человеческий глаз можно достаточно уверенно распознать положение источника сигнала. Поэтому в оптическом диапазоне можно реализовывать каналы передачи данных, защищенные по принципу определения местоположения источника сигнала. Это наглядно иллюстрирует рисунок 1.6.

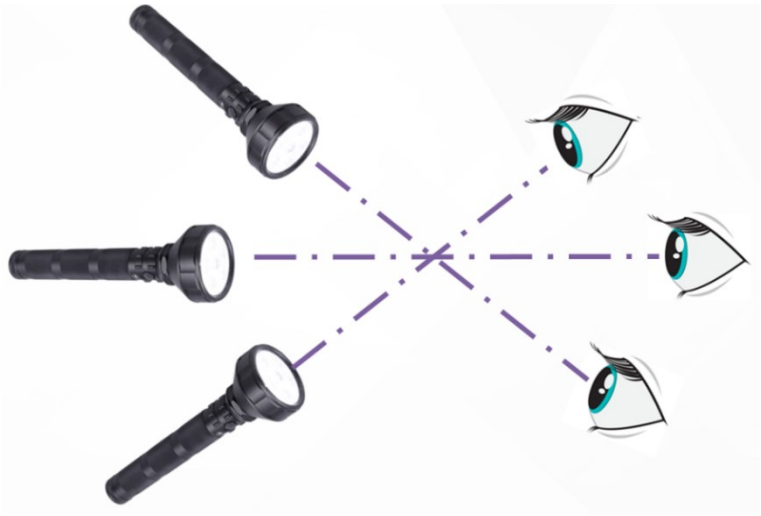


Рисунок 1.6 – Наглядная иллюстрация к формированию защищенных каналов связи в зоне прямой радиовидимости [93]

Каждый из источников света передает сообщения. Соответственно, каждый из них формирует свой канал связи, вмешаться в работу которого сторонними воздействиями практически невозможно. Сообщения можно перехватить и расшифровать, но активное воздействие оказать нельзя: адресат идентифицирует источник сообщений по месту его расположения.

В этом и состоит принципиальное отличие методов передачи информации, где задействовано распределение поля в пространстве, от методов передачи информации, где де-факто используется регистрация электромагнитного поля только в одной точке пространства. Для радиоприемника, построенного по классической схеме, источники радиоволн, находящиеся в различных точках пространства, неразличимы.

Разумеется, задачи такого рода могут быть решены и теми методами, которые используются в радиопеленгации, но рассматриваемые методы позволяют подойти к этому вопросу системно. Покажем это на примере конкретной системы, применимой к созданию защищенных каналов передачи данных.

Самый простой способ обеспечить защиту информации при использовании подхода, проиллюстрированного рисунком 1.6, состоит в том, чтобы тем или иным способом синтезировать аналог линзы, сфокусированной

на ту точку, в которой находится источник электромагнитных волн. Фокусное расстояние такой линзы и ориентация ее оси должны быть при этом, разумеется, перестраиваемыми.

Реализовывать подобную линзу физически нет никакого смысла – она будет иметь слишком большие габариты. Однако пользуясь результатами, полученными в [93,94], а также аналогией с Фурье-оптикой [100], можно предложить виртуальную линзу, построенную на преобразовании спектров сигналов в полях Галуа, которая будет решать ту же самую задачу.

Основная идея состоит в следующем.

Как показано в работах [101,102] для восстановления поля электромагнитной волны, обладающей ограниченным спектром пространственных частот, достаточно регистрировать только значения амплитуды поля в отдельных точках пространства.

В цитированных работах было показано, что если исключить из рассмотрения неоднородные волны, которые являются затухающими, то тогда классический принцип Гюйгенса-Френеля может быть приведён к дискретной форме. А именно, классический принцип Гюйгенса-Френеля предполагает, что волновой фронт излучения, распространяющегося в пространстве, можно получить, рассматривая совокупность вторичных источников, расположенных на уже сформированном волновом фронте. Это построение многократно отражено в том числе и в учебной литературе, где в том числе подчеркивается, что вторичные источники колебаний распределены по рассматриваемому волновому фронту непрерывно.

Результаты цитированных работ, в которых в том числе был доказан обобщенный вариант теоремы Котельникова, позволяют утверждать, что в действительности можно рассматривать не вторичные источники, которые распределены непрерывно, но источники, находящиеся во вполне определенных дискретных точках. Тем самым, в рассматриваемом случае допустимо говорить о дискретной форме принципа Гюйгенса-Френеля [101,102]. Более точно допустимо говорить о том, что распространение волны в рассматриваемом случае может быть сведено к указанию комплексных амплитуд поля в узлах решетки с периодом, равным половине длины волны [101,102]. На данной основе в [102] было показано, что любой преобразователь электромагнитного излучения также может быть приведён к дискретной форме.

А именно, какова бы ни была природа этого преобразователя, как бы он ни был устроен, вместо него можно рассматривать некие точечные преобразователи, отстоящие друг от друга на половину длины волны.

Соответственно, виртуальная распределенная линза может быть организована следующим образом. Падающая волна направлена на систему регистраторов, расположенных в точках, отвечающих условиям, сформулированным в [101,102]. Каждый регистратор осуществляет преобразование, отвечающее преобразованию, выполняемому элементом линзы, далее формируется интегральный результат. Подчеркиваем, что

фокусировка может осуществляться и виртуально, т.е. вместо реального распространения в пространстве используется передача преобразованного сигнала по каналам связи, локализованным внутри системы.

Характер преобразований, выполняемых регистраторами виртуальной радиоголографической линзы, может быть установлен исходя из аналогии с описанием работы тонкой линзы в терминах Фурье-оптики [100], как это показано в нашей работе [93].

Напомним, что такое описание дается в терминах фазовой функции (функции, описывающей набег фазы при распространении изучения через элемент тонкой линзы). А именно, формула, описывающая преобразование, выполняемое линзой, выглядит следующим образом

$$u(x,y) = T(x,y)u_0(x,y) \tag{1.1}$$

где $u_0(x,y)$ – распределение поля во «входной» плоскости тонкой линзы, $T(x,y)$ – ее комплекснозначная функция пропускания, $u(x,y)$ – распределение поля в «выходной» плоскости.

Термины «выходная» и «входная» плоскости отчасти являются условными, так как в приближении тонкой линзы указанные плоскости геометрически совпадают. Они, в сущности, только подчеркивают, что преобразование, выполняемое «тонким» в оптическом смысле элементом, сводится к умножению на фазовую функцию.

Подчеркиваем, что формула (1.1) записана в общей форме, она справедлива для любого элемента, который можно рассматривать как оптически тонкий (приближение параксиальной оптики). В частности, данная формула описывает также функционирование голографических элементов, работающих с использованием дифракционных эффектов.

Конкретизация формулы (1.1) для элементов, аналогичных линзе, т.е. представляющих собой некоторое тело, выполненное из оптически прозрачного материала, имеет следующий вид

$$u(x,y) = \exp\left[ikD(x,y)\right]u_0(x,y) \tag{1.2}$$

где $k = \frac{2\pi}{\lambda}$ – волновое число, $D(x,y)$ – функция оптической толщины.

Функция оптической толщины численно равна толщине элемента, выполненного из однородного материала в точке с координатами (x,y), т.е. это длина отрезка, лежащего внутри элемента, проходящего через точку (x,y) и лежащего на прямой, перпендикулярной оптической оси.

Для линзы данная функция может быть записана как [100]

$$D(x,y) = a_{11}x^2 + 2a_{12}xy + a_{22}y^2 + b_1x + b_2y \tag{1.3}$$

Именно такой вид функции оптической толщины позволяет наглядно продемонстрировать, что описание в терминах «тонких» оптических элементов, т.е. описание, при котором реальный элемент заменяется на фазовую функцию, действительно позволяет показать, что «голографическое» описание дает тот же самый результат, что и геометрическая оптика.

Это соответствие является весьма существенным для целей данной работы. А именно, оно подчёркивает, что уже существуют методы нетривиального синтеза таких оптических преобразователей как линза. В частности, ее голографическим аналогом является зонная пластинка Френеля, которая также описывается формулами (1.2) и (1.3).

Более того, такой синтез осуществляется только через набег фазы. Следовательно, общую блок-схему виртуальной радиоголографической линзы можно представить следующим образом (рисунок 1.7).

Данная схема использует тот неоднократно отмеченный в литературе факт, что методы радиоголографии (равно как и акустической голографии) в отличие от оптической могут применять системы, обеспечивающие непосредственное измерение фазы колебания [103,104].

В состав блок-схемы (рисунок 1.7) входят приемники излучения 1, фазовращатели 2, а также сумматор 3. Существенно, что изменение сдвига фазы должно быть настраиваемым. Соответственно, в рассматриваемую схему входит блок управления 4, который настраивает значение фазы, отвечающей настраиваемому фокусному расстоянию линзы, а также ее поворотов в пространстве.

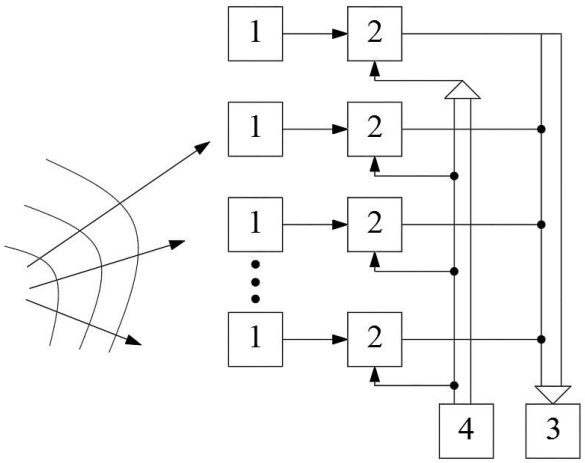


Рисунок 1.7 – Блок-схема виртуальной радиоголографической линзы

Можно видеть, что такая схема действительно является полным аналогом схемы работы линзы, отражаемой формулами (1.2) и (1.3) с той разницей, что преобразованию подвергается не фаза сигнала (точнее, распределения поля), формирующегося в некоторой плоскости, но фазы сигналов, отвечающих отдельным точкам.

Рассмотрим для наглядности конкретный вариант реализации такого подхода, отраженный в нашей работе [94].

1.5. Пример реализации квазиоптической системы защиты информации

Простейший вариант схемы защиты управляющего сигнала, основанный на рассматриваемом принципе, представлен на рисунке 1.8.

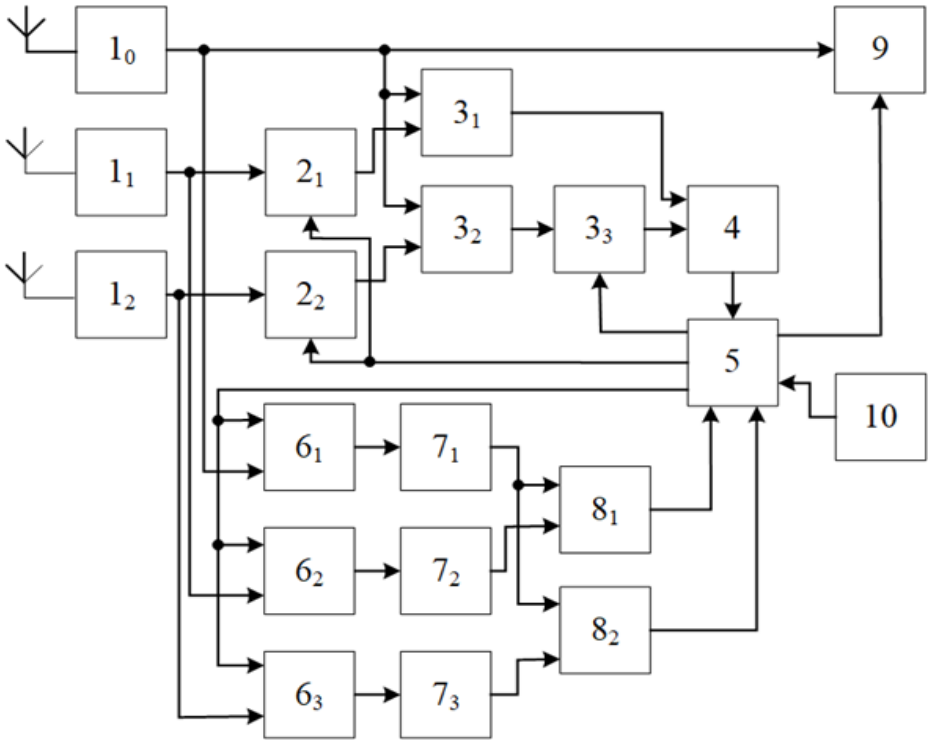


Рисунок 1.8 – Простейший вариант схемы защиты управляющего сигнала беспилотного аппарата

Внутри беспилотного аппарата располагается несколько приемников радиоволн. Будем считать, что их пространственные координаты есть r_i. Обозначим радиус вектор точки, в которой находится передатчик, через R_0.

Тогда сигналы, воспринимаемые приемниками, в скалярном приближении могут быть записаны как

$$J_i = A(R_0 - r_i) f(\omega t - k|R_0 - r_i|) \qquad (1.4)$$

где A – амплитудный множитель, зависящий только от модуля разности координат, f – амплитудно-фазовая функция, которая одновременно описывает и изменение фазы волны при ее распространении в пространстве, и изменение сигнала, вносимое модулятором передатчика, ω – круговая частота, k – волновое число (данные параметры отвечают несущей частоте, на которой работает передатчик).

Рассмотрим разность $J_i - J_j$, предполагая, что выполняется $|R_0| \gg |r_i|$. Тогда в пределах области, занимаемой беспилотным аппаратом, множитель A можно считать постоянным и записать

$$J_i - J_j \sim f(\omega t - \varphi_i) - f\left(\omega t - \varphi_j\right) \tag{1.5}$$

Будем также считать, что выполняется неравенство $\lambda \gg \left|r_i - r_j\right|$ для любых i, j. Такой выбор можно реализовать на практике, выбирая соответствующие длины волн или геометрию расположения приемников. В данном случае от разности (1.5) можно перейти к производной и записать

$$J_i - J_j \approx \left(\varphi_i - \varphi_j\right) \frac{d}{dt} f \tag{1.6}$$

Пользуясь разложением скалярной функции $|R_0 - r_i|$ в ряд Тейлора, получаем

$$\varphi_i - \varphi_j \approx -\frac{k}{k_0} R_0 (r_i - r_j) \tag{1.7}$$

Соотношения (1.6) и (1.7), в частности, показывает, что при выполнении условия $\lambda \gg |r_i - r_j|$ регистрация разности колебаний, поступающих на различные приемники, будет давать одну и ту же функцию, отличающуюся только множителем, который де-факто становится амплитудным.

Это можно выразить явной формулой, поставляя (1.7) в (1.6)

$$J_i - J_j \approx -k \frac{R_0}{R_0} (r_i - r_j) \frac{d}{dt} f \tag{1.8}$$

Непосредственно из формулы (1.8) и вытекает предлагаемый принцип действия защиты канала управления беспилотным аппаратом (точнее, его простейшая разновидность).

При условии, что известен единичный вектор $\frac{R_0}{R_0}$, задающий направление на передатчик, а также вектора r_i, коэффициент пропорциональности B в формуле (1.8) также известен.

$$B = k \frac{R_0}{R_0} (r_i - r_j) \tag{1.9}$$

Разбивая приемники излучения на пары, и используя дифференциальные усилители, можно получить сигналы, отличающиеся только постоянным заранее известным множителем (1.9).

Следовательно, защита информации обеспечивается следующим приемом. Если сигнал поступает из санкционированного источника, то сигналы, снимаемые с выходов дифференциальных усилителей, при сделанных предположениях должны отличаться друг от друга только

множителем вида (1.9), который предсказывается вычислительными средствами. Если сигнал поступает от несанкционированного источника, то он не выдерживает соответствующую проверку и в простейшем случае может быть проигнорирован.

Простейшая разновидность схемы, реализующей подобный подход (рисунок 1.8), содержит три приемника радиоволн, разнесенных в пространстве так, что выполняется условие $\lambda \gg |r_i - r_j|$.

Сигналы с приемных антенн поступают на предварительные усилители 1_i, которые также выполняют функции согласования. Сигналы с выходов усилителей 1_1 и 1_2 поступают на входы корректирующих усилителей 2_1 и 2_2, обеспечивающие подстройку коэффициента усиления с тем, чтобы исключить факторы связанные, в частности, с технологическим разбросом изготовления радиодеталей. Назначение корректирующих усилителей состоит в том, чтобы на выходе усилителя 1_0, а также усилителей 2_1 и 2_2, формировались строго одинаковые сигналы при условии, что на все три приемные антенны поступает одна и та же радиоволна.

Далее рассматриваемые сигналы разбиваются на две пары. Сигналы, отвечающие этим двум парам, поступают на входы дифференциальных усилителей 3_1 и 3_2, которые при сделанных предположениях и выполняют операцию дифференцирования, т.е. позволяют получить результат, отвечающий формуле (1.6).

Сигнал с выхода одного из этих усилителей 3_2 поступает на вход еще одного корректирующего усилителя, который производит умножение на амплитудный множитель, отвечающий формуле (1.9).

В результате, если сигнал поступает из санкционированного источника, то на выходе дифференциального усилителя 4 формируется сигнал, который интерпретируется как логический ноль.

Остальные элементы схемы предназначены для того, чтобы обеспечить работу корректирующих усилителей в описанном выше режиме. Их работа обеспечивается тем, что в сигналах, поступающих от санкционированного источника, выделяются кадры, предназначенные для обеспечения коррекции. Эти кадры чередуются с кадрами, несущими информационный (управляющий) сигнал.

В промежутки времени, отвечающие кадрам, предназначенным для обеспечения коррекции, на входы электронных ключей 6_i подается открывающий сигнал с микроконтроллера 5. На вторые входы этих электронных ключей подается сигнал с предварительных усилителей 1_i. Далее сигнал с выходов ключей 6_i подается на выпрямители 7_i. Сигналы с выходов выпрямителей 7_i группируются попарно и подаются на входы дифференциальных усилителей 8_1 и 8_2, которые вырабатывают сигналы, на основании которых микроконтроллер 5 вырабатывает управляющие сигналы, подаваемые на корректирующие усилители 2_1 и 2_2. Управляющий сигнал, подаваемый на корректирующий усилитель 3_3, определяется вычислительным

путем с помощью данных, поступающих на микроконтроллер 5 с выхода системы позиционирования 10.

При идентификации источника излучения как «свой» открывающий сигнал подается на электронный ключ 9, а далее – на управляющие системы беспилотного аппарата.

Таким образом, в принципе, действительно можно реализовать некий аналог распределённой линзы, построенной на фазовращателях, расположенных на отдельных летательных аппаратах. Такой подход, однако, следует рассматривать преимущественно как иллюстративный, поскольку, как будет показано ниже, он далеко не является оптимальным.

Задачей является не реализация виртуальной линзы, но определение координат оператора. Это можно сделать гораздо более простым и эффективным способом, который рассматривается в последующих главах.

Выводы по Главе 1

На основании анализа открытых источников информации показано, что революция в военном деле, отвечающая переходу к максимально роботизированным боевым действиям, де-факто уже состоялась. Основным трендом в обозримом будущем беспилотных систем вооружений любых типов станет снижение их стоимости, в том числе, затрат на обеспечение защиты каналов передачи информации. Существует определенная диспропорция между развитием летательных и наземных беспилотных аппаратов. Ее преодоление также станет одним из основных трендов в развитии роботизированных вооружений, причем весьма важным здесь становится реализация гибридных групп роботизированных вооружений.

Анализ открытых источников информации также показывает, что для обеспечения защиты информации, передаваемой от оператора к БПЛА или группе БПЛА, требуется развивать нетривиальные подходы.

Совершенствование средств радиоэлектронной борьбы приводит к тому, что управление с использованием шифросистем становится все менее эффективным, особенно если принять во внимание человеческий фактор, а также насыщенность линий боевого соприкосновения БПЛА.

Есть все основания полагать, что для обеспечения эффективной защиты информации требуется развивать нетривиальные методы, в том числе основанные не на шифросистемах, но на использовании тех или иных физических принципов.

Глава 2. Метод физической защиты информации при передаче команд группе БПЛА при помощи оптоволоконной связи внутри группы

В данной главе показан, что метод, предложенный нами ранее в [93,94], допускает модернизацию при переходе к использованию оптоволоконной связи между БПЛА, входящими в состав роя (группы).

Данный метод, подчеркнем еще раз, предназначен для использования в зоне прямой радиовидимости и основан на определении координат источника. Аналогом является «метод гипербол», описываемый, в частности, в [96], который основывается на измерении разности времени распространения сигнала от источника до двух пар фиксированных точек пространства, в которых расположены приемники. Отличие состоит в том, что используется единственный источник радиосигнала, формирующий исполняемые команды, а обмен информацией между приемниками сигнала, разнесенными в пространстве, осуществляется по оптоволокну.

2.1. Метод защиты информации при использовании оптоволоконной связи между БПЛА

Схема реализации метода представлена на рисунке 2.1. На данной схеме показано минимальное число БПЛА (три), обеспечивающее реализацию предложенного метода. Три используемых БПЛА формируют две пары (аппараты с номерами 1 и 2 и аппараты с номерами 2 и 3). Для каждой из этих пар регистрируется разность времени распространения сигнала от общего источника до приемников, расположенных на БПЛА Δt_{12} и Δt_{23}. При условии, что задача может быть редуцирована к задаче на плоскости (координата по высоте не принимается во внимание), измерение Δt_{12} отвечает идентификации кривой (гиперболы), описываемой уравнением

$$r_1 - r_2 = c\Delta t_{ij} \tag{2.1}$$

где $r_{1,2} = \sqrt{\left(\vec{r} - \vec{r}_{10,20}\right)^2}$, $\vec{r}_{10,20}$ – радиус-вектора приемников радиосигнала, $\vec{r} = (x, y)$ – текущий радиус-вектор, c – скорость света, Δt_{ij} – разность между временем распространения сигнала от источника до БПЛА с номером i и номером j.

Использование двух пар приемников отвечает использованию двух уравнений вида (2.1), т.е. координаты источника сигнала могут быть определены как точка пересечения двух кривых, задаваемых уравнениями рассматриваемого вида, что соответствует также методу, отраженному в таких работах как [96]. С точки зрения радиоэлектронной борьбы, уязвимости могут возникать, в том числе, при формировании каналов связи между БПЛА, входящими в состав рассматриваемой группы. Использование оптоволоконной связи минимизирует соответствующие риски. Более того, в данном случае возникают дополнительные возможности для обеспечения

синхронизации между вычислительными блоками БПЛА, определяющими значения Δt_{12} и Δt_{23}.

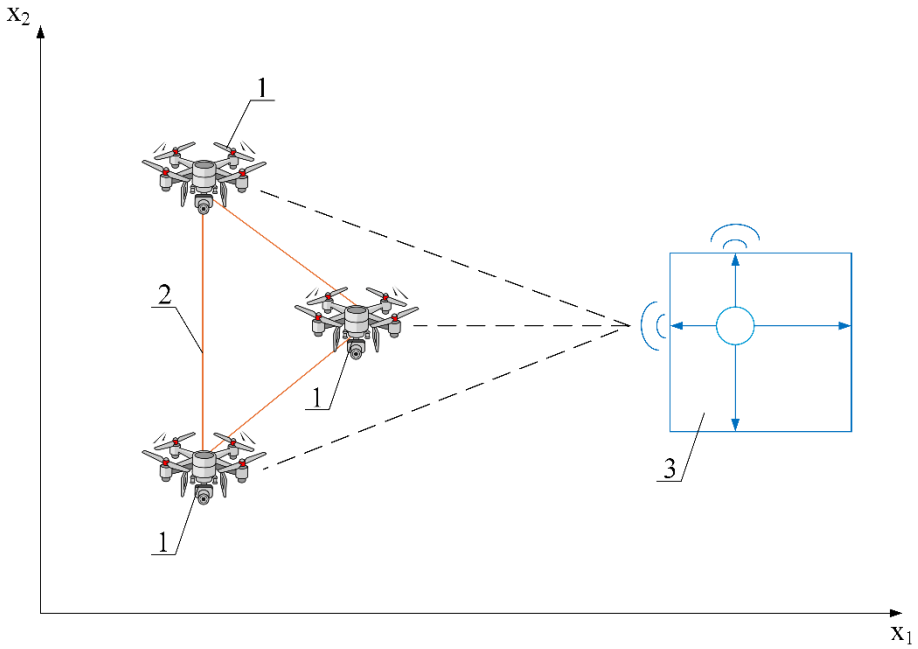


Рисунок 2.1 – Схема реализации метода защиты информации при использовании оптоволоконной связи внутри группы: 1, 2, 3 – дроны; формирующие пары; 4 – оптоволоконная линия связи; 5 – источник радиосигнала.

Следовательно, задача по обеспечению защиты информации при помощи предлагаемого метода распадается на три:

- разработка метода определения величин Δt_{ij};
- разработка алгоритма расчета положения источника сигнала на основании измеренных величин Δt_{ij}.
- аппаратная реализация предложенного алгоритма.

Решение первой из указанных выше задач существенно зависит от специфики используемого радиодиапазона. В настоящее время для управления БПЛА используется диапазон, отвечающий достаточно коротким волнам 2,4 ГГц [105]. Это не является обязательным, особенно в том случае, когда предусматривается передача на достаточно короткие расстояния (в пределах прямой радиовидимости). В частности, это означает, что можно использовать весьма слабые источники сигнала, что исключает необходимость соблюдения требований по наличии лицензии на использование данного диапазона частот. Необходимо также принимать во внимание, что число команд, реально передаваемых от оператора к БПЛА, является ограниченным [106,107]. Следовательно, при передаче данных от оператора к БПЛА можно использовать каналы связи, обладающие сравнительно низкой пропускной способностью. Это является

дополнительным аргументом в пользу использования диапазона сравнительно длинных радиоволн при управлении БПЛА в зоне прямой радиовидимости.

В простейшем случае допустимо использовать двоичный код, сформированный радиоимпульсами на определенной, причем сравнительно низкой частоте. (Отыскание конкретного диапазона частот осуществляется на основании решения рассматриваемой ниже геометрической задачи.) Это, в частности, означает, что при определенных условиях (они определяются ниже) параметры Δt_{12} и Δt_{23} могут быть определены на основании детектирования сдвига фазы гармонического сигнала.

Данный вывод позволяет предложить следующую блок-схему, обеспечивающую реализацию предложенного подхода (рисунок 2.2).

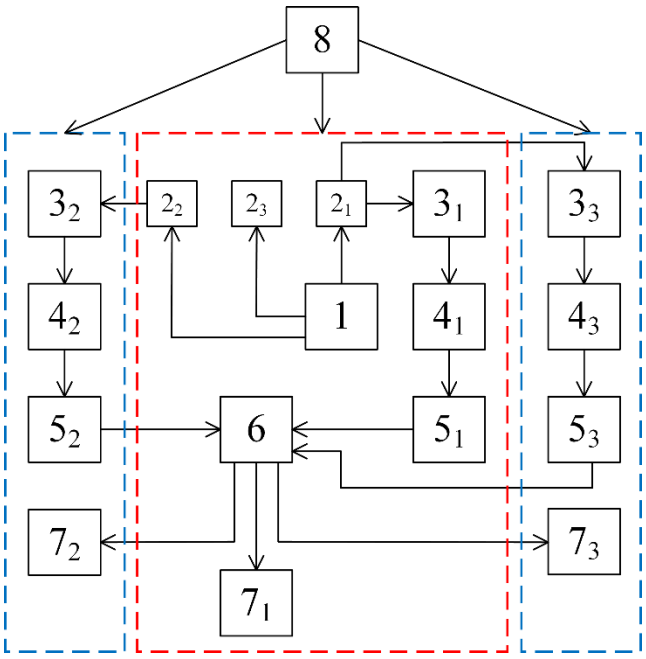


Рисунок 2.2 – Блок-схема бортовых систем группы трех БПЛА, предназначенных для определения координат источника радиосигнала

Данная блок-схема включает в себя:
- блок синхронизации (1)
- блоки формирования задержек по времени ($2_{1\text{-}3}$);
- приемники радиосигнала ($3_{1\text{-}3}$)
- блоки регистрации/вычисления фазы ($4_{1\text{-}3}$)
- блоки кратковременной памяти ($5_{1\text{-}3}$);
- вычислительный блок (6), сигналы от которого подаются на блоки ($7_{1\text{-}3}$), обеспечивающие исполнение команд.

Номером 8 на рисунке 2.2 показан источник радиосигнала. Пунктирными линиями выделены элементы схемы, относящиеся к различным БПЛА.

При использовании данной схемы ось времени разбивается на отдельные кадры, в течение которых блоки ($4_{1\text{-}3}$) осуществляют регистрацию фазы сигнала, поступающего с приемников ($3_{1\text{-}3}$). Данные значения жестко привязываются к определенному кадру, причем при идентификации каждого кадра принимается во внимание задержка сигнала, возникающая при передаче информации по оптоволокну. Синхронизацию обеспечивают блок (1) и блоки ($2_{1\text{-}3}$).

Значения фазы с блоков ($4_{1\text{-}3}$) поступают на блоки ($5_{1\text{-}3}$), где осуществляется их временное хранение, а также привязка к определенному кадру. Далее они поступают на блок (6). Подчеркиваем, что на него также поступают значения фазы, полученные регистраторами всех трех БПЛА. Эти значения привязаны к определенному кадру, что позволяет вычислить местоположение источника радиосигнала в момент времени, отвечающий указанному кадру. При таком подходе, разумеется, возникает дополнительная задержка по времени, но она заведомо не превосходит нескольких десятков миллисекунд (время, затрачиваемое на проведение вычислений), что не является существенным с точки зрения формирования команд даже при скорости движения БПЛА со скоростью до сотни километров в час.

Можно видеть, что реализация данного метода, как и в случае, рассмотренном в [96], сводится к решению геометрической задачи, т.е. к отысканию точки пересечения гипербол (если речь идет о задаче на плоскости) или гиперболоидов (если решается пространственная задача). Для решения подобных задач развиты различные методы [108-110], в том числе, в [96] предложен вариант точного решения системы гиперболических уравнений. Такой вариант, однако, является далеко не оптимальным с точки зрения эффективности использования бортовых вычислительных систем БПЛА. Нами предлагается альтернативный вариант, основанный на использовании асимптотик гипербол и специфическом выборе системы координат.

2.2. Выбор системы координат

Система координат выбирается из условия, чтобы все три БПЛА (минимальное число, необходимое для определения местоположения источника сигнала) рассматривались с единообразных позиций. Для выполнения этого условия в качестве начала координат целесообразно выбрать центр окружности, которая проходит через три точки на плоскости, отвечающие координатам БПЛА. Выбор такой окружности представляет собой элементарную тригонометрическую задачу, однако, в силу ее важности рассмотрим соответствующее построение подробно.

Три пары точек $(x_1, y_1), (x_2, y_2)$ и (x_3, y_3) лежат на одной и той же окружности радиуса ρ_0 когда выполняются следующие соотношения.

$$(x_1 - x_0)^2 + (y_1 - y_0)^2 = \rho_0^2$$

$$(x_2 - x_0)^2 + (y_2 - y_0)^2 = \rho_0^2$$

$$(x_3 - x_0)^2 + (y_3 - y_0)^2 = \rho_0^2 \quad (2.2)$$

где (x_0, y_0) – искомые координаты центра окружности.

В действительности данная задача приводится к линейной. Чтобы показать это, раскроем в уравнениях (2.2) скобки. Имеем:

$$2x_1x_0 + 2y_1y_0 = R_1^2 + R_0^2 - \rho_0^2$$

$$2x_2x_0 + 2y_2y_0 = R_2^2 + R_0^2 - \rho_0^2 \quad (2.3)$$

$$2x_3x_0 + 2y_3y_0 = R_3^2 + R_0^2 - \rho_0^2$$

где $R_i^2 = x_i^2 + y_i^2$

Вычитая второе из уравнений (2.3) из первого и третьего, получаем

$$2(x_1 - x_2)x_0 + 2(y_1 - y_2)y_0 = R_1^2 - R_2^2 \quad (2.4)$$

$$2(x_3 - x_2)x_0 + 2(y_3 - y_2)y_0 = R_3^2 - R_2^2 \quad (2.5)$$

Видно, что уравнения (2.4) и (2.5) действительно представляют собой систему линейных уравнений, которая позволяет вычислить координаты центра окружности и далее перейти к указанной выше системе отсчёта. Значение радиуса рассматриваемой окружности при этом вычисляется как

$$\rho_0^2 = x_3^2 + x_0^2 + y_3^2 + y_0^2 - 2x_3x_0 + 2y_3y_0 \quad (2.6)$$

Отметим, что уравнения (2.4) и (2.5) отвечают хорошо известному геометрическому построению, которое позволяет отыскать центр окружности, проходящей через заданные три точки (рисунок 2.3). А именно, пусть заданы три точки A, B и C. Построим отрезки AB и BC и проведем к ним перпендикуляры, проходящие через центры данных Отрезков (точки K и T, соответственно). Точки, лежащие на перпендикуляре к отрезку AB, проходящему через точку K, будут равноудалены от точек A и B. Аналогично для перпендикуляра, проходящего через точку T. Следовательно, для точки O, которая лежит на пересечении данных перпендикуляров выполняется AO = OB и OC = OB. Откуда вытекает, что расстояние от точки O до всех трех точек A, B и C одинаково, т.е. точка O действительно является центром искомой окружности.

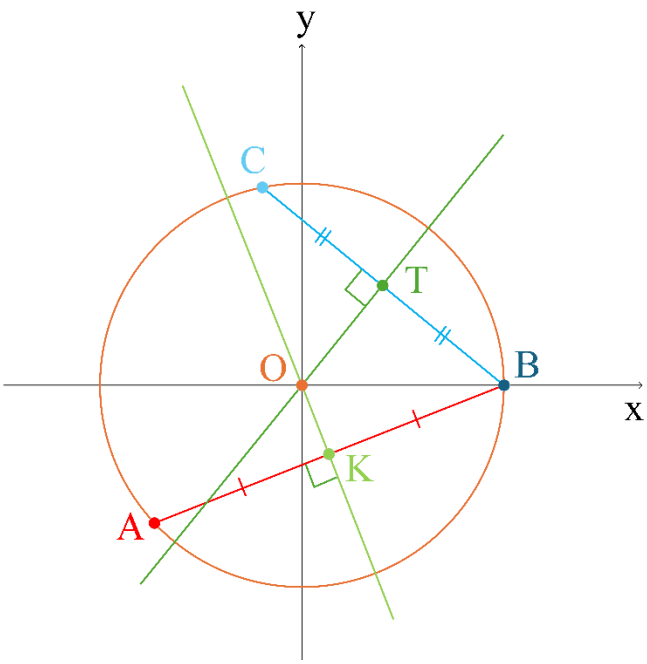


Рисунок 2.3 – К выбору используемой системы координат

Можно видеть, что это построение действительно отвечает формулам (2.4) и (2.5), так как выражение для нормали к отрезку, соединяющему пары точек $(x_1, y_1), (x_2, y_2)$ и $(x_3, y_3), (x_2, y_2)$ даются следующими выражениями.

$$\vec{n}_{1,2} = (x_1 - x_2, y_1 - y_2);\ \vec{n}_{3,2} = (x_3 - x_2, y_3 - y_2) \tag{2.7}$$

Далее все вычисления будут проводиться в предположении, что все вектора приведены к системе отсчета рассматриваемого типа, т.е. в системе отсчета, начало координат в которой совпадает с центром окружности, проходящей через точки, отвечающие положению трех рассматриваемых БПЛА.

С точки зрения геометрии, рассматриваемая задача сводится к отысканию пересечения гипербол, каждая из которых порождается данными, получаемыми отдельной парой БПЛА. Действительно, разность фаз $\Delta\phi$ связана с разностью расстояний от источника сигнала до точек, в которых расположены БПЛА с номерами 1 и 2 следующей формулой

$$r_1 - r_2 = cT\frac{\Delta\phi}{2\pi} = R \tag{2.8}$$

где $r_{1,2} = \sqrt{\left(\vec{r} - \vec{r}_{10,20}\right)^2}$, $\vec{r}_{10,20}$ – радиус-вектора приемников радиосигнала, $\vec{r} = (x, y)$ – текущий радиус-вектор, c – скорость света, T – период используемого сигнала. При этом существенно, что в силу специфики рассматриваемой задачи все рассматриваемые вектора можно считать заданными на плоскости.

Подчеркиваем, что уравнение (2.8) при использовании текущего радиус-вектора представляет собой уравнение гиперболы, т.е. одна пара БПЛА позволяет задать одну гиперболу (состоящую из двух ветвей). Вторая пара БПЛА позволяет построить еще одну гиперболу, точка пересечения которых и отвечает местоположению источника радиосигнала.

Приведем уравнение (2.8) к полярным координатам, отвечающим выбранному началу координат. Для того, чтобы устранить корни квадратные из уравнения (2.8), возведем его правую и левую часть в квадрат. Имеем

$$r_1^2 + r_2^2 - R^2 = 2r_1 r_2 \tag{2.9}$$

Снова возводя в квадрат, получаем

$$(r_1^2 + r_2^2)^2 - 2R^2(r_1^2 + r_2^2) + R^4 = 4r_1^2 r_2^2 \tag{2.10}$$

Примем во внимание, что

$$(r_1^2 + r_2^2)^2 - 4r_1^2 r_2^2 = (r_1^2 - r_2^2)^2 \tag{2.11}$$

Следовательно,

$$(r_1^2 - r_2^2)^2 - 2R^2(r_1^2 + r_2^2) + R^4 = 0 \tag{2.12}$$

Уравнение (2.12) в действительности является квадратичным, так как

$$r_1^2 - r_2^2 = -2\vec{r}\vec{r}_{10} + 2\vec{r}\vec{r}_{20} + r_{10}^2 - r_{20}^2 \tag{2.13}$$

Справедливо также соотношение

$$r_1^2 + r_2^2 = 2r^2 - 2\vec{r}\vec{r}_{10} - 2\vec{r}\vec{r}_{20} + r_{10}^2 + r_{20}^2 \tag{2.14}$$

Напомним, что в качестве начала координат выбран центр окружности, которая проходит через все три точки, отвечающие рассматриваемым БПЛА. Преимущество используемой системы координат состоит в том, что в данном случае $r_{10}^2 - r_{20}^2$ для любой пары БПЛА, т.е. в правой части соотношения (2.13) присутствует только член, линейный по $\vec{r}$. Текущий радиус-вектор, который входит в уравнение (2.14), можно записать в полярных координатах как

$$\vec{r} = \rho(\cos\varphi\,, \sin\varphi) \tag{2.15}$$

Аналогично, координаты БПЛА с номерами 1 и 2 в выбранных полярных координатах записываются как

$$\vec{r}_{10,20} = \rho_0\big(\cos\varphi_{1,2}\,, \sin\varphi_{1,2}\big) \tag{2.16}$$

Откуда

$$\vec{r}\vec{r}_{10,20} = \rho\rho_0 \cos(\varphi - \varphi_{1,2}) \quad (2.17)$$

или

$$r_1^2 - r_2^2 = -2\vec{r}\vec{r}_{10} + 2\vec{r}\vec{r}_{20} = 2\rho\rho_0[\cos(\varphi - \varphi_2) - \cos(\varphi - \varphi_1)] \quad (2.18)$$

Используя стандартные тригонометрические формулы, получаем

$$r_1^2 - r_2^2 = 4\rho\rho_0 \sin\frac{\varphi_2 - \varphi_1}{2} \sin\left(\varphi - \frac{\varphi_2 + \varphi_1}{2}\right) \quad (2.19)$$

Аналогично,

$$2\vec{r}\vec{r}_{10} + 2\vec{r}\vec{r}_{20} = 2\rho\rho_0[\cos(\varphi - \varphi_2) + \cos(\varphi - \varphi_1)] \quad (2.20)$$

Откуда

$$2\vec{r}\vec{r}_{10} + 2\vec{r}\vec{r}_{20} = 4\rho\rho_0 \cos\frac{\varphi_2 - \varphi_1}{2} \cos\left(\varphi - \frac{\varphi_2 + \varphi_1}{2}\right) \quad (2.21)$$

Используя соотношения (2.18) и (2.21), уравнение гиперболы в используемых координатах после несложных преобразований можно привести к виду.

$$(4\rho\rho_0)^2 \sin^2\frac{\varphi_2 - \varphi_1}{2} \sin^2\left(\varphi - \frac{\varphi_2 + \varphi_1}{2}\right) + 8\rho\rho_0 R^2 \cos\frac{\varphi_2 - \varphi_1}{2} \cos\left(\varphi - \frac{\varphi_2 + \varphi_1}{2}\right) - \\ -4R^2(\rho^2 + \rho_0^2) + R^4 = 0 \quad (2.22)$$

Для верификации полученного соотношения рассмотрим предельный случай, отвечающий переходу к каноническому уравнению гиперболы в полярных координатах. Для этого рассмотрим ситуацию, когда два рассматриваемых БПЛА находятся на прямой, проходящей через центр окружности, который совпадает с началом координат в выбранной системе отсчета. В этом случае допустимо положить $\varphi_1 = 0$, тогда $\varphi_2 = \pi$, т.е.

$$\sin\frac{\varphi_2 + \varphi_1}{2} = 1, \cos\frac{\varphi_2 - \varphi_1}{2} = 0 \quad (2.23)$$

Следовательно, уравнение (2.22) переходит в

$$(4\rho\rho_0)^2 \cos^2\varphi - 4R^2(\rho^2 + \rho_0^2) + R^4 = 0 \quad (2.24)$$

так как $\sin\left(\varphi - \frac{\pi}{2}\right) = -\cos\varphi$

Величины, входящие в уравнение (2.24), можно выразить через эксцентриситет гиперболы и параметр a, входящий в ее каноническое уравнение

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 \tag{2.25}$$

При этом имеют место следующие соотношения, вытекающие из классической теории конических сечений.

$$R = 2a;\ \varepsilon = \sqrt{1 + \frac{b^2}{a^2}} > 1;\ \rho_0 = \varepsilon a \tag{2.26}$$

Последнее соотношение из (2.24) справедливо в силу того, что рассматриваемые БПЛА находятся в фокусах рассматриваемых гипербол. Подставляя (2.26) в (2.24), получаем

$$\left(\frac{\rho}{a}\right)^2 (\varepsilon^2 \cos^2\varphi - 1) = \varepsilon^2 - 1 \tag{2.27}$$

Из соотношения (2.27) непосредственно вытекает каноническое уравнение для гиперболы в полярных координатах

$$\rho^2 = a^2 \frac{\varepsilon^2 - 1}{\varepsilon^2 \cos^2\varphi - 1} = \frac{b^2}{\varepsilon^2 \cos^2\varphi - 1} \tag{2.28}$$

Таким образом, полученное уравнение (2.22) отвечает рассматриваемому предельному случаю. Вернемся к общему случаю.

Перейдем к безразмерным величинам

$$q = \frac{a}{\rho_0} = \frac{R}{2\rho_0};\ s = \frac{\rho}{\rho_0} \tag{2.29}$$

Подставляя (2.29) в (2.22), получаем следующее квадратное уравнение на параметр s

$$s^2\left[\sin^2\frac{\varphi_2 - \varphi_1}{2}\sin^2\left(\varphi - \frac{\varphi_2 + \varphi_1}{2}\right) - q^2\right] + 2sq^2\cos\frac{\varphi_2 - \varphi_1}{2}\cos\left(\varphi - \frac{\varphi_2 + \varphi_1}{2}\right) - q^2 + q^4 = 0 \tag{2.30}$$

Дискриминант данного уравнения есть

$$D = 4q^4 \cos^2\frac{\varphi_2-\varphi_1}{2}\cos^2\left(\varphi-\frac{\varphi_2+\varphi_1}{2}\right) + 4q^2(1-q^2)\left[\sin^2\frac{\varphi_2-\varphi_1}{2}\sin^2\left(\varphi-\frac{\varphi_2+\varphi_1}{2}\right)-q^2\right] \quad (2.31)$$

Преобразуем соотношение (2.31), используя следующее тождество

$$\cos^2\frac{\varphi_2-\varphi_1}{2}\cos^2\left(\varphi-\frac{\varphi_2+\varphi_1}{2}\right) - \sin^2\frac{\varphi_2-\varphi_1}{2}\sin^2\left(\varphi-\frac{\varphi_2+\varphi_1}{2}\right) =$$
$$\left(1-\sin^2\frac{\varphi_2-\varphi_1}{2}\right)\cos^2\left(\varphi-\frac{\varphi_2+\varphi_1}{2}\right) - \sin^2\frac{\varphi_2-\varphi_1}{2}\sin^2\left(\varphi-\frac{\varphi_2+\varphi_1}{2}\right) =$$
$$\cos^2\left(\varphi-\frac{\varphi_2+\varphi_1}{2}\right) - \sin^2\frac{\varphi_2-\varphi_1}{2} \quad (2.32)$$

Откуда

$$\frac{D}{4q^2} = q^2\left(\cos^2\left(\varphi-\frac{\varphi_2+\varphi_1}{2}\right) - \sin^2\frac{\varphi_2-\varphi_1}{2}\right) + \sin^2\frac{\varphi_2-\varphi_1}{2}\sin^2\left(\varphi-\frac{\varphi_2+\varphi_1}{2}\right) - (1-q^2)q^2 \quad (2.33)$$

Или

$$\frac{D}{4q^2} = -q^2\left(\sin^2\left(\varphi-\frac{\varphi_2+\varphi_1}{2}\right) + \sin^2\frac{\varphi_2-\varphi_1}{2}\right) + \sin^2\frac{\varphi_2-\varphi_1}{2}\sin^2\left(\varphi-\frac{\varphi_2+\varphi_1}{2}\right) + q^4$$

$$\frac{D}{4q^2} = \sin^2\left(\varphi-\frac{\varphi_2+\varphi_1}{2}\right)\left(\sin^2\frac{\varphi_2-\varphi_1}{2}-q^2\right) - q^2\left(\sin^2\frac{\varphi_2-\varphi_1}{2}-q^2\right)$$

$$\frac{D}{4q^2} = \left(\sin^2\frac{\varphi_2-\varphi_1}{2}-q^2\right)\left(\sin^2\left(\varphi-\frac{\varphi_2+\varphi_1}{2}\right)-q^2\right) \quad (2.34)$$

Следовательно,

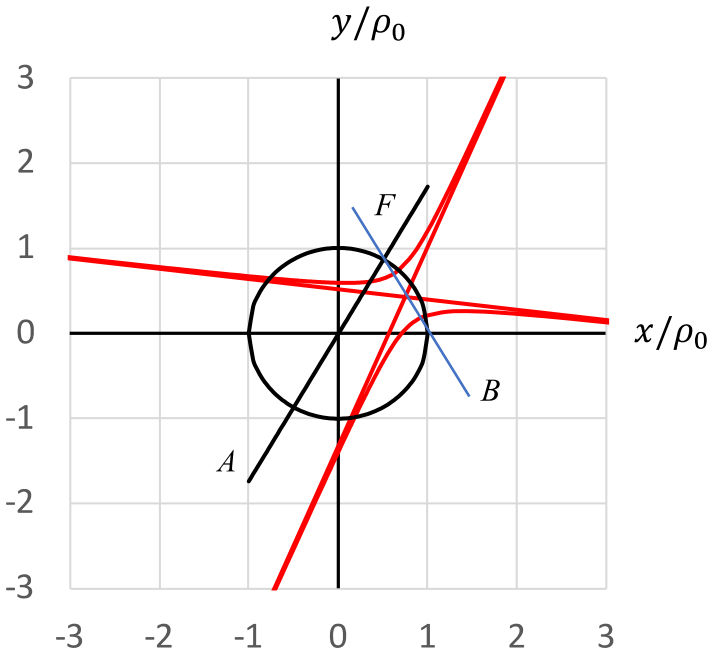
$$s_{1,2} = q\,\frac{-q\cos\frac{\varphi_2-\varphi_1}{2}\cos\left(\varphi-\frac{\varphi_2+\varphi_1}{2}\right) \pm \sqrt{\left(\sin^2\frac{\varphi_2-\varphi_1}{2}-q^2\right)\left(\sin^2\left(\varphi-\frac{\varphi_2+\varphi_1}{2}\right)-q^2\right)}}{\sin^2\frac{\varphi_2-\varphi_1}{2}\sin^2\left(\varphi-\frac{\varphi_2+\varphi_1}{2}\right)-q^2} \quad (2.35)$$

Для проверки полученного соотношения допустимо положить $\varphi_1 = 0$. Имеем

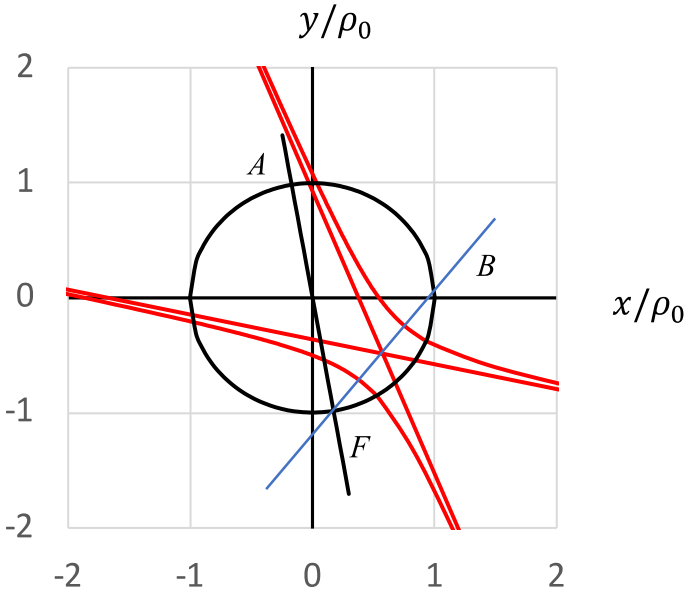
$$s_{1,2} = q\,\frac{-q\cos\frac{\varphi_2}{2}\cos\left(\varphi-\frac{\varphi_2}{2}\right) \pm \sqrt{\left(\sin^2\frac{\varphi_2}{2}-q^2\right)\left(\sin^2\left(\varphi-\frac{\varphi_2}{2}\right)-q^2\right)}}{\sin^2\frac{\varphi_2}{2}\sin^2\left(\varphi-\frac{\varphi_2}{2}\right)-q^2} \quad (2.36)$$

Примеры, полученные с использованием полученных формул, представлены на рисунке 2.4а,б. На данных рисунках показаны зависимости приведенной ординаты $\frac{y}{\rho_0} = \frac{\rho}{\rho_0}\sin\varphi$ от приведенной абсциссы $\frac{x}{\rho_0} = \frac{\rho}{\rho_0}\cos\varphi$.

Видно, что данные решения действительно отвечают гиперболам, фокусы которых расположены на окружности единичного радиуса, что отвечает переходу к безразмерным переменным по формулам (2.29).



а)



б)

Рисунок 2.4 – Примеры зависимостей приведенной ординаты $\frac{y}{\rho_0} = \frac{\rho}{\rho_0}\sin\varphi$ от приведенной абсциссы $\frac{x}{\rho_0} = \frac{\rho}{\rho_0}\cos\varphi$; $\varphi_2 = 60^0$ (а), $\varphi_2 = -80^0$ (б); AF – прямая, проходящая через центр координат, на которой расположен фокус F, B – симметричный ему второй фокус

На рисунке 2.5 показан также пример зависимости параметра s от угла φ. Как и следовало ожидать, видно, что параметр s стремится к бесконечности при приближении угла φ к значению, определяемому равенством

$$\sin^2\frac{\varphi_2}{2}\sin^2\left(\varphi-\frac{\varphi_2}{2}\right)-q^2=0 \qquad (2.37)$$

Эти значения отвечают асимптотикам полученной гиперболы.

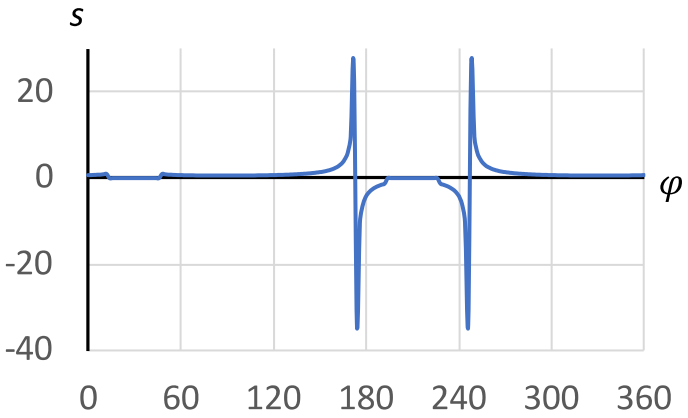


Рисунок 2.5 – Пример зависимости параметра s от угла φ; $\varphi_2 = 60^0$

Данный пример показывает, что значения $s \gtrsim 8$ могут реализовываться только при условии, что угол φ приближается к углу, задаваемому соотношением (2.37). Это, в свою очередь, означает, что для решения рассматриваемой задачи целесообразно использовать асимптотики гипербол, так как источник сигнала заведомо находится на относительно большом расстоянии от начала координат в выбранной системе отсчета. Точнее, данное расстояние существенно превышает ρ_0.

Сделанный вывод иллюстрируют рисунок 2.6, на которых показан пример, отвечающий отысканию точек пересечения двух гипербол, порождаемых двумя разностями фаз, регистрируемыми двумя парами БПЛА.

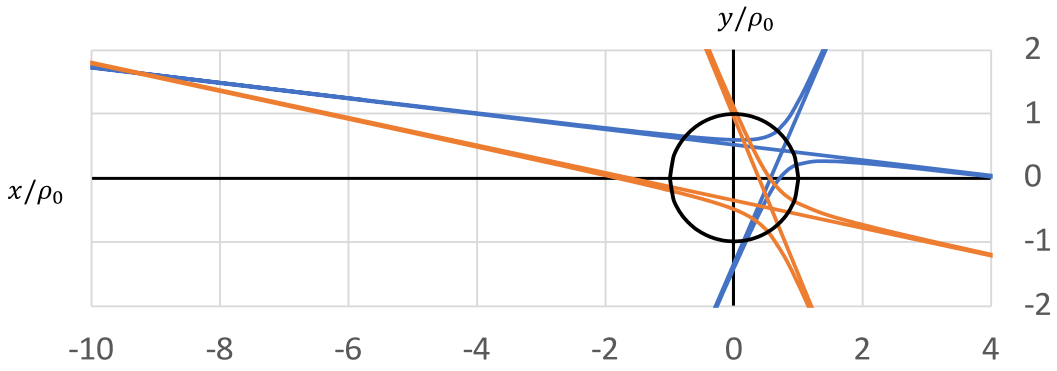
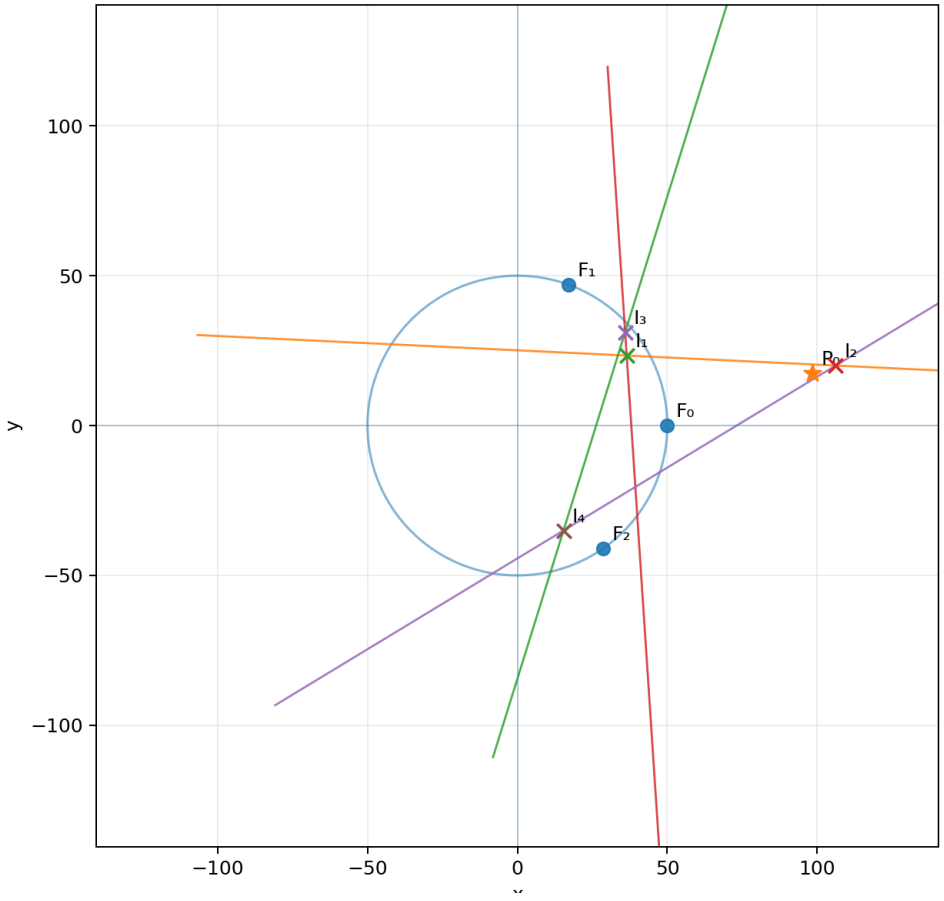


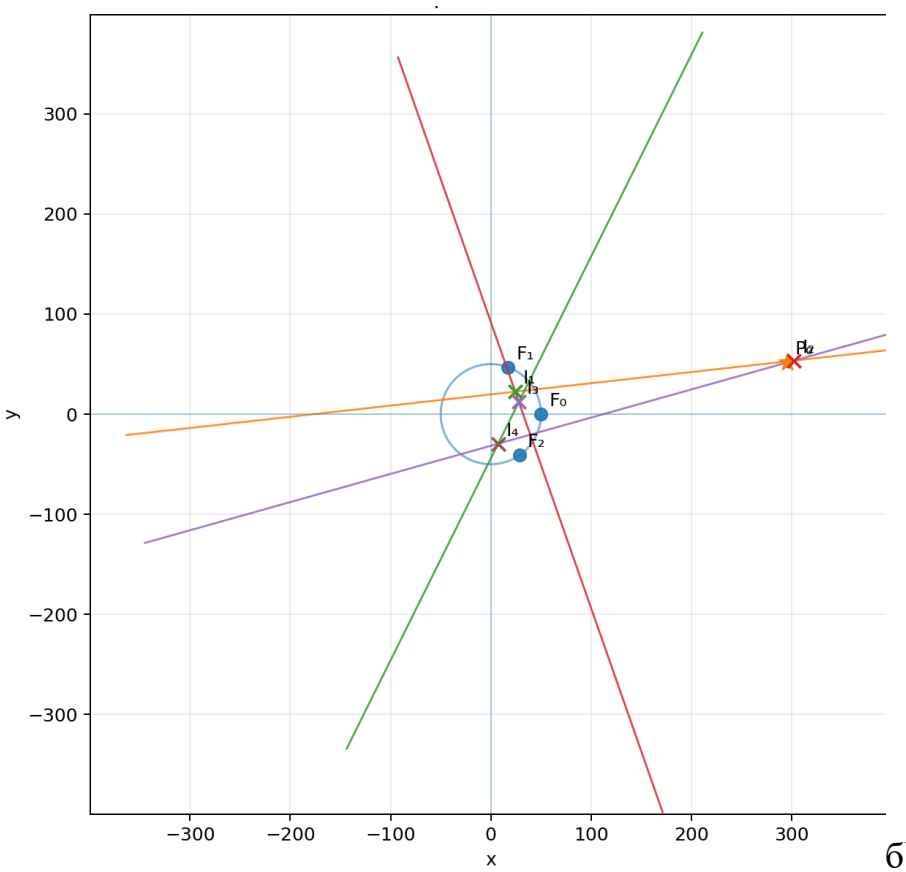
Рисунок 2.6 – Иллюстрация к отысканию точек пересечения гипербол

Данный пример качественно иллюстрирует следующий предварительный вывод, который и обеспечивает однозначность решения рассматриваемой задачи. А именно, интерес (с точки зрения определения координат источника сигнала) представляет только та точка пересечения гипербол, которая лежит за пределами окружности, используемой для построения выбранной системы координат. Для этого чтобы обосновать этот вывод количественно, будем использовать уравнение (2.12).

Аналогичный предварительный вывод подтверждается и результатами компьютерных экспериментов (используемый код приведен в Приложении В). На рисунке 2.7 представлены графики, показывающие асимптоты гиперболы и точки их пересечения при определенных условиях модели. Видно, что предложенный метод действительно позволяет определять координаты оператора с точностью, приемлемой для поставленных целей, и что точность возрастает по мере увеличения отношения (D/R), где (D) — расстояние от центра окружности, на которой расположены БПЛА, до оператора.



а)



б)

Рисунок 2.7 – Расположение точек пересечения гипербол при заданных условиях модели: а) $R = 50$, $\varphi_1 = 70°$, $\varphi_2 = -55°$, $\rho_0 = 100$, $\theta_0 = 10°$, б) $R = 50$, $\varphi_1 = 70°$, $\varphi_2 = -55°$, $\rho_0 = 300$, $\theta_0 = 10°$ (на основе результатов компьютерного эксперимента)

Вернемся к уравнению (2.12) и отыщем его асимптотическое решение, отвечающее прямой линии. Конкретно, будем искать асимптотическое решение в параметрической форме

$$\vec{r} = t\vec{e} + \frac{1}{2}(\vec{r}_{01} + \vec{r}_{02}) \tag{2.38}$$

где $\vec{r}$ – текущий радиус-вектор, t – текущий параметр, $\vec{e}$ – единичный вектор, задающий направление рассматриваемой прямой.

$$\vec{e} = (\cos\alpha\,, \sin\alpha) \tag{2.39}$$

Свободный член в уравнении (2.38) выбран из очевидных геометрических соображений: асимптотика гиперболы, отвечающей определенной паре БПЛА, должна проходить через точку, которая лежит на середине отрезка, соединяющего точки, в которых они расположены. Подставляя (2.38) в (2.13), и принимая во внимание специфику используемой системы координат ($r_{10}^2 = r_{20}^2$), получаем

$$r_1^2 - r_2^2 = -2(\vec{r}_{10} - \vec{r}_{20})\left[t\vec{e} + \frac{1}{2}(\vec{r}_{01} + \vec{r}_{02})\right] = -2t(\vec{r}_{10} - \vec{r}_{20})\vec{e} \quad (2.40)$$

Подставляя (2.38) в (2.14), и снова принимая во внимание специфику используемой системы координат ($r_{10}^2 = r_{20}^2$), получаем

$$r_1^2 + r_2^2 = 2t^2 + t\vec{e}(\vec{r}_{01} + \vec{r}_{02}) - t\vec{e}(\vec{r}_{01} + \vec{r}_{02}) + \vec{e}_c = 2t^2 + \vec{e}_c \quad (2.41)$$

Где через $\vec{e}_c$ обозначен вектор, который не зависит от t.

Подставляя (2.40) и (2.41) в уравнение (2.12), получаем

$$4t^2\left((\vec{r}_{10} - \vec{r}_{20})\vec{e}\right)^2 - 4R^2t^2 + const = 0 \quad (2.42)$$

В данном уравнении, поскольку ищется асимптотика гиперболы, допустимо приравнять нулю сумму коэффициентов при t^2. Обратим внимание, что линейный член по t в уравнении (2.42) не фигурирует, что показывает адекватность выбора искомого решения в виде (2.38). Следовательно, уравнение (2.42) фактически представляет собой уравнение на угол, задающий единичный вектор $\vec{e}$. Действительно, при отыскании асимптотики уравнение (2.42) принимает вид

$$\left((\vec{r}_{10} - \vec{r}_{20})\vec{e}\right)^2 = R^2 \quad (2.43)$$

При этом

$$(\vec{r}_{10} - \vec{r}_{20})\vec{e} = \rho_0(cos(\alpha - \varphi_1) - cos(\alpha - \varphi_2)) \quad (2.44)$$

Откуда

$$(\vec{r}_{10} - \vec{r}_{20})\vec{e} = 2\rho_0\, sin\frac{\varphi_2 - \varphi_1}{2} sin\left(\varphi - \frac{\varphi_2 + \varphi_1}{2}\right) \quad (2.45)$$

Откуда вытекает выражение для угла α, задающего направление асимптотик гиперболы в выбранной системе координат.

$$\sin^2\left(\alpha - \frac{\varphi_2 + \varphi_1}{2}\right) = \frac{R^2}{4\rho_0^2 \sin^2\frac{\varphi_2 - \varphi_1}{2}} \quad (2.46)$$

Этот результат совпадает с тем, что вытекает из формулы (2.37), так как (2.29) $q = \frac{R}{2\rho_0}$.

Он легко интерпретируется из геометрических соображений. Обратимся к рисунку 2.8, который отвечает случаю $\varphi_1 = 0$, который далее и будет рассматриваться. Это допустимо так как всего возможно осуществить поворот осей координат. На данном рисунке прямые CQ_1 и CQ_2 отвечает двум

асимптотам гиперболы, а отрезок AB соединяет точки, отвечающие положению БПЛА (вектора $\vec{r}_{01}$ и $\vec{r}_{02}$).

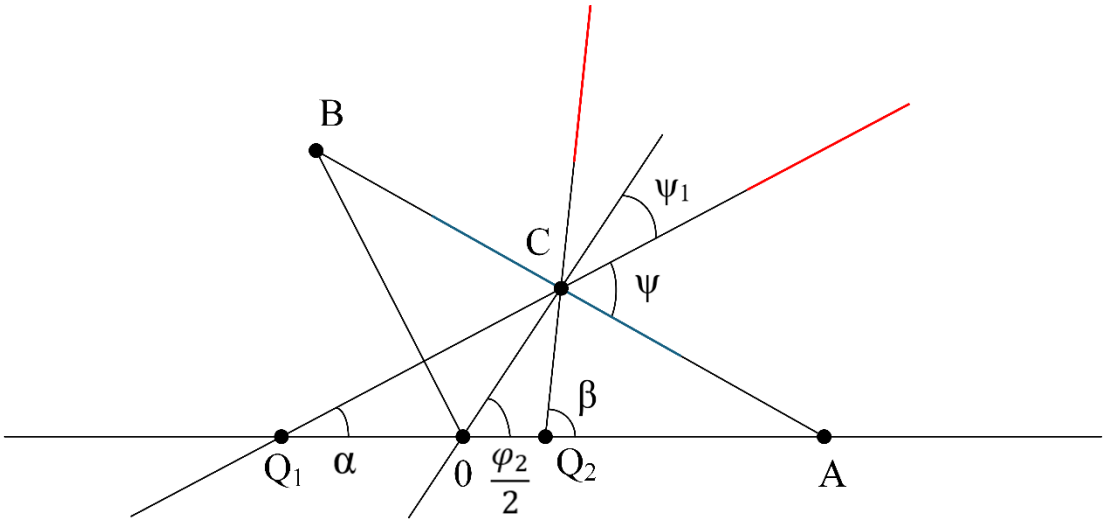


Рисунок 2.8 – К геометрической интерпретации полученных решений

Прежде всего отметим, что величина $\rho_0 \sin\frac{\varphi_2}{2}$ есть ровно половина расстояния $\Delta l_{1,2}$ между рассматриваемыми БПЛА, что, в том числе, непосредственно вытекает из рассмотрения треугольника OCA. Следовательно, формулу (2.46) для рассматриваемого случая можно записать в форме

$$\sin^2\left(\alpha - \frac{\varphi_2}{2}\right) = \frac{R^2}{\Delta l_{1,2}^2} \tag{2.47}$$

Мысленно перейдем в систему отсчета, в которой точка C является началом координат, а прямая AB совпадает с осью абсцисс. Такая система координат отвечает каноническому уравнению гиперболы (2.25), следовательно, угол ψ есть в точности угол, который будет получен, если рассматривать асимптотику канонического уравнения, т.е. угол, отвечающий прямой

$$y = \pm\frac{b}{a}x = \pm x\ tg\psi \tag{2.48}$$

Следовательно, уравнение (2.47) допустимо представить в форме

$$\sin^2\left(\alpha - \frac{\varphi_2}{2}\right) = \cos^2\psi \tag{2.49}$$

Рассмотрим треугольник CQ_1O. Для угла $\widehat{Q_1OC}$ справедливо следующее соотношение

$$\frac{\varphi_2}{2} + \widehat{Q_1OC} = \pi \tag{2.50}$$

Поскольку сумма углов любого треугольника равна π, то из (2.48) следует, что

$$\pi - \frac{\varphi_2}{2} + \alpha + \psi_1 = \pi \tag{2.51}$$

где α – угол, который задает направление одной из асимптот, в соответствии с формулой (2.39). При этом

$$\psi + \psi_1 = \frac{\pi}{2} \tag{2.52}$$

Откуда

$$\alpha = \frac{\varphi_2}{2} + \psi - \frac{\pi}{2} \tag{2.53}$$

Подставляя формулу (2.53) в выражение (2.49), можно видеть, что она отвечает одному из решений этого уравнения, так как $\sin\left(\psi - \frac{\pi}{2}\right) = -\sin\left(\frac{\pi}{2} - \psi\right) = -\cos\psi$.

Рассмотрим треугольник CQ_2O. В данном случае угол β является дополнительным к углу $\widehat{OQ_2C}$, т.е. $\widehat{Q_1OC} + \beta = \pi$. Следовательно,

$$\frac{\varphi_2}{2} + \psi_1 + \pi - \beta = \pi \tag{2.54}$$

Откуда

$$\beta = \frac{\varphi_2}{2} + \frac{\pi}{2} - \psi \tag{2.55}$$

Подставляя эту формулу в выражение (2.49), получаем, что угол, даваемый, формулой (2.55), является вторым решением полученного уравнения, так как $\sin\left(\frac{\pi}{2} - \psi\right) = \cos\psi$.

Таким образом, представленные расчеты приводят к результату, понятному из элементарных геометрических соображений. Для того, чтобы отыскать направление асимптот в выбранной системе координат, нужно провести отрезок, соединяющий БПЛА из определенной пары и отыскать его центр (точка С на рисунке 2.8). Далее нужно провести прямую, соединяющую эту точку и центр окружности (прямая ОС на рисунок 2.8). Далее нужно провести прямые, проходящие через точку С (или ее аналог), угол между которыми и прямой ОС определяется из условия $\sin^2\psi = \frac{R^2}{\Delta l_{1,2}^2}$. Положение

источника радиосигнала при этом отвечает пересечению полученных асимптот.

2.3. Обеспечение однозначности определения координат источника сигнала

Возникает немаловажный вопрос об однозначности определения координат источника сигнала при помощи предлагаемого метода. Как вытекает из соображений, которые иллюстрирует рисунок 2.9, в том случае, когда источник достаточно удален от окружности, используемой для построения выбранной системы координат, допустимо рассматривать пересечения асимптотик гипербол, т.е. пересечения четырех прямых. Если исключить из рассмотрения пересечения асимптот одной и той же гиперболы, то число точек пересечения, вообще говоря, равно четырём. Из них, следовательно, нужно выбрать ту, которая представляет интерес с точки зрения рассматриваемой задачи. Покажем, что данная задача (если отталкиваться от соображений, представляющих интерес с точки зрения практического использования) решается в общем случае.

Будем задавать асимптоты в параметрической форме.

$$\vec{r}_i = l_i\vec{e}_i + \vec{r}_{0i},\ i = 1,2,3,4 \tag{2.56}$$

где $\vec{e}_i = (\cos\alpha_i, \sin\alpha_i)$ – единичный вектор, задающий направление асимптоты, определяемый из соотношения (2.43), $\vec{r}_0$ – радиус-вектор, отвечающий точке, которая лежит на середине отрезка, соединяющего пару БПЛА, l – параметр, имеющий размерность длины, индекс i нумерует четыре прямые, показанные на рисунке 2.9.

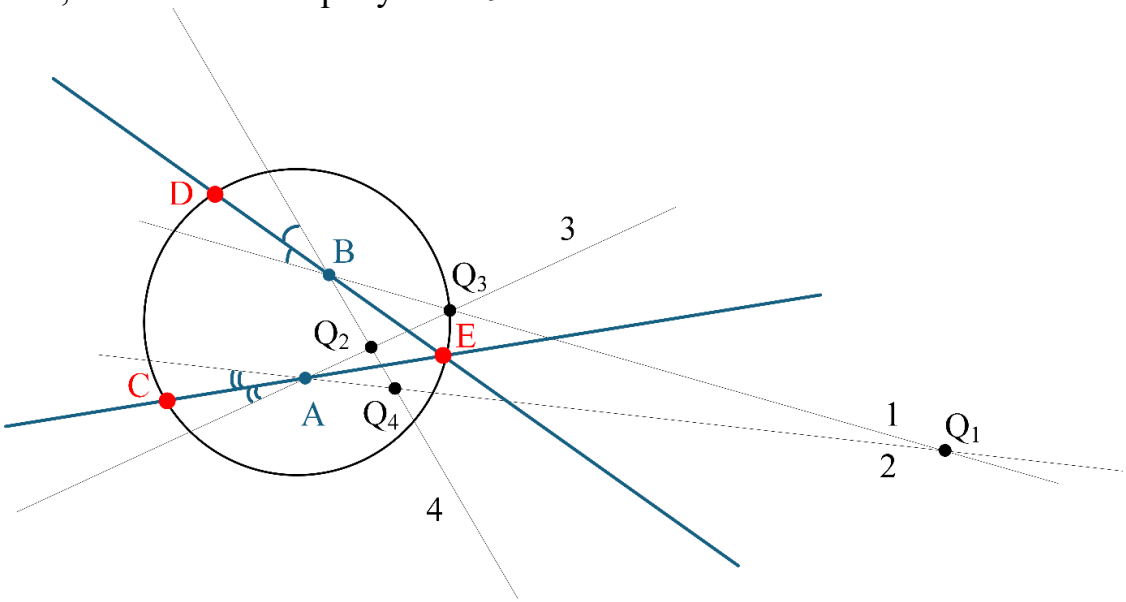


Рисунок 2.9 – К вопросу об однозначности определения координат источника сигнала методом пересекающихся асимптот гипербол

Точка пересечения двух прямых (рассматриваются прямые 1 и 2 по рисунку 2.9), соответственно, определяется из уравнений

$$0 = l_1 \cos\alpha_1 - l_2 \cos\alpha_2 + x_{10} - x_{20} \tag{2.57}$$

$$0 = l_1 \sin\alpha_1 - l_2 \sin\alpha_2 + y_{10} - y_{20} \tag{2.58}$$

где $l_{1,2}$ – значения расстояний от точки пересечения рассматриваемых прямых до точки, отвечающей $l_{1,2} = 0$. Комбинируя уравнения (2.57) и (2.58) стандартным образом, получаем

$$0 = l_1(\sin\alpha_2 \cos\alpha_1 - \sin\alpha_1 \cos\alpha_2) + (x_1 - x_2)\sin\alpha_2 - (y_1 - y_2)\cos\alpha_2 \tag{2.59}$$

Или

$$l_1 = \frac{(x_1 - x_2)\sin\alpha_2 - (y_1 - y_2)\cos\alpha_2}{\sin(\alpha_1 - \alpha_2)} \tag{2.60}$$

Вектор

$$\vec{e}_{2\perp} = (\sin\alpha_2\,, -\cos\alpha_2) \tag{2.61}$$

Ортогонален вектору $\vec{e}_2 = (\cos\alpha_2\,, \sin\alpha_2)$, задающему направление рассматриваемой асимптоты

$$\vec{e}_{2\perp}\vec{e}_2 = \sin\alpha_2 \cos\alpha_2 - \cos\alpha_2 \sin\alpha_2 = 0 \tag{2.62}$$

Следовательно, соотношение (2.60) можно записать как

$$l_1 = \frac{(\vec{r}_{01} - \vec{r}_{02})\vec{e}_{2\perp}}{\sin(\alpha_1 - \alpha_2)} \tag{2.63}$$

Аналогично,

$$l_2 = \frac{(\vec{r}_{01} - \vec{r}_{02})\vec{e}_{1\perp}}{\sin(\alpha_2 - \alpha_1)} \tag{2.64}$$

Для числителей, стоящих в правых частях формул (2.63) и (2.64) справедливо следующее неравенство

$$0 \le (\vec{r}_{01} - \vec{r}_{02})\vec{e}_{2\perp} \le \Delta l_{12} \tag{2.65}$$

где Δl_{12} – расстояние между БПЛА с номерами 1 и 2.

В частности, это означает, что когда идентифицируется местоположение источника сигнала, достаточно удаленного от окружности, формирующей выбранную систему отсчета, т.е. $l_i \gg \rho_0$, то должно иметь место

$$\alpha_2 \approx \alpha_1 \tag{2.66}$$

Выполнение приближенного равенства (2.66) означает, что направления асимптотик гипербол, отвечающих двум разным парам БПЛА, должны приближенно совпадать. По рисунку 2.8 это – прямые с номерами 1 и 2, точка их пересечения Q_1. Каждая из рассматриваемых гипербол обладает еще одной асимптотикой, прямые с номерами 3 и 4. Соответственно, имеются еще три точки пересечения асимптотик, относящихся к различным гиперболам $Q_{2\text{-}4}$. Угол между прямой 3 и прямой 1 (точка пересечения Q_3) в силу равенства (2.66) приближённо равен $2\psi_{1A}$ – удвоенному углу, который фигурирует в формуле (2.52). Аналогично угол между прямой 4 и прямой 2 (точка пересечения Q_4) приближённо равен $2\psi_{1B}$.

Из формул (2.47), (2.49) и (2.52) вытекает, что

$$\sin^2\psi = 1 - \frac{R^2}{\Delta l_{1,2}^2};\ \sin^2\psi_1 = \frac{R^2}{\Delta l_{1,2}^2} \tag{2.67}$$

Откуда

$$0 \le l_i \le \frac{\Delta l_{i,j}^2}{R} \tag{2.68}$$

Аналогичные соображения справедливы и по отношению к точке Q_2.

Полученный результат решает вопрос об однозначности отыскания источника радиосигнала, удаленного от рассматриваемой группы БПЛА более чем на $\sim 5\rho_0$. А именно, все точки, кроме Q_1, удалены от начала координат на расстояние порядка ρ_0, что, в том числе, непосредственно иллюстрирует рисунок 2.8. Следовательно, для решения поставленной задачи достаточно найти расстояния до всех четырех точек пересечения асимптот и выбрать из них наибольшее.

Этот вывод иллюстрируется результатами численного эксперимента, представленными в таблице 2.1. Видно, что, как следует из рассмотренных выше соображений, предложенный метод позволяет определять координаты оператора с приемлемой точностью при условии $D \gg R$; в частности, настоящий эксперимент показывает, что должно выполняться требование $D \geq 6R$. Эксперимент также показывает, что выбор точки пересечения должен производиться в соответствии с указанным выше критерием: следует выбирать точку пересечения, наиболее удаленную от центра окружности, на которой расположены БПЛА. Этот критерий также действителен, когда выполняется условие $D \gg R$.

Таблица 2.1 – Результаты вычисления координат четырех точек пересечения асимптот в нормированных полярных координатах $\left(\frac{\rho_k}{R}, \psi_k\right)$, где ψ_k задано в градусах, R — радиус окружности, на которой расположены БПЛА, а k — индекс точки пересечения (упорядоченный по расстоянию). Вычисления представлены для заданных наборов параметров $(\varphi_1, \varphi_2, D/R, \theta)$, где φ_1 и φ_2 — углы, определяющие положение БПЛА, а $\left(\frac{D}{R}, \theta\right)$ — нормированные истинные полярные координаты источника сигнала.

Случаи	**φ₁, градус**	**φ₂, градус**	**D**	**θ, градус**	**k**	**ρₖ/R**	**ψₖ, градус**
Случай 1	40	220	5	60	3	6.895	−111.332
					4	6.410	−111.374
					2	5.019	60.016
					1	4.667	59.958
Случай 2	60	200	6	300	3	6.314	−59.706
					1	1.331	−53.312
					2	0.893	−136.481
					4	0.788	−134.831
Случай 3	30	210	10	135	3	9.870	135.040
					2	7.292	−16.721
					1	1.648	−39.963
					4	1.283	169.748

Результаты компьютерных экспериментов более подробно представлены на рисунках 2.10–2.12. На рисунке 2.10 показан пример результата компьютерного эксперимента, а именно зависимость ΔD (отклонение оценочного расстояния до источника сигнала от его истинного значения) от параметра D, который представляет собой расстояние от источника сигнала до центра окружности, на которой расположены БПЛА. Видно, что это отклонение довольно резко уменьшается с увеличением D.

На рисунке 2.11 представлен еще один пример результата компьютерного эксперимента: зависимость $\Delta\psi = \psi - \psi_0$ (ψ — оценочный угол пеленга до источника сигнала, а ψ_0 — истинный угол) от D. Этот результат также подтверждает приведенный выше вывод: точность оценки координат оператора повышается с увеличением отношения D/R.

На рисунке 2.12 представлены результаты компьютерного эксперимента, предназначенного для оценки того, как ошибки измерения разницы времени прихода влияют на точность определения координат оператора. На рисунке показаны точки пересечения асимптот гипербол, одна из которых соответствует предполагаемому положению оператора, а также точка, соответствующая истинному положению. В эксперименте в значения $c\,\Delta t_{12}$ и $c\,\Delta t_{23}$ для рассматриваемого модельного примера искусственно вносилась контролируемая ошибка в 3% и 5% соответственно. Видно, что и в этом случае точность локализации оператора остается достаточной для поставленной задачи (идентификация источника сигнала с использованием принципа «свой-

чужой», при условии, что задана область, где источники, принадлежащие противоположной стороне, не могут быть обнаружены).

Компьютерные эксперименты также показали, что могут возникать вырожденные случаи (рисунок 2.12), в которых асимптоты гипербол почти параллельны и образуют лишь небольшой угол друг с другом. В таких случаях ΔD может достигать относительно больших значений; однако это не всегда существенно влияет на предлагаемый метод защиты информации. Например, если группа БПЛА развернута в непосредственной близости от зоны боевых действий, может быть достаточно определить не полные координаты источника сигнала, а только его пеленг. Случай, показанный на рисунке 2.12, демонстрирует, что в таких условиях пеленг можно оценить с приемлемой точностью даже при сравнительно малых значениях параметра D/R.

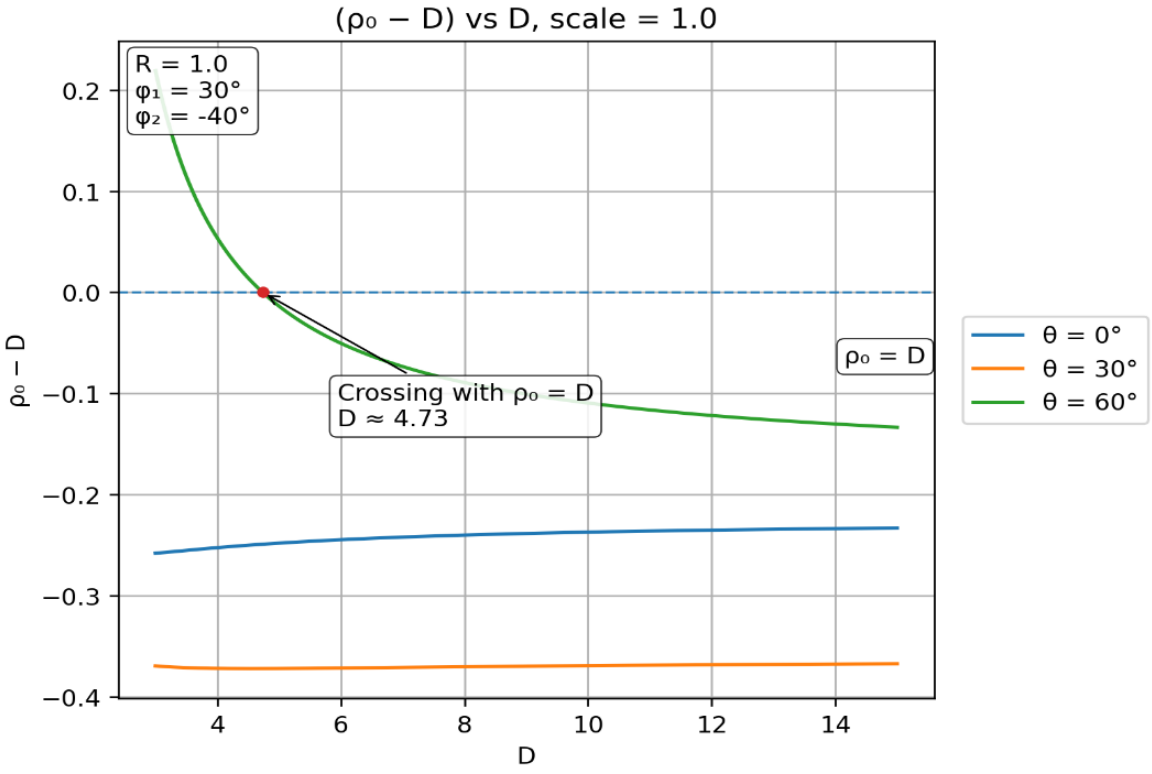


Рисунок 2.10 – Зависимость ΔD (отклонение расчетного расстояния до источника сигнала от истинного значения этого параметра) от D

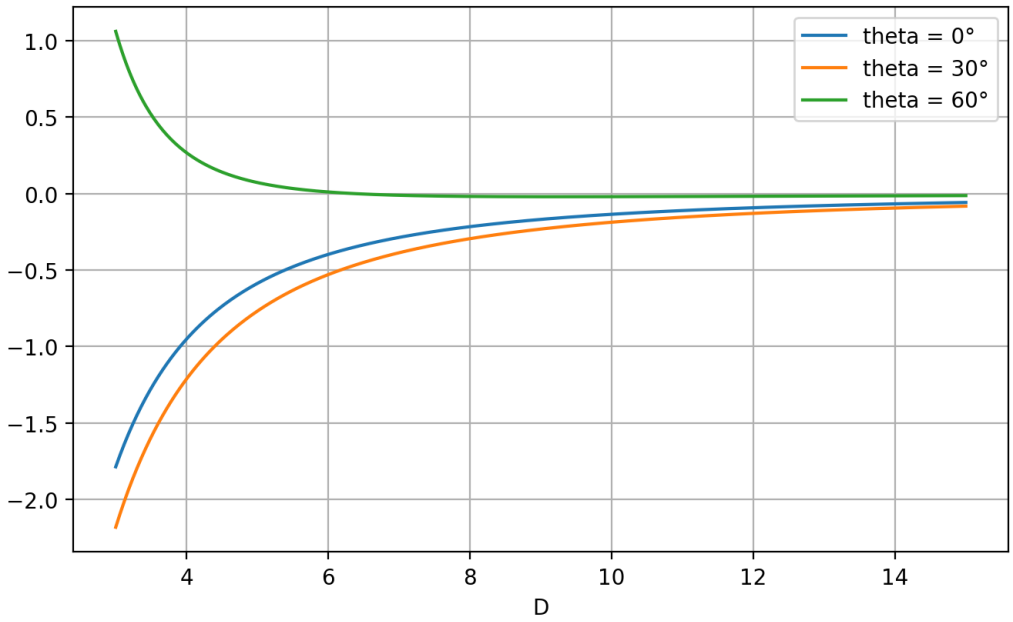


Рисунок 2.11 – Зависимость отклонения расчетного угла пеленга (направления к источнику сигнала) от истинного значения от параметра D; использовались три значения угла пеленга источника (указаны на рисунке). По оси y показано $\Delta\psi$, по оси x — D

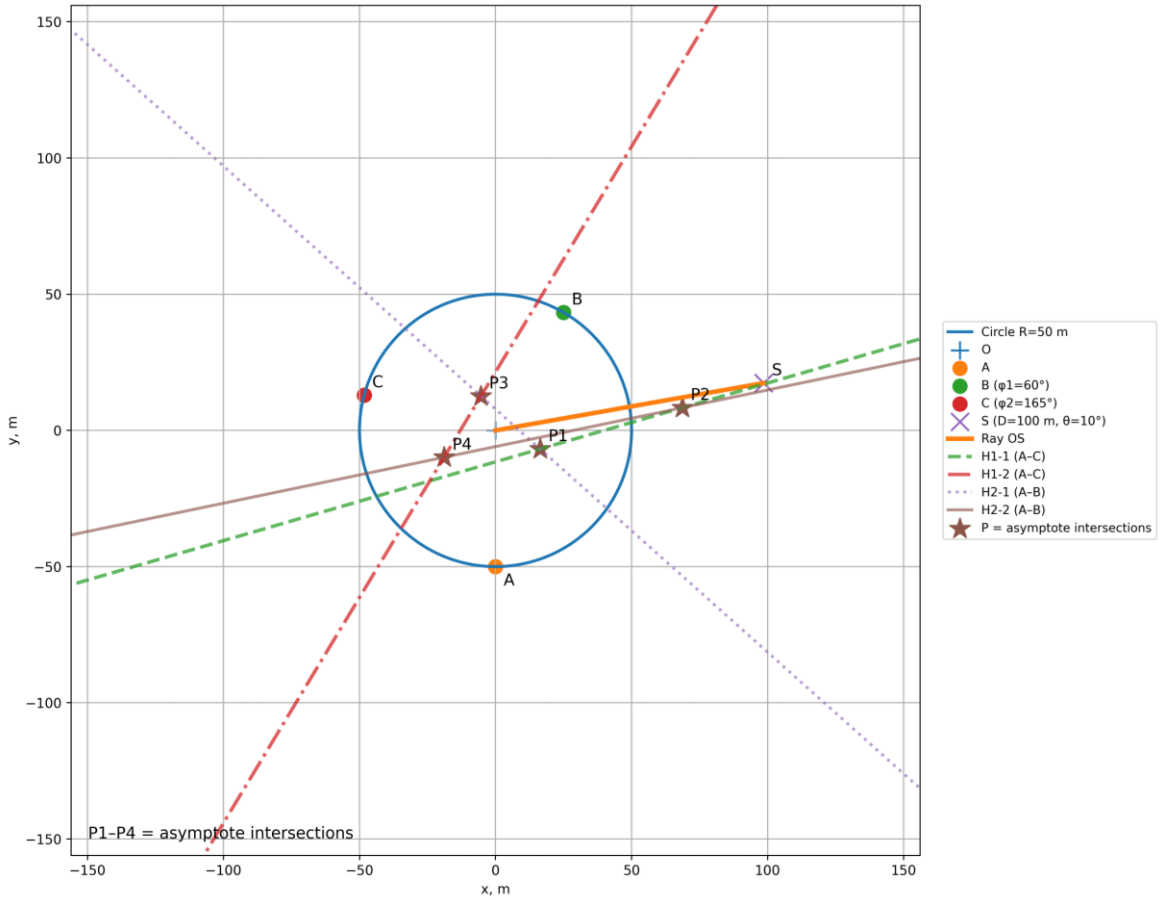


Рисунок 2.12 – Иллюстрация возможности оценки угла пеленга в случае выраженного вырождения; условия компьютерного эксперимента: $R = 50$, $\varphi_1 = 60°$, $\varphi_2 = 165$, $\rho_0 = 100$, $\theta_0 = 10°$, Δ error +5%

Таблица 2.2 – Сравнение основных характеристик предлагаемого метода с ранее известными подходами

Критерии	Предлагаемый метод (в данной работе): формация из 3 БПЛА + внутригрупповая волоконно-оптическая синхронизация + пересечение асимптот гипербол	Классическая TDoA-мультилатерация (численное пересечение гипербол)	Криптографически защищённое радиоуправле-ние роем	Прямое волоконно-оптическое управление по кабелю (оператор-БПЛА)	AoA/DoA-пеленгация (на базе антенной решётки)
Основная цель	Физическая защищённость передачи команд и однозначная локализация источника/оператора	Максимизация точности оценки координат источника	Конфиденциальность и аутентичность команд в радиоканале	Максимальная помехоустойчивость и надёжность линии управления	Оценка направления на источник (пеленг) и последующая локализация
Наблюдаемые параметры	Временная разность прихода (TDoA) и/или разность фаз между сигналами, принятыми на разных БПЛА; далее – геометричес-кая обработка (асимптотический критерий)	Временные разности прихода (TDoA) между несколькими приёмниками	Криптографические теги и параметры протокола (MAC/подписи, шифртекст); не геометри-ческие измерения	Параметры проводной оптической линии (сигнал по волокну); геолокация не является встроенной функцией	Углы прихода (AoA/DoA), то есть оценка пеленга; при необходимости - фазовые/амплитудные соотношения элементов решётки
Минимальное число воздушных узлов	3 БПЛА (две базовые линии измерения)	Обычно не менее 3 приёмников (часто больше для устойчивости)	Произвольное (определяется топологией сети)	1 БПЛА на одну кабельную линию	Обычно не менее 2 независимых пеленгов; либо 1 пункт при наличии антенной решётки, обеспечивающей измерение AoA
Требования к синхронизации времени	Снижены за счёт распределённой синхронизации по волоконно-оптическому каналу; в экспериментальной части допускается ошибка временного разрешения порядка не более 10%	Высокие требования к межприёмниковой синхронизации; точность сильно зависит от стабильности и согласованности часов	Как правило, определяется протоколом связи; для задач геолокации не применимо	Для защищённости проводного канала синхронизация не критична	Для AoA синхронизация по времени вторична; важнее калибровка и фазовая когерентность/согласование трактов
Разрешение неоднозначностей	Предусмотрено снятие геометрической неоднозначности: выбор «правильной» точки пересечения асимптот по критерию относительно центра формации; паразитные решения остаются в пределах	Возможны множественные решения; снятие неоднозначности часто требует дополнительных ограничений, фильтрации или вспомогательных датчиков	Геометрическую неоднозначность не устраняет; обеспечивает только защиту содержимого команд	В канале неоднозначностей нет; локализация не обеспечивается	Неоднозначность возможна из-за многолучёвости и неблагоприятной геометрии; пересечение пеленгов может давать ложные решения

	геометрии формации				
Вычислительная сложность	Низкая: вычисление направлений асимптот + до 4 точек пересечения + выбор решения с максимальной дальностью.	Более высокая: решение нелинейной системы / численное пересечение гипербол.	Низкая/средняя (зависит от выбранного криптокомплекта).	Низкая (по каналу), но высокая механическая нагрузка/сложность из-за кабеля.	Средняя/высокая (обработка данных решётки, калибровка).
Устойчивость к внешним радиопомехам	Высокая для внутригрупповой координации (по волокну) + возможность атрибуции источника команд («свой–чужой») при работе в зоне прямой видимости (LoS).	Потенциально уязвима (ограничения ВЧ-трактов, подмена/спуфинг, постановка помех).	Уязвима к помехам даже при шифровании; возможны компрометация ключей/ошибки человеческого фактора.	Очень высокая устойчивость к радиопомехам, но решение тяжёлое и конструктивно сложное.	Уязвима к помехам и многолучёвости; качество зависит от отношения сигнал/шум (SNR) и параметров решётки.
Предпочтительные условия эксплуатации	Сценарий прямой видимости (LoS): локализация источника/оператора/средств РЭБ в зоне LoS.	Широкие условия (LoS/NLoS), однако в NLoS характеристики заметно ухудшаются.	Широкие условия применения.	Доминируют физические ограничения: длина/масса кабеля и связанные с ними ограничения.	Лучше всего работает в LoS; многолучёвость ухудшает результат.
Синхронизация движения роя	Не требуется: система координат задаётся окружностью, проходящей через 3 БПЛА; метод применим при произвольной взаимной геометрии.	Не является методом синхронизации роя; могут требоваться предположения о стабильной геометрии/конфигурации.	Требует сетевой координации; синхронизация роя — отдельная задача.	Не является методом роя как такового.	Не является методом синхронизации роя.
Масштабируемость (добавление узлов)	Может расширяться за счёт дополнительных БПЛА, направленных антенн и маломощных ретрансляторов (ядро из 3 БПЛА — как опорный/ретрансляционный контур).	Масштабируется добавлением приёмников, но растут требования к синхронизации и вычислительной обработке.	Масштабируется естественно, однако с ростом сложности увеличивается поверхность атаки.	Низкая (кабельные «поводки» плохо масштабируются).	Масштабируется добавлением пеленгов/решёток, но увеличивает аппаратную сложность.
Типичный компромисс	Снижение алгоритмической сложности + физическая защищённость внутри группы; в отдельных сценариях — менее строгие требования к точности локализации оператора.	Потенциально более высокая точность, но более жёсткие требования к синхронизации и устойчивому снятию неоднозначностей.	Сильна по конфиденциальности/аутентичности, но слабее по устойчивости к постановке помех.	Высокая физическая защищённость, но серьёзные практические ограничения (масса/длина).	Хороша для получения направления на источник, но требует сложной аппаратуры и калибровки.

Предлагаемый подход может быть также использован и для определения координат сторонних источников радиосигнала (например, месторасположения операторов дронов противоборствующей стороны или месторасположения средств, ведущих радиоэлектронную борьбу). Принцип действия остается тем же самым, отличие состоит только в том, с какой точностью следует определять координаты источника сигнала. Такой метод, разумеется, также применим только в зоне прямой радиовидимости, но, как показывает опыт современных вооруженных конфликтов, средства радиоэлектронной борьбы, применяемые непосредственно вблизи линии боевого соприкосновения, приобретают все большее значение. Следовательно, актуальным является и создание технических средств, обеспечивающих ведение контригры. Очевидно, что такие средства должны быть максимально защищены от возможного воздействия противника (во всяком случае – информационного). Использование оптоволоконных линий связи между БПЛА, составляющими группу, заведомо исключает такое воздействие, особенно в том случае, когда группа действует в автономном режиме.

Отметим также, что предложенный подход создает предпосылки для использования методов абстрактной алгебры, которые разрабатывались, в частности, в работах [111-115]. Такая возможность связана прежде всего с тем, что радиус окружности, на который располагается БПЛА, и центр которой совпадает с началом координат, может меняться в процессе полета группы БПЛА от минимального расстояния до максимального. Максимальное значение этого радиуса предполагает возможность уверенной идентификации источника сигнала на расстоянии около 2 км, поскольку именно такая дальность представляет интерес для конкретного использования групп БПЛА вблизи линии боевого соприкосновения.

Регулируя радиус указанной окружности, можно регулировать и отношение данного радиуса к расстоянию до оператора, поддерживая его примерно постоянным. Именно это ситуацию и иллюстрирует рисунок 2.13. Здесь, исходя из расстояния до оператора, который помечен цифрой 1, можно выделить три категории зон, причем каждый из этих зон разбивается на некоторое количество участков прямыми, проходящими через начало координат.

Первая зона имеет форму круга, и в ней расположены сегменты, которые с точки зрения идентификации заведомо отпадают, потому что расстояние от начала координат до любой точки в этих сегментах меньше, чем ожидаемое расстояние до оператора. Аналогично, отпадают и сегменты из третьей зоны, которая лежит за тем кольцом, где располагается оператор.

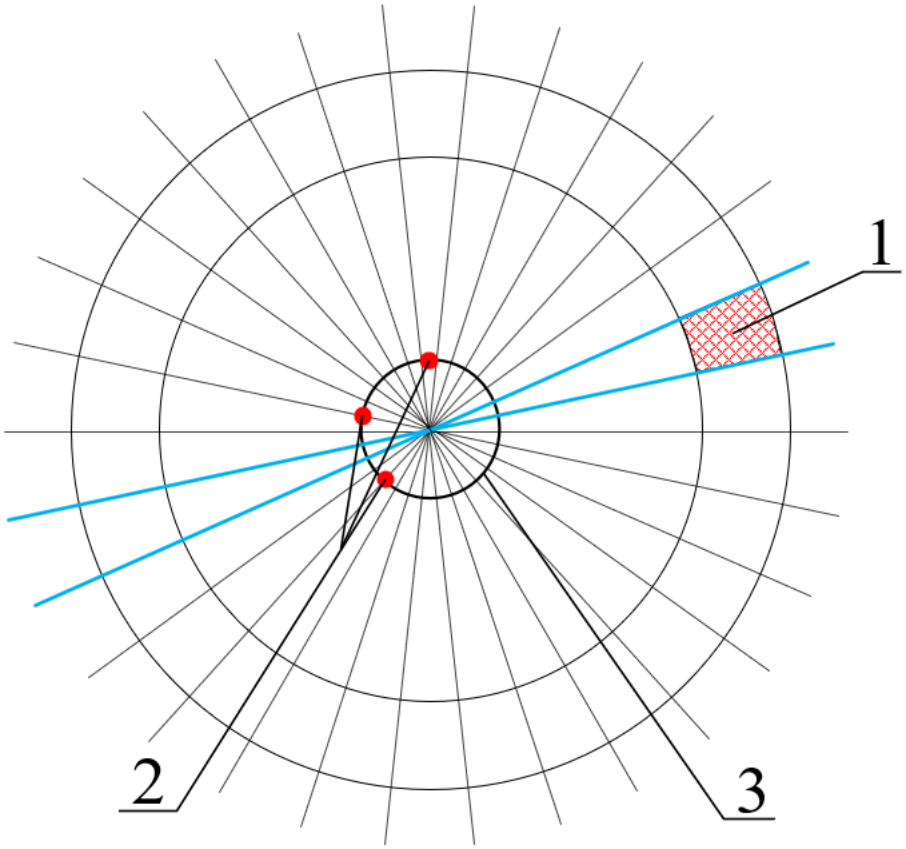


Рисунок 2.13 – К выделению зон при идентификации координат оператора/источника сигнала

Следовательно, в данном случае задача по определению зоны, где расположен оператор становится полностью дискретной. Это, в свою очередь, означает, что можно оперировать системой координат, который отвечает Галуа-координатам. Одно измерение отвечают полю Галуа GF(3), которая содержит три элемента (в данном случае эти три элемента маркируют классификацию по дальности), а второе поле Галуа отвечает разбиению выделенного кольца на сегменты. С учетом реальной обстановки, это число может быть разным, но есть основания предполагать, что для идентификации координат оператора по принципу «свой-чужой» можно использовать поле Галуа GF(31), что отвечает определению направления на оператора с точностью примерно до 12 градусов.

Таким образом, данный подход допускает дальнейшие совершенствования, в том числе, и с использованием методов абстрактной алгебры. Примем, однако, во внимание, что он может применяться не только для целей идентификации координат оператора, то есть не только для защиты информации, но и для целей пеленгации. Здесь, как показано в следующем параграфе, также существует возможность привести решение рассматриваемой задачи к геометрической задаче о пересечении прямых линий.

2.4. Возможности дальнейшего совершенствования предложенного подхода

Рассмотрим два квадратичных уравнения, записанных в общем виде

$$a_{11}x^2 + 2a_{12}xy + a_{22}y^2 + 2a_{13}x + 2a_{23}y + a_{33} = 0 \quad (2.69)$$

$$b_{11}x^2 + 2b_{12}xy + b_{22}y^2 + 2b_{13}x + 2b_{23}y + b_{33} = 0 \quad (2.70)$$

Эти уравнения отвечают квадратичным формам с симметричными матрицами $\hat{A}$ и $\hat{B}$ и могут быть записаны в форме

$$\vec{\rho}\hat{A}\vec{\rho} = 0;\ \vec{\rho}\hat{B}\vec{\rho} = 0 \quad (2.71)$$

где $\vec{\rho} = (x, y, 1)$ допустимо рассматривать как вектор, отвечающий проективным координатам на плоскости.

Допустимо поставить задачу, аналогичную задаче на отыскание собственных значений матрицы, т.е. отыскать такое значение λ, что

$$\det\left(\hat{A} + \lambda\hat{B}\right) = 0 \quad (2.72)$$

Данное уравнение имеет третью степень по параметру λ, следовательно, имеет, как минимум одно решение. Матрица $\hat{C} = \hat{A} + \lambda\hat{B}$, очевидно, также представляет собой матрицу квадратичного уравнения, которое может быть получено линейной комбинацией уравнений (2.69) и (2.70) и обладает следующими коэффициентами

$$c_{i,j} = a_{i,j} + \lambda b_{i,j} \quad (2.73)$$

Для квадратичного уравнения с коэффициентами (2.73) выполнение условия (2.72) означает, что кривая второго порядка, описываемая таким уравнением, становится вырожденной. В частности, данная кривая вырождается в две скрещенные прямые (вырожденная гипербола) при выполнении условия

$$\det\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} < 0 \quad (2.74)$$

Следовательно, комбинируя уравнения (2.69) и (2.70), допустимо перейти к задаче, в которой, как минимум рассматриваются пересечения кривой второго порядка с прямыми линиями. Если же решений уравнения (2.72) больше одного, то задача сводится к отысканию пересечений прямых линий.

Покажем, что такой подход обладает следующим преимуществом. При решении задачи об отыскании точки пересечения гипербол использование уравнения (2.72) позволяет свести данную задачу к решению стандартного

кубического уравнения, порождающего решение, которое также может быть стандартизовано. Это создает определенные преимущества с точки зрения разработки бортового вычислительного блока БПЛА, использующего предлагаемый метод защиты информации.

Для демонстрации сущности предлагаемого подхода рассмотрим частный случай, отвечающий следующему расположению приемников излучения на плоскости

$$\vec{r}_{10} = (a, a);\ \vec{r}_{20} = (-a, a);\ \vec{r}_{23} = (a, -a) \tag{2.75}$$

Для данного частного случая выражения (2.13) и (2.14) приводят к следующим формулам

$$r_1^2 - r_2^2 = 4xa,\ r_1^2 + r_2^2 = 2x^2 + 2y^2 - 4ya + 4a^2 \tag{2.76}$$

Откуда

$$16x^2a^2 - 4R_1^2(x^2 + y^2 - 2ya + 2a^2) + R_1^4 = 0 \tag{2.77}$$

или

$$(16a^2 - 4R_1^2)x^2 - 4R_1^2y^2 + 8R_1^2ay - 8R_1^2a^2 + R_1^4 = 0 \tag{2.78}$$

Аналогично, для пары приемников с номерами 1 и 3 получаем

$$(16a^2 - 4R_2^2)y^2 - 4R_2^2x^2 + 8R_2^2ax - 8R_2^2a^2 + R_2^4 = 0 \tag{2.79}$$

где R_1 и R_2 – расстояния, отвечающие измеренной разности фаз для каждой из пар приемников.

Отличительной особенностью уравнений (2.78) и (2.79), как и следовало ожидать, является то, что коэффициент при произведении xy равен нулю. Для этого случая условия, при которых гипербола становится вырожденной, т.е. выполняется соотношение вида (2.72), можно получить непосредственно. Для наглядности приведем соответствующие выкладки, попутно получив конкретные соотношения для коэффициентов, скрещенных прямых, отвечающих вырожденной гиперболе.

Будем отталкиваться от соотношения

$$(a_1x + b_1y + 1)(a_2x + b_2y + 1) = A_1x^2 + A_2y^2 + 2B_1x + 2B_2y + 1 \tag{2.80}$$

Можно видеть, что с точностью до множителя $R_{1,2}^4$ правая часть (2.80) совпадает по виду с левой частью (2.78) и (2.79). Выполнение соотношения (2.80) приводит к следующим соотношениям

$$a_1 a_2 = A_1,\ b_1 b_2 = A_2 \tag{2.81}$$

$$a_1 + a_2 = 2B_1,\ b_1 + b_2 = 2B_2 \tag{2.82}$$

$$a_1 b_2 + b_1 a_2 = 0 \tag{2.83}$$

Это – пять уравнений на четыре неизвестных. Следовательно, чтобы они имели решение на величины $A_{1,2}$ и $B_{1,2}$ должны быть наложены определенные ограничения. Установим их. Из (2.83) непосредственно вытекает, что

$$\frac{b_1}{a_1} = -\frac{b_2}{a_2} \tag{2.84}$$

Следовательно, можно использовать множитель α такой, что

$$b_1 = \alpha a_1,\ b_2 = -\alpha a_2 \tag{2.85}$$

Соотношение (2.85) позволяет перейти к следующей системе четырех уравнений на три неизвестных параметра.

$$a_1 a_2 = A_1,\ \alpha^2 a_1 a_2 = -A_2 \tag{2.86}$$

$$a_1 + a_2 = 2B_1,\ \alpha(a_1 - a_2) = 2B_2 \tag{2.87}$$

Решения уравнений (2.87) очевидны

$$a_1 = B_1 + \frac{B_2}{\alpha},\ a_2 = B_1 - \frac{B_2}{\alpha} \tag{2.88}$$

Следовательно, система уравнений (2.86) – (2.87) будет иметь решение, если одновременно будут выполняться следующие два уравнения на параметр α

$$\alpha^2 B_1^2 - B_2^2 = \alpha^2 A_1 \tag{2.89}$$

$$\alpha^2 B_1^2 - B_2^2 = -A_2 \tag{2.90}$$

Это возможно только в том случае, если имеет место

$$(B_2^2 - A_2)(B_1^2 - A_1) - B_2^2 B_1^2 = 0 \tag{2.91}$$

или

$$4A_1 A_2 - A_2 B_1^2 - A_1 B_2^2 = 0 \tag{2.92}$$

Это условие совпадает с условием равенства нулю определителя матрицы, которое определяет вырождение гиперболы в скрещенные прямые.

$$\begin{vmatrix} A_1 & 0 & B_1 \\ 0 & A_2 & B_2 \\ B_1 & B_2 & 1 \end{vmatrix} = A_1(A_2 - B_2^2) - A_2 B_1^2 = 0 \quad (2.93)$$

Таким образом, от уравнений (2.88) и (2.89) допустимо перейти к уравнению, определяющим вырождение гипербол

$$\begin{vmatrix} 16a^2 - 4R_1^2 - 4\lambda R_2^2 & 0 & 4\lambda R_2^2 \\ 0 & \lambda(16a^2 - 4R_2^2) - 4R_1^2 & 4R_1^2 \\ 4\lambda R_2^2 & 4R_1^2 & R_1^4 + \lambda R_2^4 \end{vmatrix} = 0 \quad (2.94)$$

Уравнение (2.94) за счет сокращения численных коэффициентов по строкам и столбцам приводится к следующему виду

$$\begin{vmatrix} 1 - q_1 - \lambda q_2 & 0 & 2\lambda q_2 \\ 0 & \lambda - q_1 - \lambda q_2 & 2q_1 \\ 2\lambda q_2 & 2q_1 & q_1^2 + \lambda q_2^2 \end{vmatrix} = 0 \quad (2.95)$$

где $q_{1,2} = \frac{R_{1,2}^2}{2a}$

Подчеркиваем, что метод, рассмотренный в последнем разделе данной главы, в сущности, решает ту же самую задачу, которую и решает метод гипербол – это решение системы квадратичных уравнений с использованием довольно специфического метода, основанного на решение обобщенной спектральной задачи, то есть задачи, которая обобщает задачу о поиске собственных векторов некоторой матрицы. На первый взгляд использование такого подхода не вполне рационально, поскольку существует методы решений квадратичных уравнений, в том числе и точные [96]. Более того, при не слишком высокой точности (подчеркнем еще раз, что высокая точность в данном случае требуется далеко не всегда) все необходимые уравнения могут быть решены численно, в том числе, при помощи бортовых вычислительных систем.

Однако, как вытекает из материалов данной главы, если рассматривается задача о защите информации, то есть определении координат оператора, местоположение которого нам известно, то достаточно использовать метод, основанный на пересечении асимптот гипербол, что не требует точного решения упомянутой выше системы квадратичных уравнений.

Более сложные задачи возникают в том случае, когда речь, например, идет о задачах пеленгации, то есть об определении координат некого стороннего источника, местоположение которого неизвестно и его требуется

определить. В этом случае, целесообразно использовать группы дронов, причем не ограничиваться использованием их минимального числа, как это вытекает, например, из классического «метода гипербол». Источников может быть несколько, они могут влиять друг на друга, и следовательно, здесь целесообразно использовать большее количество пар дронов. Именно поэтому целесообразно сводить рассматриваемую задачу к геометрической задаче о пересечении прямых линий. Главное преимущество здесь состоит в том, что это позволяет максимально просто и удобно совместить решения, отвечающие различным парам дронов, а также осуществить классификацию метаположений источников сигнала, которая неизбежно станет необходимой, в том случае, когда таких источников имеется достаточно много.

Таким образом, использование оптоволоконной связи между БПЛА, составляющими группу (рой), создает вполне определенные преимущества с точки зрения защиты информации, передаваемой от оператора к данной группе. С одной стороны, в данном случае сохраняются все те преимущества, которые обеспечиваются при прямой передаче команд от оператора к БПЛА по оптоволокну. С другой стороны, в данном случае возникает возможность существенно уменьшить протяженность оптоволоконных линий связи.

Такой метод защиты информации предназначен для использования в зоне прямой радиовидимости и основан на независимом определении координат источника сигнала бортовыми вычислительными системами группы БПЛА.

Реализация такого подхода требует решения соответствующих геометрических задач, в простейшем случае данная задача сводится к отысканию пересечений асимптот гипербол, а в общем – к решению которые сводятся к решению систем квадратичных уравнений.

В последнем случае также можно предложить удобный (в том числе, с точки зрения оптимизации логической структуры бортовых вычислительных систем) способ решения таких уравнений, позволяющий свести задачу к задаче о пересечении прямых линий.

Предлагаемый метод в перспективе применим также для определения координат иных источников радиосигналов, например, средств ведения радиоэлектронной борьбы, координат операторов дронов противоборствующей стороны и т.д.

Выводы по Главе 2

Представлен новый геометрический метод однозначной локализации удаленных источников радиосигналов с использованием трех БПЛА, соединенных волоконно-оптическими линиями связи, основанный на пересечении асимптот гипербол, а не полных гиперболических кривых. Мы показываем, что физически корректное местоположение излучателя всегда находится в точке пересечения асимптот, наиболее удаленной от центра формации БПЛА, в то время как все ложные решения остаются ограниченными радиусом формации.

Метод обеспечивает безопасную, устойчивую к помехам передачу команд от оператора к группе БПЛА и поддерживает обнаружение внешних радиоизлучателей (включая операторов и системы радиоэлектронной борьбы) в условиях прямой видимости. Защита информации основана на идентификации источника сигнала по принципу «свой-чужой». Метод особенно эффективен, когда область, в которой невозможно обнаружить вредоносные источники сигнала, известна заранее, по крайней мере приблизительно (например, с одной или другой стороны линии контакта). В данном случае координаты оператора можно оценить с относительно низкой точностью, на уровне, достижимом для рассматриваемого метода.

Глава 3. Применение метода фазовых портретов для определения мгновенного значения частоты и фазы гармонического или квазигармонического колебания

В данной главе рассматривается конкретизация того подхода, адекватность которого была обоснована как в главе 2, так и в главе 1. Показано, что для максимально эффективного использования предложенного подхода необходимо развить специфический метод определения разности фаз. Обоснование использования данного метода отражается в первом параграфе данной главы. В дальнейших главах отражается его конкретизация, в том числе, на уровне электронных схем. Представлены конкретные электронные схемы, которые позволяют реализовать этот метод, доказывается их работоспособность. Кроме того, рассматривается вопрос о том, когда на группу беспилотных летательных аппаратов поступают сигналы от нескольких источников. В противном случае, возникает возможность просто отсечь эту ситуацию и отказаться от исполнения команды. Однако, в конкретных боевых условиях, это не всегда является адекватным. Поэтому требуется выделить те команды, которые действительно исходят от оператора. Исходя из этого, в последующих разделах данной главы рассматривается общий подход к анализу квазигармонических колебаний с использованием того метода, который позволяет идентифицировать местоположение оператора, исходя из определений разности фаз. Материал данной главы в основном отражен в работах [116, 117].

3.1. Метод фазовых портретов

Предлагаемый нами подход основывается на использовании фазовых портретов. Под фазовым портретом, в соответствии с [118, 119], понимается зависимость производной по времени $\frac{du}{dt}$ некоторой функции u от самой этой функции u. В частности, фазовый портрет гармонического колебания представляет собой эллипс. Действительно, в этом случае

$$u = A\cos(\omega t)\,;\ \frac{du}{dt} = -\omega A\sin(\omega t) \tag{3.1}$$

Следовательно,

$$u^2 + \frac{1}{\omega^2}\left(\frac{du}{dt}\right)^2 = A^2 \tag{3.2}$$

Формула (3.2), очевидно, представляет собой каноническое уравнение эллипса в координатах $x = u;\ y = \frac{du}{dt}$. Этот факт позволяет поставить вопрос о вычислении локальных значений частоты квазигармонического колебания. Действительно, параметр, интерпретируемый как круговая частота ω, может быть вычислен по формуле (3.2) даже при рассмотрении одного периода колебаний (или части периода).

На рисунке 3.1 представлена модельная кривая, отвечающая частотно-моделированному колебанию следующего вида:

$$U = A_0 \sin\left(\frac{2\pi g t}{T_0}\right) \tag{3.3}$$

Модуляция по частоте описывается множителем, конкретные значения параметров указаны в подписи к рисунку 3.1.

$$g = 1 + \frac{B_0}{1+\exp[(t_0 - t)/\tau]} \tag{3.4}$$

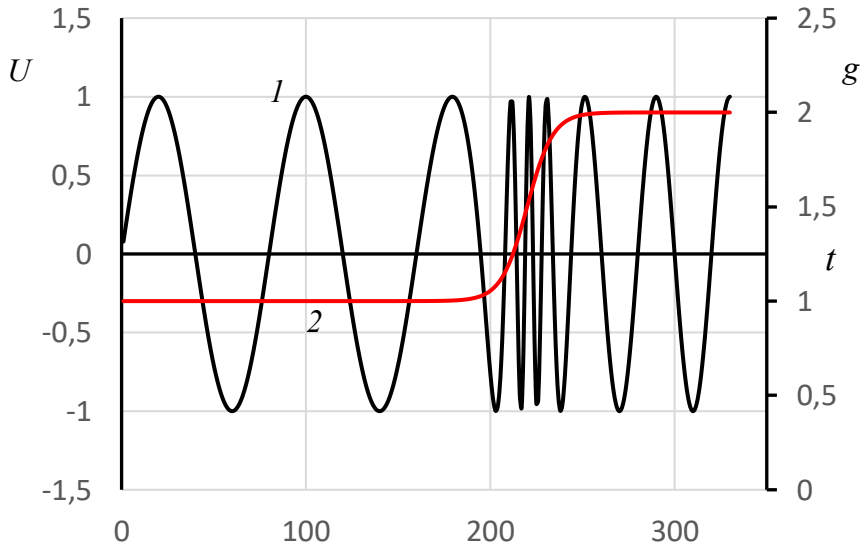


Рисунок 3.1 – Модельное частотно-моделированное колебание U (кривая 1) и множитель g, задающий модуляцию частоты колебаний (кривая 2); $A_0 = 1, B_0 = 1, \tau = 7, t_0 = 220, T_0 = 80$

Фазовый портрет данного модельного колебания представлен на рисунке 3.2. Как и следовало ожидать, отдельные фрагменты данного портрета отвечают эллипсам.

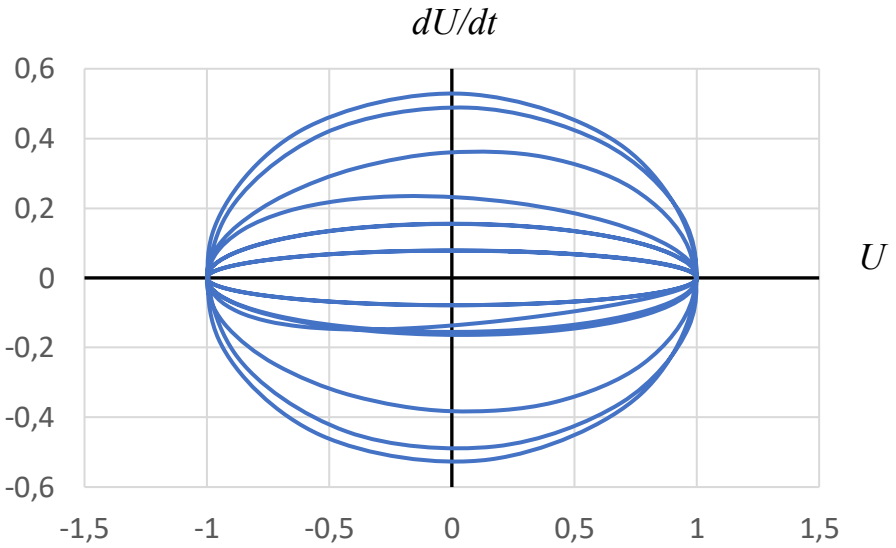


Рисунок 3.2 – Фазовый портрет модельного колебания, представленного на рисунке 3.1

На рисунке 3.3 представлено еще одно модельное колебание, отвечающее случаю амплитудной модуляции. Это колебание описывается следующей формулой с множителем $g(t)$, который задается формулой (3.5).

$$U = A_0 g(t) \sin\left(\frac{2\pi t}{T_0}\right) \tag{3.5}$$

Фазовый потрет данного колебания представлен на рисунке 3.4. Видно, что и в этом случае по крайней мере некоторые фрагменты фазового портрета представляют собой фрагменты эллипсов, причем отчётливо виден переход к эллипсам, отвечающим колебаниям с большей амплитудой.

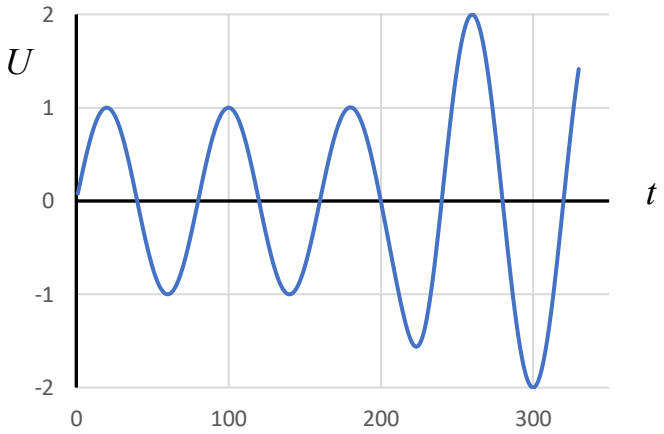


Рисунок 3.3 – Модельное частотно-моделированное колебание U (кривая 1) и множитель g, задающий модуляцию частоты колебаний (кривая 2); $A_0 = 1, B_0 = 1, \tau = 7, t_0 = 220, T_0 = 80$

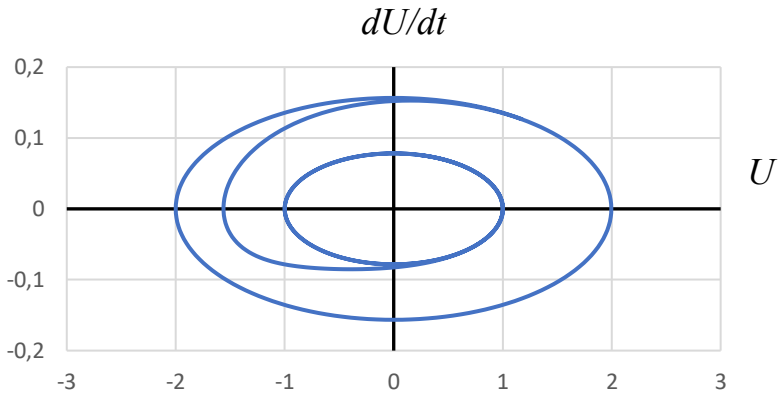


Рисунок 3.4 – Фазовый портрет модельного колебания, представленного на рисунке 3.3

Этот метод похож на широко распространенный метод скользящего среднего [120, 121], но отличается от него характером передаточной функции. Свертка с функцией вида (3.1) более точно идентифицирует колебание, спектр которого включает гармоники с периодом меньше T_0.

3.2. Описание предлагаемого алгоритма

Предлагаемый алгоритм состоит в следующем. Фазовый портрет разбивается на фрагменты, приближенно отвечающие ¼ основного периода исследуемого колебания. Каждый из таких фрагментов аппроксимируется сегментом кривой второго порядка при помощи метода наименьших квадратов. Задача ставится более широко, так как встречающиеся на практике фрагменты фазовых портретов не обязательно должны отвечать сегментам эллипса. Участки колебания, которые допускают аппроксимацию эллипсами с приемлемой точностью, трактуются как отвечающие квазигармоническим колебаниям. Процедура аппроксимации в данном случае автоматически дает три параметра, характеризующие эллипс: амплитуду, квадрат частоты и постоянную составляющую. Последний параметр отвечает ситуации, когда аппроксимирующий эллипс смещен по оси. Все эти параметры могут рассматриваться как мгновенные, точнее относящиеся к моменту времени, который отвечает центру рассматриваемого фрагмента (рисунок 3.5).

Наибольший интерес (во всяком случае, с точки зрения использования групп БПЛА для определения местоположения источника сигнала) представляет, однако, определение мгновенного значения фазы φ_t. В соответствии с построением рисунка 3.5, под φ_t допустимо понимать момент времени, отвечающий центру сегмента AB, т.е. точке C.

$$\varphi_t = \arccos \frac{1}{\omega^2 A} y\big(x(t)\big) \tag{3.6}$$

В данной формуле $y(x(t))$ есть функция, по которой вычисляется аппроксимация, A – действующее значение амплитуды колебаний. Значение $y(x)$, равно как ω^2 и A, соответственно, может быть вычислено для каждой точки x, отвечающей рассматриваемому фрагменту. (Расчетные формулы для вычисления ω^2 и A рассматривается ниже.)

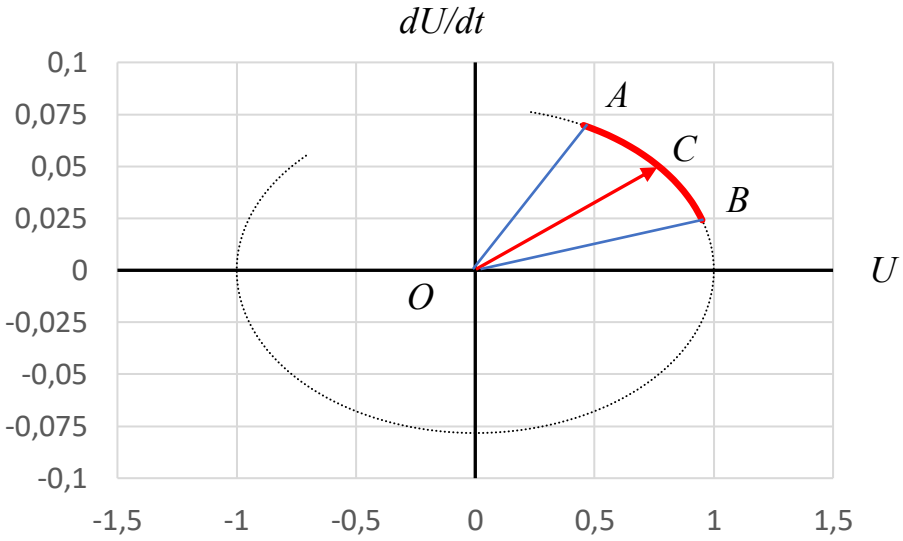


Рисунок 3.5 – Фазовый портрет фрагмента модельного колебания

Здесь, разумеется, возникает вопрос о том, насколько такое истолкование «мгновенного значения фазы» является корректным. Ответить на него проще всего с точки зрения практического использования (метод определения координат источника радиосигнала). Если в среде, в которой распространяется радиоволна, отсутствует дисперсия, то профиль колебания во всех точках пространства будет одинаковым. Отличия будут связаны только со сдвигом по оси времени. Следовательно, вычисления φ_t при помощи предложенного метода будут решать поставленную задачу независимо от характера интерпретации данной величины. Рассмотрим, как предложенный метод может быть применен на практике.

3.3. Базовая схема для определения координат оператора

Определение мгновенного значения фазы колебания, как отмечалось выше, представляет интерес также для обеспечения защиты информации при передаче команд от оператора к группе БПЛА, при помощи метода, основанного на идентификации координат источника радиосигнала [93,94]. В данной главе осуществляется конкретное воплощение схемы, которая рассматривалась в предыдущей главе (рисунок 2.2). Подчеркнем, что данная схема, в частности, может быть реализована на основе группы БПЛА, связь между которыми осуществляется по оптоволокну.

Как было показано выше, реализация предлагаемого метода сводится к решению геометрической задачи, т.е. к отысканию точки пересечения

гипербол (если речь идет о задаче на плоскости) или гиперболоидов (если решается пространственная задача).

Это означает, что решение поставленной задачи может быть осуществлено расчетным путем при помощи известных алгоритмов, реализуемых программой, устанавливаемой на микроконтроллер. Аналогично, расчетным путем могут быть определены параметры фрагмента фазового портрета, при условии, что используемая схема обеспечивает преобразование сигнала в цифровой формат.

В частности, для отыскания параметров кривых второго порядка, аппроксимирующих экспериментальные данные, допустимо использовать следующий функционал

$$J = \sum\left(y_i^2 + a_1 x_i^2 + a_2 x_i - a_3\right)^2, \tag{3.7}$$

Дифференцируя J по каждому из параметров a_i, получаем уравнения, позволяющие определить их значения

$$\frac{dJ}{da_1} = 2\sum x_i^2\left(y_i^2 + a_1 x_i^2 + a_2 x_i - a_3\right) = 0 \tag{3.8}$$

$$\frac{dJ}{da_2} = 2\sum x_i\left(y_i^2 + a_1 x_i^2 + a_2 x_i - a_3\right) = 0 \tag{3.9}$$

$$\frac{dJ}{da_3} = -2\sum\left(y_i^2 + a_1 x_i^2 + a_2 x_i - a_3\right) = 0 \tag{3.10}$$

Данная аппроксимация отвечает эллипсу если $a_1 > 0$. В этом случае

$$a_1 = \omega^2, a_2 = -2\omega^2 c, a_3 = \omega^2 A^2 - \omega^2 c^2\ . \tag{3.11}$$

Последняя из формул (3.11), в частности, позволяет вычислить величину A, фигурирующую в формуле (3.6). Аппроксимация фрагмента фазового портрета с помощью эллиптической кривой в этом случае определяется формулой

$$y_i = \pm\sqrt{a_3 - a_1 x_i^2 - a_2 x_i} \tag{3.12}$$

Конкретная реализация предлагаемой системы основана на высокопроизводительном микроконтроллере, работающем на частоте 480 МГц, что обеспечивает значительные вычислительные возможности для обработки сигналов и выполнения сложных алгоритмов. Высокая тактовая частота позволяет микроконтроллеру эффективно управлять периферийными устройствами и обеспечивать минимальные задержки в обработке данных.

Для преобразования входного сигнала с приёмника используется встроенный 16-битный АЦП1, функционирующий при частоте 240 МГц и способный выполнять до 2 миллионов преобразований в секунду (2 MSPS). Такая производительность позволяет с высокой точностью захватывать динамические аналоговые сигналы, что критично для систем, требующих быстрого и точного измерения.

Для обеспечения высокоскоростного запуска преобразований задействован таймер TIM1, работающий в режиме Trigger mode. Он генерирует внешние триггерные сигналы (TRGO) с частотой 1,6 МГц, что соответствует периоду в 625 нс для каждого импульса. Режим работы АЦП – ADC_Regular_ConversionMode – позволяет инициировать преобразование внешним сигналом. Таким образом, каждый импульс TRGO, генерируемый нарастающим фронтом при событии обновления таймера, запускает процесс аналого-цифрового преобразования входного сигнала.

После получения триггерного сигнала от TIM1, АЦП1 начинает преобразование входного аналогового сигнала, результат которого мгновенно записывается в регистр данных. Важно отметить, что при такой высокой скорости преобразований традиционная обработка результатов центральным процессором могла бы вызвать существенную нагрузку на систему, что отрицательно сказывалось бы на производительности.

Для оптимизации обработки данных применяется механизм прямого доступа к памяти (DMA). DMA обеспечивает автоматическую передачу результатов преобразований из регистра АЦП в заранее настроенный буфер оперативной памяти. Буфер рассчитан на 40 последовательных преобразований, и при каждом срабатывании прерывания данные копируются напрямую, без вмешательства центрального процессора. Такой подход позволяет существенно снизить загрузку CPU, обеспечивая параллельную обработку других задач и гарантируя, что поток данных не будет прерван даже при интенсивном режиме работы.

Комбинированное использование микроконтроллера с высокой тактовой частотой, быстрого 16-битного АЦП с возможностью 2 MSPS, точного таймера TIM1 для генерации триггерных сигналов и эффективного механизма DMA обеспечивает надежное, быстрое и точное преобразование входного аналогового сигнала в цифровую форму. Такая архитектура идеально подходит для приложений, где критична минимальная задержка и высокая скорость обработки данных, позволяя системе работать стабильно даже при высоких темпах обмена информацией.

Электронная схема, обеспечивающая реализацию предложенного подхода, представлена на рисунке 3.6. Она обеспечивает преобразование регистрируемого сигнала в цифровую форму, а далее осуществляются расчёты параметров фрагмента фазового портрета в соответствии с описанным выше методов.

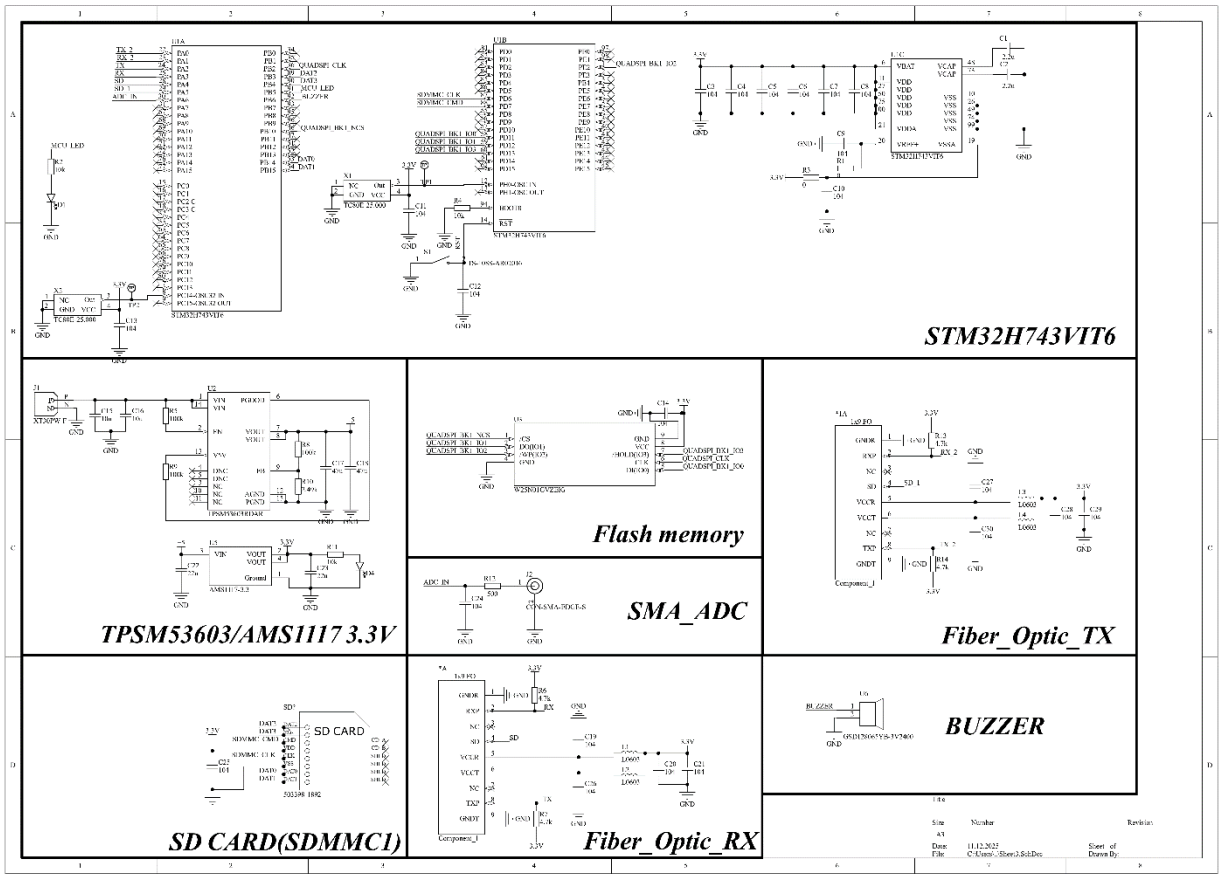


Рисунок 3.6 – Электронная схема блока построения фрагмента фазового портрета – детектора мгновенного значения амплитуды и фазы колебания

Схема построена на базе микроконтроллера STM32H743VIT6, работающего на частоте 480 МГц. Эта частота тактирования формируется за счёт использования внешнего кварцевого генератора с рабочей частотой 24 МГц, сигнал которого умножается внутренним ФАПЧ (фазово-автоподстраивающимся генератором). Такой подход обеспечивает высокую стабильность и точность тактового сигнала, что критично для высокопроизводительных приложений.

Для приёма входного сигнала на плате используется SMA-коннектор. Он обеспечивает прямое подключение к источнику сигнала и высокое качество передачи. Входной сигнал поступает на вывод PA6 микроконтроллера, который соответствует первому входу АЦП1, что позволяет выполнять высокоточные аналого-цифровые преобразования. Дополнительно, трассировка сигнала от SMA-коннектора до микроконтроллера реализована с использованием переходных отверстий, что значительно повышает помехозащищённость и целостность сигнала, особенно в условиях высокочастотных воздействий.

Для передачи и приёма данных по оптическому каналу в схеме применены высокоскоростной оптоволоконный приёмник и передатчик HFBR-2412T. Эти компоненты предназначены для надёжной передачи цифровых сигналов по оптическому волокну, что обеспечивает высокий уровень защиты от электромагнитных помех. На стороне передатчика

дополнительно установлен высокоскоростной CMOS-трансивер SN75451BDR, позволяющий корректно согласовать уровни сигналов и обеспечить быструю обработку цифровых данных. Для хранения предустановок используется flash-память W25N01GVZEIG. Результаты преобразований записываются через интерфейс SDMMC, который передаёт данные по 4-битной шине на SD-карту. Такой подход обеспечивает высокую скорость записи и надёжное сохранение данных даже при интенсивном потоке информации.

Питание всей схемы осуществляется через DC-DC преобразователь TPSM53603RDAR, который обеспечивает стабильное и эффективное питание всех компонентов. Это позволяет минимизировать шумы и колебания напряжения, что особенно важно для корректной работы высокочастотных и чувствительных элементов схемы.

Блок-схема программы, устанавливаемой на микроконтроллер, показана на рисунке 3.7.

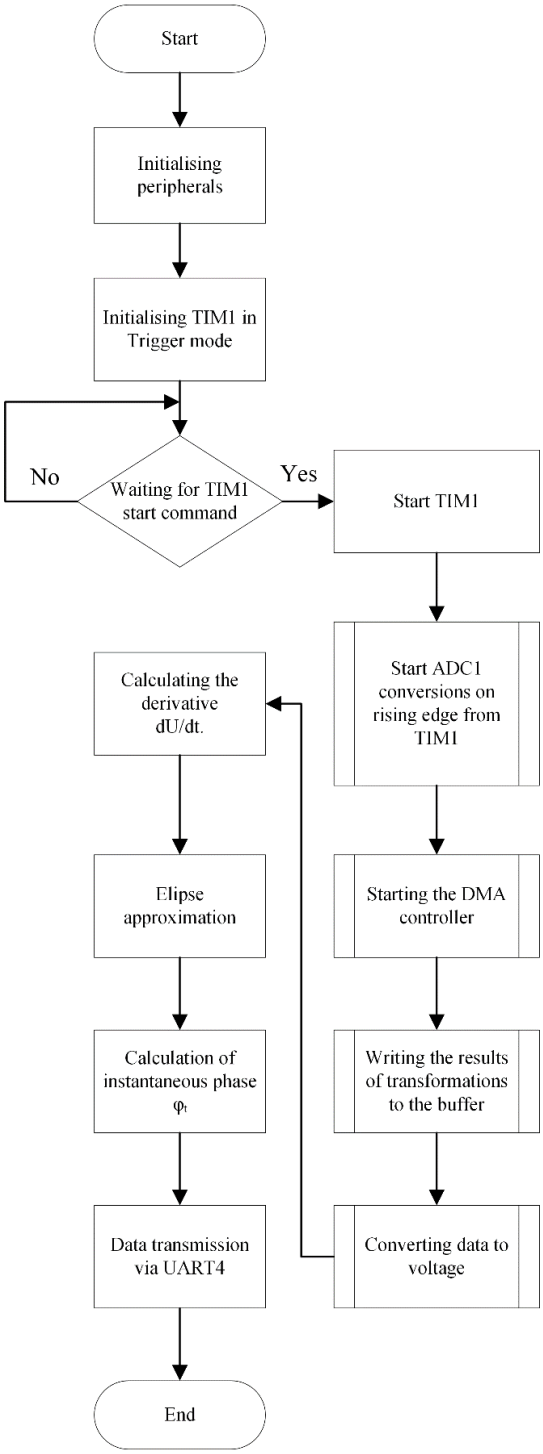


Рисунок 3.7 – Блок-схема работы программы микроконтроллера

Печатная плата разработана с использованием стековой компоновки JLC04161H-7628 Stackup (рисунок 3.8), что обеспечивает точное соблюдение требуемых параметров для высокочастотных схем. Все трассы рассчитаны на поддержание импеданса в 50 Ом, что критически важно для сохранения качества сигнала и минимизации отражений в высокоскоростных системах. Питание распределено по внутренним слоям, что способствует снижению электромагнитных помех и улучшению стабильности работы всей системы.

Такой подход в проектировании позволяет добиться высокой надежности и оптимальной работы печатной платы в условиях интенсивного обмена данными и высокочастотных воздействий. Трассировка дорожек печатной платы показана на рисунке 3.9, а ее модель – на рисунке 3.10.

#	Name	Material	Type	Thickness	Dk	Df	Color	Solid	Weight
	Top Overlay		Overlay						
	Top Solder	Solder Resist	Solder Mask	0.01016mm	3.5		#00FFFFFF		
1	Top Layer	CF-004	Signal	0.035mm					1oz
	Dielectric 4	PP-006	Prepreg	0.0994mm	4.1	0.02			
2	L2_GND	CF-004	Signal	0.0152mm					1/2oz
	Dielectric 2	PP-023	Prepreg	0.55mm	4.1	0.02			
3	L3_PWR		Signal	0.0152mm					1/2oz
	Dielectric 1	FR-4	Dielectric	0.1164mm	4.4				
4	L4		Signal	0.0152mm					1/2oz
	Dielectric 3	PP-023	Prepreg	0.55mm	4.1	0.02			
5	L5_GND	CF-004	Signal	0.0152mm					1/2oz
	Dielectric 5	PP-006	Prepreg	0.0994mm	4.1	0.02			
6	Bottom Layer	CF-004	Signal	0.035mm					1oz
	Bottom Solder	Solder Resist	Solder Mask	0.01016mm	3.5		#00FFFFFF		
	Bottom Overlay		Overlay						

#	Name	Material	Type	Weight	Thickness	Dk	Copper Ori	Top Ref	Bottom Ref	Width (W1)	Trace Gap...	Impe...	Devia...	Delay...
	Top Overlay		Overlay											
	Top Solder	Solder Resist	Solder Mask		0.01016mm	3.5								
1	Top Layer	CF-004	Signal	1oz	0.035mm		Above		2 - L2_GND	0.4369mm	0.127mm	50.01	0.02%	5.922...
	Dielectric 4	PP-006	Prepreg		0.0994mm	4.1								
2	L2_GND	CF-004	Signal	1/2oz	0.0152mm		Above	1 - Top Layer	3 - L3_PWR	0.36964mm	0.127mm	49.99	0.02%	6.830...
	Dielectric 2	PP-023	Prepreg		0.55mm	4.1								
3	L3_PWR		Plane	1/2oz	0.0152mm		Above							
	Dielectric 1	FR-4	Dielectric		0.1164mm	4.4								
4	L4		Plane	1/2oz	0.0152mm		Below							
	Dielectric 3	PP-023	Prepreg		0.55mm	4.1								
5	L5_GND	CF-004	Signal	1/2oz	0.0152mm		Below	4 - L4	6 - Bottom...	0.36964mm	0.127mm	49.99	0.02%	6.830...
	Dielectric 5	PP-006	Prepreg		0.0994mm	4.1								
6	Bottom Layer	CF-004	Signal	1oz	0.035mm		Below	5 - L5_GND		0.4369mm	0.127mm	50.01	0.02%	5.922...
	Bottom Solder	Solder Resist	Solder Mask		0.01016mm	3.5								
	Bottom Overlay		Overlay											

Рисунок 3.8 – PCB Stackup

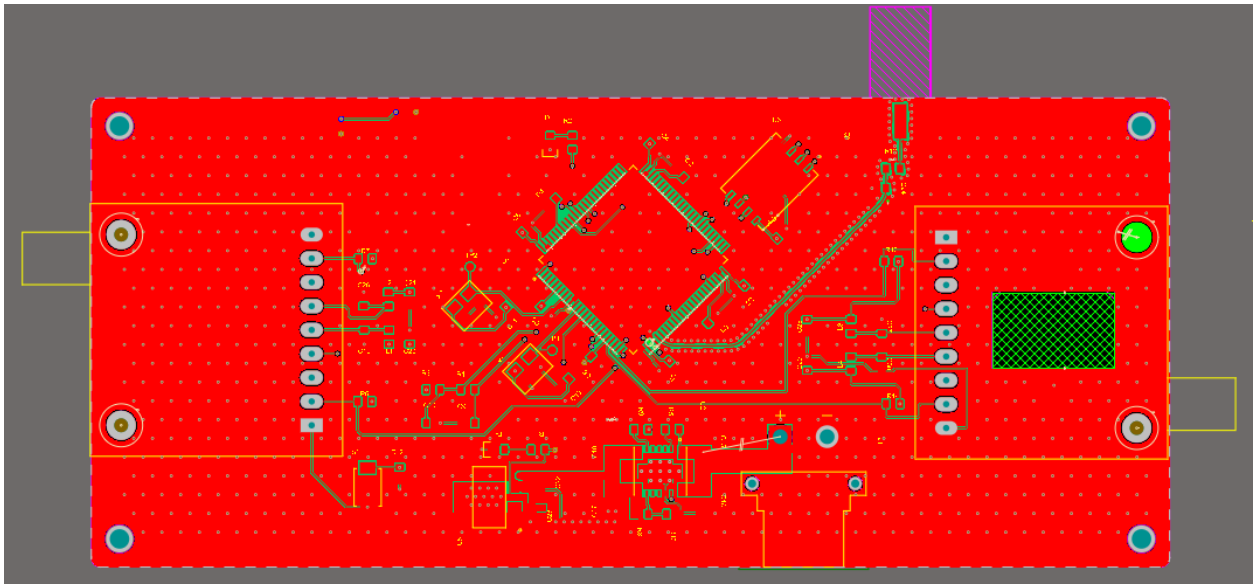


Рисунок 3.9 – Трассировка дорожек используемой печатной платы

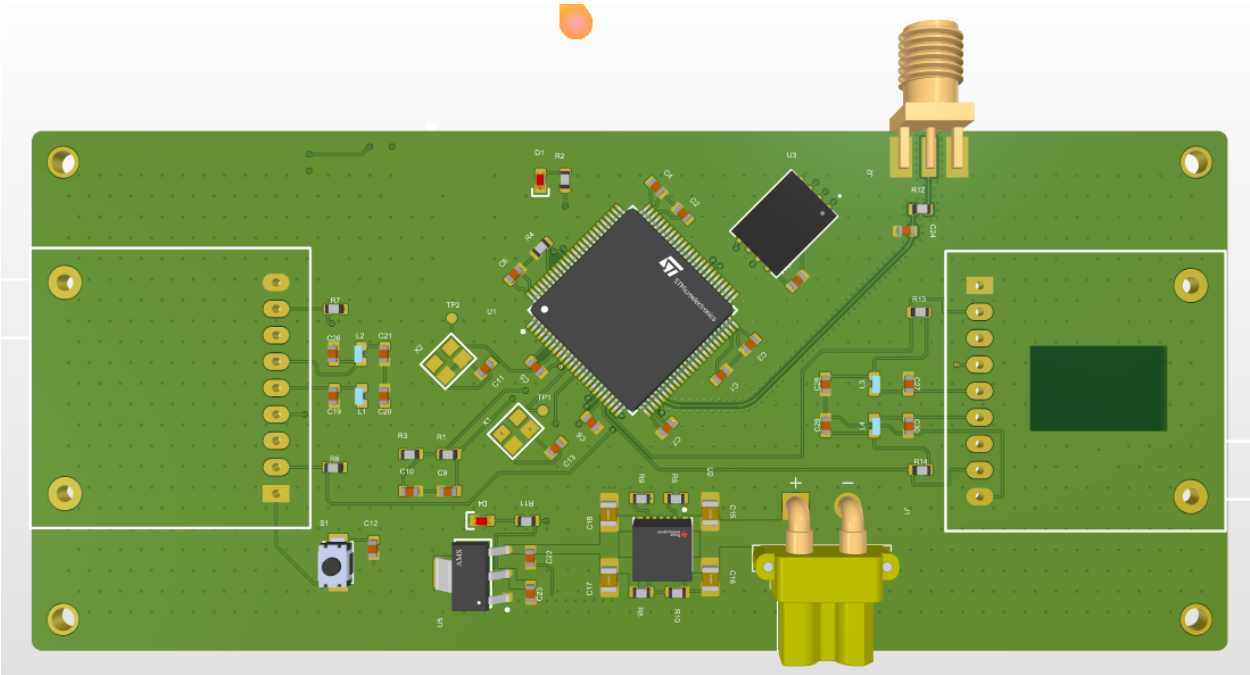


Рисунок 3.10 – Печатная плата

Отработка схемы осуществлялась в ходе эксперимента, блок-схема проведения которого показана на рисунке 3.11. Для отработки схемы был задействован функциональный генератор для генерации синусоидального сигнала частотой 20кГц, также микроконтроллер STM32H743VIT6 для отработки алгоритма постройки фазового портрета исследуемого сигнала. Вывод результатов и пошаговая проверка кода выполнялись в программной среде STM32CubeIDE. Результаты экспериментов представлены на рисунке 3.12. Видно, что предложенная схема действительно обеспечивает построение фрагментов фазовых портретов, отвечающих определенному участку гармонического колебания.

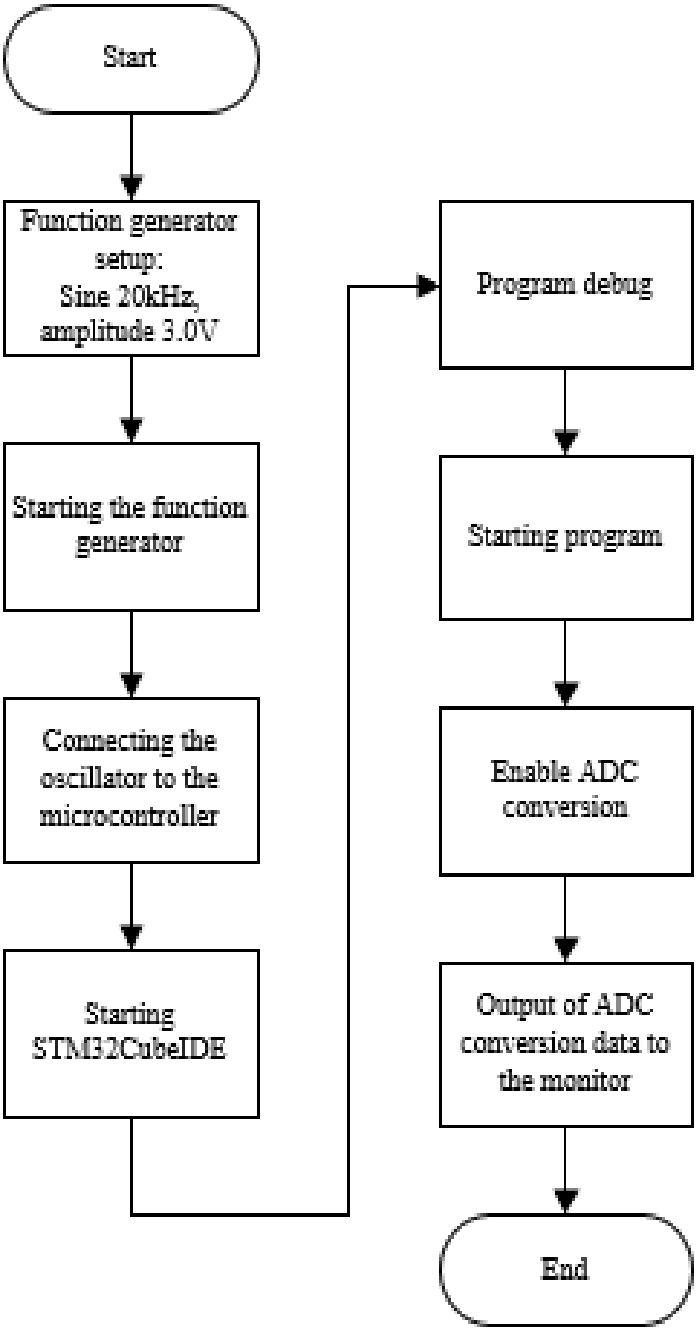
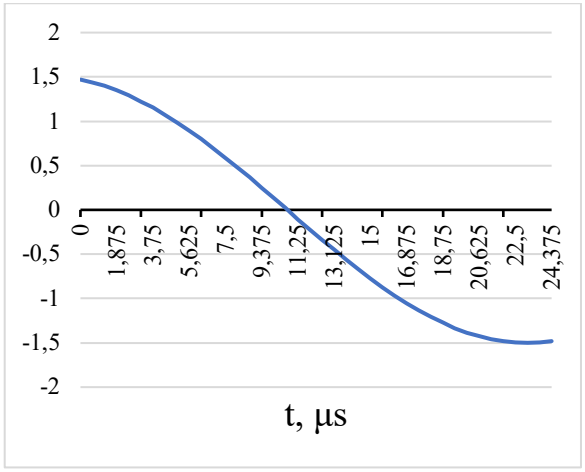
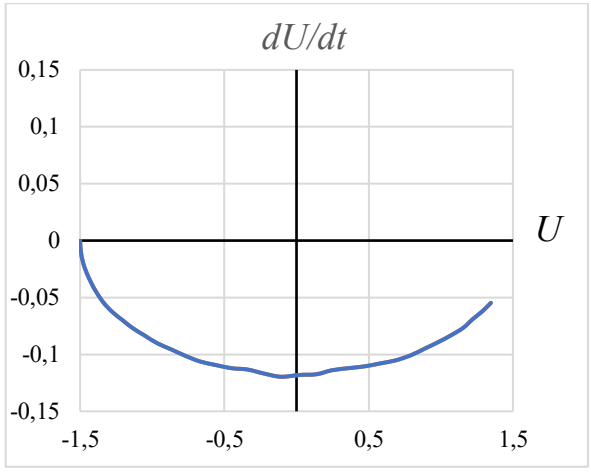


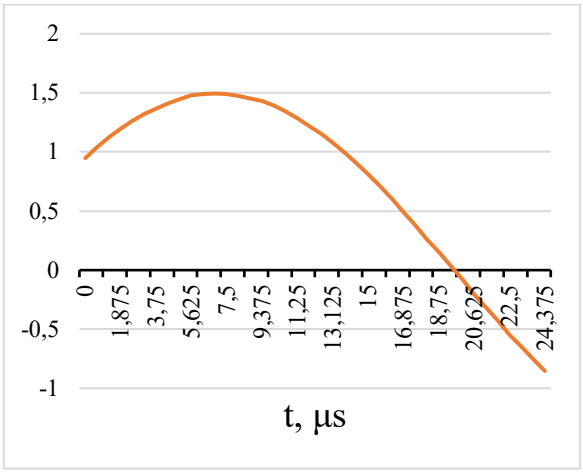
Рисунок 3.11 – Блок-схема эксперимента



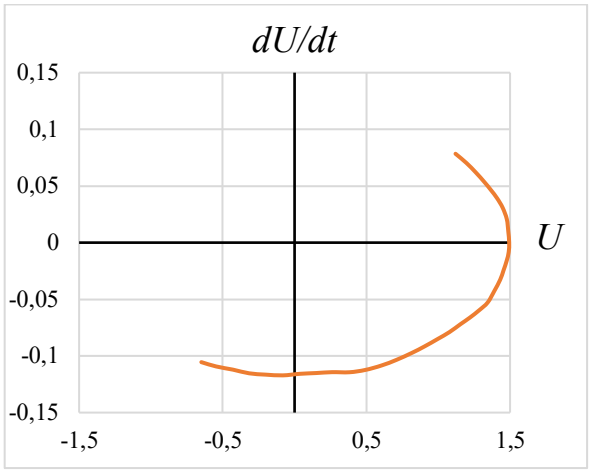
a)



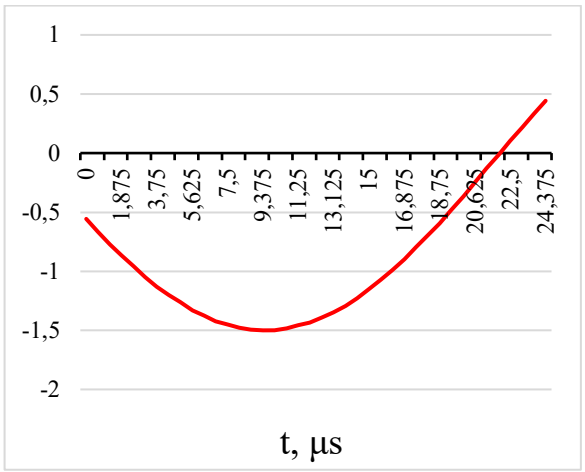
b)



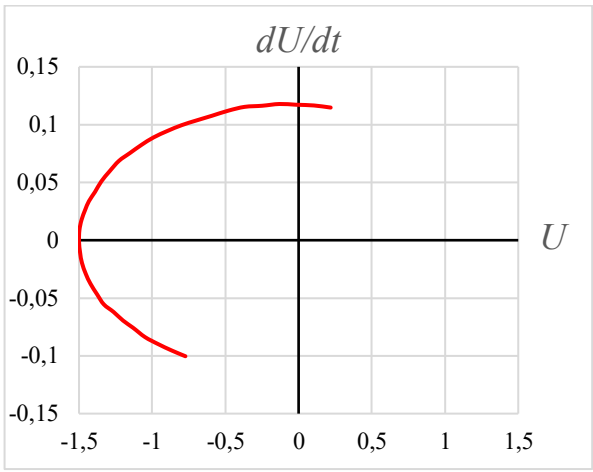
c)



d)



e)



f)

Рисунок 3.12 – Результаты обработки сигналов при помощи АЦП и программы, установленной на микроконтроллер; a), c), e) – примеры оцифрованных колебаний; b), d), f) – отвечающим им фрагменты фазовый портретов

Основным назначением предлагаемого алгоритма на основе фазовых портретов является определение сдвига фазы. Однако он применим также и

для идентификации характера колебаний (гармоническое или квазигармоническое, например). Использование предлагаемого алгоритма для этой цели удобно проследить на конкретном примере.

3.4. Возможные варианты дальнейшего совершенствования предложенного семейства беспилотных вооружений

Как показано в предыдущих главах, анализ характера развития современных систем беспилотных вооружений, в частности, анализ конструкций беспилотных морских дронов, используемых ВСУ, однозначно показывает, что доминирующая тенденция нацелена не столько на использование новых физических или технических принципов, сколько на использование хорошо известных элементов, но в неожиданных комбинациях. Такой подход де-факто отвечает новой парадигме разработки вооружений, ориентированных на максимально упрощение их конструкции и удешевление конечного изделия. Подчеркиваем еще раз, что потеря даже достаточно большого количества роботизированных систем может оказаться вполне приемлемой при условии резкого снижения их стоимости. Тогда достаточно, чтобы цели достиг даже один аппарат из нескольких десятков. Центр тяжести переносится на интеллектуальную составляющую, причем это касается и самих групп роботизированных вооружений (в том числе, управляемых искусственным интеллектом в автономном режиме), и процесса разработки, где перед инженерами встает задача максимально эффективно использовать уже имеющиеся технические решения и физические компоненты в неожиданных комбинациях.

Перспективность такого подхода, де-факто применяемого в данной работе, иллюстрирует еще один пример, связанный уже с разработками роботизированных систем воздушного базирования.

По свидетельству СМИ, гражданские квадрокоптеры широко используются в современных боевых действиях, в том числе, и для целей бомбометания. Например, на них крепится сбрасываемый боеприпас, причем такие системы зачастую изготавливаются способами, близкими к кустарным.

Этот факт, во-первых, демонстрирует недостаточное внимание, уделяемое ранее максимально душевым системам со стороны официальных научных подразделений ОПК, а, во-вторых, реальные возможности для использования максимально простых по конструкции систем в боевых условиях.

Используемые на ЛБС системы по конструкции, как правило, не существенно отличаются от дронов гражданского назначения, совершенствованию конструкции которых посвящена обширная патентная литература, например, [122-124].

Данные аппараты полностью ориентированы на использование классической винтомоторной техники. Однако такой подход далеко не является оптимальным с точки зрения поражения цели. Как показывает характер текущих боестолкновений на территории бывшего СССР,

важнейшим фактором становится состязание в области применения беспилотной авиации, которое включает в себя не только средства РЭБ, но и средства уничтожения беспилотных аппаратов противника. Соответствующие тенденции также отражены в текущей патентной литературе, например, [125]. Данный пример, разумеется, остается уязвимым для критики, поскольку неочевидно, что затраты на обеспечение многоствольной пусковой установки окажутся экономически эффективными в условиях столкновений, когда «роботы сражаются с роботами». Тем не менее, представленный пример заслуживает внимание именно с точки зрения усложнения характера боевого применения беспилотных средств.

Представляется очевидным, что в условиях обострения контр-дроновой борьбы главенствующим фактором является обнаружение именно боевой части системы. Действительно, при условии, что стоимость беспилотных средств неуклонно снижается, носитель боевой части после ее отстрела уже теряет ценность.

Следовательно, допустимо ставить вопрос об использовании комбинированных движителей (т.е. о сочетании движения, обеспечиваемого винтовыми моторами, и движения реактивного характера). Соответствующие тенденции также отражены в текущей патентной литературе, например, [126].

Весьма ярко данная тенденция проявляется в конструкции, предложенной в [127]. Предложенная авторами данного патента ракетная система сочетает в себе преимущества винтомоторного и реактивного движения (рисунок 3.13), что непосредственно видно из представленной на рисунке.

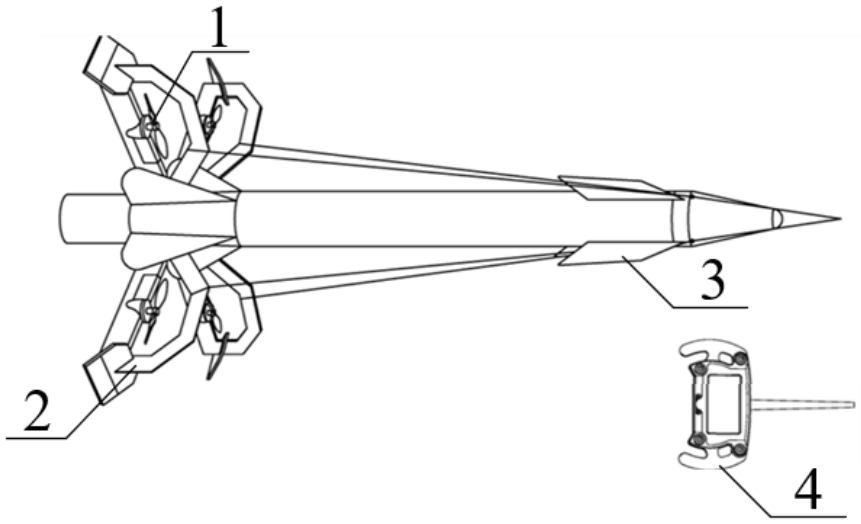


Рисунок 3.13 – Пример конструкция системы, сочетающей винтомоторную и реактивную тягу [127]: 1 – пропеллер, 2 – крылья, 3 – крылья вторичной ракеты беспилотника, 4 – беспроводной пульт управления

В перспективе конструкции такого рода способны решать ту же самую задачу, которую в настоявшее время решают блоки коррекции, устанавливаемые на фугасные авиабомбы советского производства.

Неуправляемый полет авиабомб делает носитель (самолет) уязвимым для средств ПВО противника, а возможность коррекции полета позволяет снизить значение данного фактора.

Сходным образом, сочетание винтомоторной и реактивной тяги позволяет разделить траекторию движения беспилотного аппарата на две части. Движение по первой части траектории осуществляется на винтомоторной тяге, а на второй (где, собственно, и происходит наведение на цель и завершающий высокоскоростной подлет к ней) – на реактивной.

Покажем, что такой подход позволяет реализовать преимущества, создаваемые новой парадигмой развития боевой техники, ориентированной на максимальное снижение стоимости физических компонент вооружений, а также на нестандартное использование уже существующих технических решений и существующих компонент.

Возможность обеспечения реактивного движения вытекает из закона сохранения импульса

$$m_1 v_1 = m_2 v_2 \tag{3.13}$$

где, применительно к рассматриваемой задаче, m_1 – масса боевой части (включая носитель), m_2 – масса вещества, обеспечивающего реактивное движение (например, продуктов сгорания топлива в реактивном двигателе), v_2 – скорость движения данных продуктов, v_1 – скорость боевой части.

Энергия E, затрачиваемая на обеспечение реактивного движения, соответственно дается формулой, в которой учитываются обе составляющие

$$E = \frac{1}{2} m_1 v_1^2 + \frac{1}{2} m_2 v_2^2 \tag{3.14}$$

Формулы (3.13) и (3.14), разумеется, не учитывают различные осложняющие факторы (потери энергии различного рода, сопротивление воздуха и т.д.), однако, они позволяют сделать базовые выводы относительно энергоэффективности обеспечения реактивного движения.

Введем следующие вспомогательные коэффициенты

$$k = \frac{E}{m_1};\ \mu = \frac{m_1}{m_2} \tag{3.15}$$

Тогда из закона сохранения импульса вытекает, что

$$v_2 = \mu v_1 \tag{3.16}$$

А из формулы (3.14) вытекает следующая связь между коэффициентами (3.15) и скоростью движения боевой части (включая носитель)

$$k = \frac{1}{2}(1 + \mu) v_1^2 \tag{3.17}$$

Из формулы (3.17) можно получить следующее выражение для скорости движения боевой части

$$v_1 = \sqrt{\frac{2k}{1+\mu}} = \sqrt{\frac{2Em_2}{m_1(m_2+m_1)}} \tag{3.18}$$

Определим величину Q, которую можно трактовать как удельную энерговооруженность реактивной системы, т.е. отношение энергии, затрачиваемой на обеспечение реактивного движения к суммарной массе реактивной системы

$$Q = \frac{E}{m_2+m_1} \tag{3.19}$$

Тогда скорость движения боевой части определяется формулой

$$v_1 = \sqrt{\frac{m_2 Q}{m_1}} \tag{3.20}$$

Из полученной формулы (3.20), невзирая на ее простоту, следуют важные выводы. Эффективность использования энергии, затрагиваемой на обеспечение реактивного движения, будет тем выше, чем больше отношение «сбрасываемой массы» с «полезной массе». В качестве таковой при реактивном движении традиционного типа выступает боевая часть в совокупности с носителем. Формула (3.20), в том числе, показывает, что традиционный тип реактивного движения обладает не слишком высокой эффективностью по энергозатратам, так как масса продуктов сгорания является достаточно низкой.

Более того, несмотря на простоту, данная формула позволяет определять оптимальные соотношения масс. Для примера рассмотрим простейший случай, когда поражающее действие системы определяется значением импульса боевой части (как это имеет место, например, для обычной пули). Имеем

$$m_1 v_1 = \sqrt{m_1 m_2 Q} \tag{3.21}$$

Допустимо поставить следующую задачу. Какова должна быть масса боевой части, чтобы поражающее действие (в данном случае – значение импульса $m_1 v_1$) было максимальным? При этом предполагается, что суммарная масса объекта, а также энерговооруженность остается постоянной, т.е. величина Q является заданной.

Очевидно, что данная задача сводится к поиску экстремума произведения $m_1 m_2$ при условии, что $M = m_1 + m_2 = const$. Имеем

$$m_1 m_2 = m_1(M - m_1) \tag{3.22}$$

Дифференцируя функцию, стоящую в правой части формулы (3.22) по m_1, получаем, что оптимальным для рассматриваемого случая является значение

$$m_1 = \frac{M}{2} \tag{3.23}$$

Т.е. масса боевой части и «сбрасываемая масса» должны быть одинаковы. Аналогичным образом можно поставить и решить задачу и в том случае, когда поражающее действие определяется другими факторами, например, объемным взрывом. Однако, даже простейший анализ, представленный выше, показывает, что рассматриваемые массы должны быть сопоставимыми.

Исходя из сказанного выше, в настоящей работе предложена следующая конструкция дрона-камикадзе, использующего принцип реактивного движения (рисунок 3.14). На нее получен патент [128] (Приложение А).

Предлагаемая схема содержит: 1 – боевую часть, 2 – заряд, снабженный детонатором, 3 – обтекатель боевой части, 4 – винтовые двигатели, аналогичные тем, что в настоящее время устанавливаются на квадрокоптерах, 5 – обтекатель базового корпуса, 6 – базовый корпус, снабженный стабилизаторами полета, 7 – блок дистанционного управления.

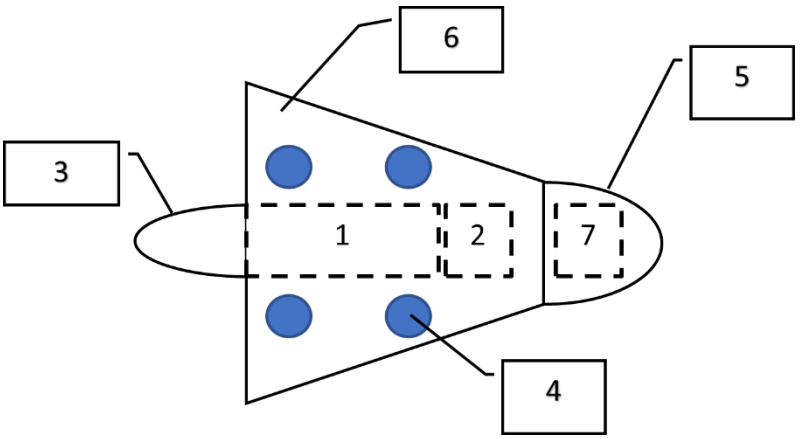


Рисунок 3.14 – Схема дрона-камикадзе с реактивным обеспечением нацеливания боевой части

Основой данной конструкции является базовый корпус, состоящий из элементов (5) и (6). Он несет, в том числе, винтовые моторы (4), которые обеспечивают ее перемещение в воздухе на том же принципе, что и квадрокоптер. Внутри корпуса располагается боевая часть (1), снабженная обтекателем (3), а также снабженный детонатором заряд (2) и блок управления (7).

При подлете к цели на дистанцию выстрела систему наводят на цель, задавая ее положение в пространстве при помощи винтовых моторов (4). Далее осуществляется детонация заряда (2), вследствие чего и боевая часть, и базовый корпус получают ненулевые импульсы, причем направленные в противоположные стороны. Боевая часть направляется на цель, базовый корпус – в обратном направлении. Устойчивость начального вектора полета боевой части обеспечивается стабилизаторами базового корпуса (6). В известном смысле, базовый корпус представляет собой аналог реактивного летательного аппарата, движение которого в заданном направлении обеспечивается стабилизаторами и отстреливаемой от него боевой частью. Тем самым обеспечивается и наведение боевой части на цель, что непосредственно вытекает из закона сохранения импульса, записываемого в векторной форме.

Предлагаемый в данной работе подход может быть также использован и для определения координат сторонних источников радиосигнала (например, месторасположения операторов дронов противоборствующей стороны или месторасположения средств, ведущих радиоэлектронную борьбу). Принцип действия остается тем же самым, отличие состоит только в том, с какой точностью следует определять координаты источника сигнала. Такой метод, разумеется, также применим только в зоне прямой радиовидимости, но, как показывает опыт текущего военного конфликта, средства радиоэлектронной борьбы, применяемые непосредственно вблизи линии боевого соприкосновения, приобретают все большее значение. Следовательно, актуальным является и создание технических средств, обеспечивающих ведение контригры. Очевидно, что такие средства должны быть максимально защищены от возможного воздействия противника (во всяком случае – информационного). Использование оптоволоконных линий связи между БПЛА, составляющими группу, заведомо исключает такое воздействие.

Предлагаемый подход позволяет (в перспективе) также наращивать число БПЛА в группе уже без использования оптоволоконной связи. Соответствующая схема представлена на рисунке 3.15. Рассматриваемая группа включает в себя три БПЛА (1), соединенных друг с другом линиями оптоволоконной связи (2), БПЛА (4), снабженный направленными антеннами (5). Управление группой осуществляется оператором (3) с использованием метода [116]. Однозначность определения координат оператора доказана выше.

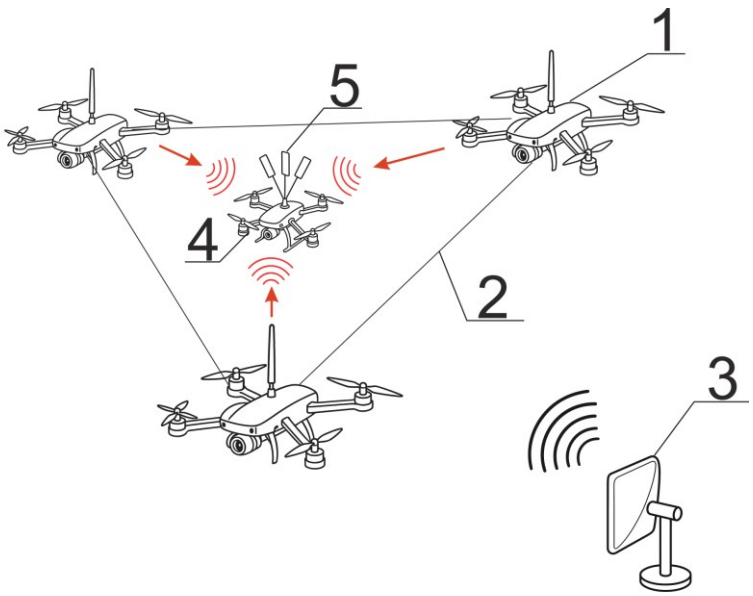


Рисунок 3.15 – Использование направленных антенн для увеличения числа БПЛА в группе [117]

В данной схеме основная группа из трех БПЛА (1) служит, в том числе, ретранслятором управляющего сигнала, предаваемого БПЛА (4). Таких БПЛА в группе может быть несколько. В простейшем случае защита информации от сторонних атак обеспечивается за счет сравнения команд, поступающих от трех различных источников.

Использование направленных антенн, как минимум, позволяет выявлять помехи со стороны противника на основе чисто геометрических факторов. Это можно проиллюстрировать на примере развертывания БПЛА в условиях продолжающегося вооруженного конфликта: во многих случаях эффективная ширина зоны контакта приблизительно соответствует дальности прямой видимости (до 2 км). В таких условиях установление дополнительных каналов передачи команд по радиосвязи противостоящей стороной, как минимум, затруднительно. Следовательно, получение идентичных команд с разных направлений позволяет идентифицировать полученную команду по принципу «свой-чужой».

С аналогичной точки зрения можно также рассмотреть требуемую точность оценки координат оператора. Любое улучшение этой возможности связано с увеличением стоимости, что особенно актуально для военных применений роботизированных систем. В то же время, когда группа БПЛА использует предложенный подход, требования к точности локализации оператора могут быть намеренно ослаблены. Действительно, в данном случае достаточно получить лишь приблизительное местоположение оператора, поскольку вероятность того, что подразделения радиоэлектронной борьбы окажутся в непосредственной близости от своих передовых позиций, ничтожна из-за связанного с этим риска. На этом основании можно заключить, что предложенный подход остается применимым при наблюдаемых уровнях

ошибок локализации оператора, включая те, которые использовались в компьютерных экспериментах.

Для дополнительной защиты (в приложениях, отличных от вышеуказанных) могут быть использованы различные облегченные криптографические протоколы, например, аналогичные [129-131], а также методы обфускации данных [132-134].

Наиболее существенно, что в качестве элемента группы (4) может выступать также и наземный дрон. Очевидно, что для управления такими дронами по оптоволокну существуют непреодолимые технические трудности (деревья, рельеф местности и т.д.). Следовательно, применение наземных дронов заведомо ограничено факторами радиоэлектронной борьбы. Предложенная схема снимает затруднения подобного рода. Этот пример еще раз подчеркивает важность разработки систем защиты информации в условиях прямой видимости: наземные дроны по своей природе предназначены для работы преимущественно вблизи линии соприкосновения. Разработка специальных схем управления для наземных дронов, безусловно, потребует дальнейших исследований; однако этот пример уже показывает, что предложенный подход имеет значительный потенциал для дальнейшего развития.

Эта схема позволяет также решить еще ряд проблем, существование которых выявлено в ходе современных военных конфликтов. В частности, боевое применение дронов, как правило, ограничено достаточно короткими расстояниями (атаки на тяжелую технику и т.д.). Это делает дроны обнаруживаемыми и позволяет обеспечить достаточно эффективное противодействие. Группа, схематически показанная на рисунке 3.15, может быть укомплектована и элементами, позволяющими преодолеть данный фактор.

3.5. Частотный диапазон и допонительные возможности использования предложенного подхода

Таким образом, уже имеющийся опыт использования дронов с дистанционным управлением по оптоволокну, относящийся, в том числе, к реальным боевым условиям в современных вооруженных конфликтах, позволяет перейти к использованию нового подхода к защите информации, основанном на идентификации местоположения оператора и обмене информацией между БПЛА по оптоволокну. При этом для обеспечения оптоволоконной связи между дронами могут использоваться те же самые технические приемы, которые используются для связи между дроном и оператором. Отличие состоит в том, что протяженность линий оптоволоконной связи в соответчики с предлагаемым методом может быть сделан на порядок (или более меньше).

Переход к такому методу защиты информации, в том числе, позволяет существенно снизить требования к производительность бортовых вычислительных системам, так как отпадает необходимость использования

криптографических методов защиты информации, связанным с кодированием сигналов и т.д. В результате возникает целый ряд преимуществ. В частности, пропускная способность канала передачи данных от оператора к рою дронов может быть сделана весьма низкой (менее десятка бит в секунду), так как число исполняемых команд, реально передаваемых группе дронов невелико. Это позволяет перейти к использованию диапазона сравнительно длинных волн, причем существующие ограничения на использование такого радиодиапазона не являются критичными, так как предложенный подход предполагает использование передатчиков невысокой мощности (достаточной для передачи сигнала только в пределах зоны прямой радиовидимости). Допустимо отметить, что аналогичный подход используется в сотовой связи, где один и тот же частотный диапазон может использоваться различными абонентами, но находящимися в пределах разных сот за счет разнесения в пространстве.

Переход к такому диапазону, в том числе, позволяет существенно снизить требования к технологии изготовления используемых электронных схем.

Так, на частоте 300 кГц длина волны примерно равна 1 км, что значительно больше размеров типичных плат. Это позволяет не прибегать к сложному моделированию линий передачи, строгому импедансному согласованию и специализированному экранированию, как это требуется для схем на ГГц диапазонах. В результате структура печатной платы остаётся значительно проще, что снижает производственные затраты. Далее, при использовании диапазона вблизи 300 кГц достаточно вычислительной мощности микроконтроллеров среднего уровня, например, STM32H743. Такие чипы обладают достаточной производительностью для реализации необходимых алгоритмов управления, при этом они дешевле и энергоэффективнее по сравнению с высокопроизводительными решениями, требуемыми для работы на более высоких частотах. Более низкая частота снижает вероятность возникновения паразитных эффектов и электромагнитных помех, что повышает общую надёжность системы управления дроном, особенно при синхронном запуске нескольких устройств по одному управляющему сигналу. В результате, применение длинноволновых сигналов, отвечающих частоте около 300 кГц, позволяет снизить стоимость разработки и производства электроники за счет упрощения конструкции печатных плат и использования более доступных микроконтроллеров, таких как STM32H743, без ущерба для производительности и надёжности системы управления дроном.

Для реализации предлагаемого подхода удобно использовать метод фазовых портретов, который находит применение в различных науках. Нами показано, что он действительно позволяет определять мгновенные значения частоты, амплитуды и фазы как гармонического, так и квазигармонического колебания, в том числе, в том случае, когда анализируются колебания, отвечающие диапазону сравнительно длинных радиоволн. Более того, есть

основания предполагать, что данный алгоритм может быть использован для анализа квазигармонических колебаний в других науках, где они встречаются достаточно часто.

Например, квазипериодические и квазигармонические колебания и волны представляют значительный интерес для нелинейной механики [135, 136]. Такие колебания возникают, например, в турбулентных потоках жидкости [137, 138]. Квазипериодические колебания характерны также для многих природных процессов: например, для солнечной активности в широчайшем диапазоне частот, которые синхронизируют многие геофизические процессы [139]. Квазигармонические колебания развиваются во многих слоях атмосферы, примером являются акустико-гравитационные волны [140,141]. Известны многочисленные примеры того, когда при изменении управляющих параметров системы регулярные колебания (или волны) переходят в квазипериодические [142,143]. Примером являются ионизационные волны в газовом разряде инертных газов низкого давления [144,145], которые при повышении давления могут переходить в квазипериодический режим [146]. Анализ квазипериодических колебаний представляет интерес с точки зрения общих проблем синергетики, так как они во многих случаях связаны с установлением порядка через хаос [147,148].

Для исследования квазипериодических и квазигармонических колебаний в настоящее время применяются различные методы: спектральный анализ [149,150] и различные его модификации (в том числе, связанные с использованием различных разновидностей базисных функций, например, базиса Уолша [151,152]), вейвлет-анализ [153,154], фрактальный анализ [155,156] и т.д. Результат применения таких методов отражает поведение системы в течение достаточно больших промежутков времени. Так, результат вычисления преобразования Фурье заведомо определяется полным профилем исследуемой функции на достаточно протяженном временном интервале. Однако, если частота того или иного процесса изменяется, например, в результате того или иного кратковременного воздействия, то спектральные или аналогичные им методы не позволяют, как минимум, выявить момент времени, отвечающий такому воздействию.

В перспективе данный метод может быть использован и для целей пеленгации, причем этот вывод связан с соображениями фундаментального характера, отраженными в работах [101,102]. А именно, в работе [101] на основании обобщения теоремы Найквиста-Шеннона был проанализирован объем информации, который может быть получен за счет регистрации радиоволн при условии, что приемники произвольного характера сосредоточены в ограниченной области пространства. Было показано, что для каждой монохроматической составляющей этот объем является конечным, но он непосредственно зависит от объема данной области. Это означает, что какие бы средства пеленгации не были использованы, эффективность их работы по соображениям, непосредственно связанным с общей теорией информации, будут тем выше, чем больше область пространства, по которой

они распределены. Более того, как вытекает из результатов работы [101] для регистрации максимального объема информации, которые радиоволны приносят в ограниченный объем, допустимо использовать «точеные» приемники. Это позволяет утверждать, что рой беспилотных аппаратов, объединенных оптоволоконными линиями связи, неуязвимыми для сторонних воздействий также может быть использован в качестве распределенного пеленгатора или средства диагностики самых различных объектов, в том числе, и подповерхностных, с использованием электромагнитных волн радиодиапазона. Данная задача, как отмечалось в предыдущих главах, становится все более актуальной, что, в частности, служит стимулом для дальнейшего совершенствования методов радиоголографии, в том числе, для диагностики подповерхностных объектов [103,104]. Отметим также, что применительно к подповерхностным объектам, в особенности протяжённым, также имеет смысл использовать излучение сравнительно большой длины волны, что также служит аргументом в пользу дальнейших работ, нацеленных на использование групп БПЛА предлагаемого типа.

Таким образом, разработка методов защиты информации, передаваемых от оператора к рою дронов (БПЛА), и основанных на идентификации положения оператора/источника радиосигнала, актуализируется в связи с успешным применением дронов, управляемых по оптоволокну, в ходе реальных боевых действий. Как показано выше, существует возможность обеспечить защиту информации указанного выше характера, используя группы дронов, связанных друг с другом оптоволоконными линиями передачи данных. Предлагаемый метод применим только в зоне прямой радиовидимости, но как показывает опыт упомянутого выше конфликта, обеспечение защищенного управления в зоне прямой радиовидимости является не менее актуальной задачей, нежели управление дронами дальнего действия. Предлагаемый подход, прежде всего, позволяет полностью отказаться от использования шифрования сигналов, что, в свою очередь, резко снижает требования к пропускной способности радиоканала, обеспечивающего передачу данных от оператора к группе БПЛА. Отсюда, с учетом передачи команд на сравнительно небольшие расстояния (порядка километра) вытекает возможность использования длинноволнового радиодиапазона (вплоть до километра по длине волны). Это, в свою очередь, как показано выше, резко снижает требования к электронным схемам и печатным платам, обеспечивающим работу бортовых систем БПЛА. Кроме того, переход к указанному выше радиодиапазону позволяет использовать метод определения координат оператора, основанный на определении фазовых сдвигов при помощи построения фазовых портретов, что обеспечивает детектирование мгновенного значения частоты, фазы и амплитуду как гармонического, так и квазигармонического сигнала. Преимуществом данного метода является простота реализации, а также возможность уверенного детектирования отличий квазигармонического сигнала от гармонического.

Выводы по Главе 3

Переход к указанному радиочастотному диапазону позволяет использовать метод определения координат оператора на основе обнаружения фазового сдвига путем построения фазового портрета. Это обеспечивает обнаружение мгновенных значений частоты, фазы и амплитуды как гармонических, так и квазигармонических сигналов. Преимущество этого метода заключается в простоте реализации, а также в возможности уверенного обнаружения различий между квазигармоническими и гармоническими сигналами.

Предложенный подход обеспечивает масштабируемую основу для расширения групп БПЛА с узлами, использующими направленные антенны и легкие механизмы защиты, поддерживая отказоустойчивые архитектуры и передовые конфигурации, такие как гибридные силовые установки или платформы БПЛА с реактивной тягой.

Глава 4. Особенности вычисления дискретных логарифмов в квази-мерсенновских полях Галуа и некоторые перспективы их практического применения

В данной главе представлен новый подход к вычислению дискретных логарифмов в квази-мерсенновских простых полях Галуа $GF(p)$, $p = 2^n+1$, n – целое число, с опорой на разложения Фурье–Галуа и метод парциальных логарифмов. Продемонстрированы существенные особенности применения метода парциальных логарифмов к случаю квази-мерсенновких полей Галуа. Метод подробно разработан для полей $GF(17)$, где кратность корней из единицы приводит к спектральной структуре, отвечающей 4 тактам, и малому числу ненулевых коэффициентов. Для аппаратной реализации метода использована знакопеременная двоичная кодировка элементов поля. В этом случае умножение на 2 сводится к циклическому сдвигу со сменой знака, что обеспечивает упрощение электронной схемы и потребление вычислительных ресурсов. Работоспособность подтверждена прототипом в Proteus для $GF(17)$. Доказана корректность работы схемы. Показано, что предложенный подход допускает обобщение на поле $GF(257)$, которое соответствует сигналам с 256 уровнями. Обсуждается возможность использования предлагаемого подхода для создания новых криптографических систем, использующих передачу данных по 256 – уровневым каналам. Показано, что предлагаемый подход применим к обфускации данных, предаваемых по 256-уровневым каналам связи.

4.1. Существующие методы вычисления дискретных логарифмов

Понятие дискретного логарифма тесно связано со спецификой полей Галуа, которые находят все большее применение в самых различных информационных технологиях, в том числе в криптографии [157-159], теории кодирования [160,161], цифровой обработке сигналов [162,163] и т.д. А именно, из самых общих положений абстрактной алгебры [164] вытекает, что произвольный элемент поля Галуа может быть представлен в виде степени примитивного элемента θ.

$$x = \theta^m \tag{4.1}$$

В формуле (4.1) показатель степени m может быть заменен на значение $m_1 \equiv m(p^n - 1)$, где скобки означают, что число m берется по модулю $p^n - 1$, где p -характеристика рассматриваемого поля Галуа, n – степень алгебраического расширения.

Данное уточнение существенно, так как любое поле Галуа по определению представляет собой конечное коммутативное тело (в алгебраическом смысле данного термина). Тот факт, что число элементов поля Галуа конечно, выражается, в частности, в том, что все его ненулевые элементы удовлетворяют соотношению

$$x^{p^n-1} = 1 \tag{4.2}$$

Дискретный логарифм определяется через сопоставление

$$x \to m \tag{4.3}$$

Проблема вычисления дискретных логарифмов [165] тесно связана со многими задачами из области криптографии [166-168], в том числе, квантовой [169-171]. В литературе представлен целый ряд алгоритмов, предназначенных для вычисления дискретных логарифмов: Joux's algorithm [172], baby step–giant step algorithm [173,174], Pohling–Hellman's algorithm [175,176] и т.д. Для конечных полей малой характеристики применим эвристические квазиполиномиальные алгоритмы [177], для квантовых вычислений - Shor's algorithm [178,179]. До последнего времени рассматриваемая задача была далека от общего решения. Более того, в [180,181] подчеркивалось, что сложность вычисления дискретных логарифмов была использована для построения ряда криптографических методов. Как отмечено в [182], воспринимаемая сложность задачи о дискретном логарифме обусловлена не неопределенностью существования решения, а самой проблемой поиска.

Новый алгоритм отыскания дискретных логарифмов, применимый в самом общем случае, был предложен в работе [183]. В той же работе, однако, подчеркивалось, что предлагаемый в ней подход, вообще говоря, требует учета специфики конкретного поля Галуа. Важность учета этого факта отмечалась также в [182], где данный вывод был подкреплен конкретными примерами.

Такая специфика наиболее наглядно проявляется в случае полей Галуа, которые, в соответствии с работами [184], могут быть названы квази-мерсенновскими. К этому классу мы относим такие поля $GF(p)$, для которых $p = 2^k + 1$. Напомним, что простые числа Мерсенна, которые также широко используются в современных информационных технологиях [185,186], определяются похожей формулой $p = 2^k - 1$, что и определяет правомочность используемого термина «квази-мерсеннвские простые числа». Полагается оправданным использование специального термина для данного класса полей Галуа, в силу их важности для практического использования.

С практической точки зрения наибольший интерес представляют два первых квази-мерсенновские числа: 17 и 257. Число ненулевых элементов в первом из таких чисел составляет 16, а во втором – 256. Система счисления с основанием 16 используется в информатике и компьютерной технике, например, для записи адресов памяти, определения цветов (в формате RGB [187]), представления кодов символов, а также в низкоуровневом программировании [188]. Число 256 отвечает 8-разрядном устройствам, которые также широко используются на практике (голосовая связь и простое

аудио без сложных кодеков [189], широкоимпульсная модуляция для плавного диммирования LED [190] и т.д.).

В данной главе показано, что методика вычисления дискретных логарифмов, предложенная в цитированной выше работе [183], может быть распространена на вычисление дискретных логарифмов в квази-мерсенновских полях Галуа (с учетом специфики последних).

Демонстрируется также, что новый подход к вычислению дискретных логарифмов создает вполне определенные перспективы для разработки новых методов обфускации данных [191,192].

Совершенствование методов обфускации данных представляет интерес по следующим причинам. В этой связи уместно отметить, что существующие подходы к защите информации отличаются большим разнообразием, в том числе, и по отношению к решаемым задачам. Наряду с достаточно сложными криптографическими системами (например, [193-195]) на практике используются «легкие» криптографические протоколы (например, для устройств, отвечающих концепции Интернета вещей [129,130], микроконтроллеров с криптографической нагрузкой [131,196] и т.д.). «Легкие» криптографические протоколы могут также представлять интерес для формирования групп беспилотных летательных аппаратов, использующих обмен информацией между элементами группы [197-199]. В этом случае криптографическая защита информации может быть скомбинирована с методами, предложенными в [93,94]. Отметим, что такие лёгкие криптографические протоколы как SPONGENT и PRESENT также используют конечные алгебраические поля для минимизации вычислительных затрат на устройствах с ограниченными ресурсами [200,201]. (Нужно отметить, что легкие криптографические протоколы, такие как SPONGENT и PRESENT, также используют конечные алгебраические поля для минимизации вычислительных затрат на устройствах с ограниченными ресурсами. [203,204].) Более того, методы, предложенные в [93,94], могут быть скомбинированы с и методами обфускации данных, так как указанные методы требуют только минимальной дополнительной защиты.

4.2. Метод вычисления дискретных логарифмов на основе алгебраической дельта-функции

В работе [183] было показано, что дискретный логарифм $Dl(x)$ элемента x в поле Галуа $GF(p)$ может быть вычислен по следующей формуле

$$Dl(x) = \sum_{n=0}^{n=p-2} n\delta(x - \theta^n), \tag{4.4}$$

Идея вывода формулы (4.4) основывается на использовании алгебраической дельта-функции, предложенной в [114]. Данная функция определяется как

$$\delta(x - x_0) = 1 - (x - x_i)^{p-1} \quad (4.5)$$

Она обладает следующим свойством, которое вытекает непосредственно из формулы (4.2)

$$\delta(x - x_0) = \begin{cases} 1, & x = x_i \\ 0, & x \neq x_i \end{cases} \quad (4.6)$$

Вывод формулы (4.4) основывается на том, что элементы поля Галуа можно нумеровать произвольным образом, в том числе, и отталкиваясь от степени примитивного элемента. Тем самым, каждому слагаемому в формуле (4.4) ставится вполне определенное значение дискретного логарифма, определяемое степенью n элемента θ^n. Подчеркивается, что суммирование в (4.6) распространяется на $n = p - 2$. Это отражает свойство, $\theta^{p-1} = 1$, и, следовательно, $Dl(x = \theta^{p-1}) = 0$. Формула (4.4) подчеркивает, что операция дискретного логарифмирования может быть вычислена для произвольных значений x.

В цитированной выше работе [183] также было показано, что формула (4.4) может быть приведена к виду

$$Dl(x) = -\sum_{k=1}^{k=p-1} x^{p-1-k} Q_k \quad (4.7)$$

где

$$Q_k = \sum_{n=1}^{p-2} n\, \theta^{nk} \quad (4.8)$$

Там же подчеркивалось, что формула (4.7) может быть получена и независимым образом, причем в общем случае (т.е. для произвольной функции одной переменной, принимающей значения в рассматриваемом поле Галуа – предполагается, что аргумент данной функции также принадлежит данному полю). Альтернативной способ вывода формулы (4.8) и ее обобщения основывается на использовании прямого и обратного преобразование Фурье-Галуа. А именно, если исходная функция $f(x)$ задана в табличной форме (такая форма представления традиционно используется в работах по математической логике [202,203]), то можно перейти и к таблице, в которой значения функции ставятся в соответствие показателям степени, что можно выразить через табулирование рассматриваемой функции в виде $f(\theta^l)$. Совершая преобразование Фурье-Галуа над функцией, задаваемой в табличной форме, можно получить явное алгебраическое выражение для рассматриваемой функции одной переменной так как в выражение для обратного преобразования Фурье-Галуа может входить переменная, принимающая произвольные значения.

Тем самым, формула (4.7), как и подчеркивалось выше, является частным случаем представления функции одной переменной (в полях Галуа), заранее

представляемой в табулированной форме. Для наглядности, приведем формулу, обобщающую (4.8):

$$Q_k = \sum_{l=1}^{l=p-1} f(\theta^l)\,\theta^{kl}\,, \tag{4.9}$$

Далее, в работе [183] было показано, что существуют поля Галуа, для которых вычисление дискретного логарифма может быть существенно упрощено за счет перехода к парциальным цифровым логарифмам. Такой подход удобно использовать для полей следующего вида.

Если $GF(p)$ – поле Галуа, то p – простое число. Число $p-1$, следовательно, таковым не является и допускает разложение вида

$$p - 1 = p_1^{q_1} p_2^{q_2} \dots p_k^{q_k} \tag{4.10}$$

Такое разложение отвечает использованию инструментов модулярной арифметики (что соответствует использованию residue number systems [204,205]). Разложению (4.10) отвечает также следующему преставлению произвольного ненулевого элемента поля $GF(p)$

$$z = g_1^{s_1} g_2^{s_2} \dots g_k^{s_k} \tag{4.11}$$

где показатели $s_i = 0,1,2,\dots,\mathrm{s}_{im}$, g_i – элементы рассматриваемого поля, удовлетворяющее условиям

$$g_i{}^{p_1^{q_1}} = 1, \tag{4.12}$$

$$\mathrm{s}_{im} = \frac{p-1}{p_i^{q_i}} - 1 \tag{4.13}$$

Значение дискретного логарифма m может быть представлено через величины s_i, которые интерпретируются как парциальные дискретные логарифмы, как

$$m \equiv e_1 s_1 + e_2 s_2 + \dots + e_N s_N, mod(p-1) \tag{4.14}$$

где e_i – идемпотентные взаимно аннулирующие элементы. Эти элементы сформированы по правилу, использованному, в частности, в [206]

$$e_i = \alpha_i \prod_{i \neq j}^{N} p_j^{q_j} \tag{4.15}$$

где α_i – целое число. Выбор данных чисел осуществляется исходя из условия

$$e_i e_i = 1 \tag{4.16}$$

Как показано в [183], значения s_i для каждого конкретного x могут быть вычислены по формуле

$$s_i(x) = \sum_{m=1}^{m=p-1} s_i(\theta^m)\delta(x-\theta^m), i = 1,2,\dots,k \tag{4.17}$$

где все функции $s_i(\theta^m)$ известны, на участке от 1 до $p_i^{q_i}$ они даются формулой

$$s_i(\theta^m) = \begin{cases} m, m \le p_i^{q_i} - 1 \\ 0, m = p_i^{q_i} \end{cases}, \tag{4.18}$$

Формула (4.17), как показано в [183], также приводится к представлению через ряд Фурье-Галуа, а именно

$$S_i(x) = -\sum_{n=1}^{n=p-1} x^{p-1-n} Q_{ni} \tag{4.19}$$

где

$$Q_{ni} = \sum_{l=1}^{l=p-1} s_i(\theta^l)\,\theta^{nl}, \tag{4.20}$$

Преимущество формулы (4.20) по сравнению с формулой (4.8) состоит в том, что функции (4.18) обладают периодом, который в несколько раз меньше, чем значение $p-1$. Следовательно, только некоторые величины Q_{ni}, получаемые по формуле (4.20), отличаются от нуля.

Такой подход позволяет существенно упростить вычисление дискретного логарифма для многих полей $GF(p)$ [183]. Однако данное преимущество отсутствует в важных частных случаях, отвечающих квази-мерсенновским полям Галуа [184], для которых $p-1=2^n$, где n целое число. Можно видеть, что в данном случае представление (4.14) будет содержать только одно слагаемое. Соответственно, представление (4.11) – только один сомножитель. Квази-мерсенновские поля Галуа не могут не представлять прикладного интереса: в частности, число ненулевых элементов поля $GF(257)$ равно 256, т.е. разрядности многих двоичных устройств, используемых на практике (8 двоичных разрядов).

Исходя из этого допустимо поставить следующую задачу.

- Разработать алгоритм, аналогичный алгоритму, построенному на использовании парциальных дискретных логарифмов, но применимый для квази-мерсенновских полей Галуа, а также продемонстрировать его применимость для решения прикладных задач, в частности, из области защиты информации.

4.3. Аналог парциальных дискретных логарифмов для квази-мерсенновских полей Галуа

Выражение (4.1), которое лежит в основе понятия дискретного логарифма, для поля $GF(17)$ можно представить в форме

$$x = \theta^{4m_1+m_2} = (\theta^4)^{m_1}\theta^{m_2}\ , \tag{4.21}$$

Аналогично, для поля $GF(257)$ – в форме

$$x = \theta^{16m_1+m_2} = (\theta^{16})^{m_1}\theta^{m_2}\ , \tag{4.22}$$

Очевидно, что в первом случае $m_2 \equiv m(4)$, а во втором - $m_2 \equiv m(16)$. Очевидно также, что для вычисления дискретного логарифма достаточно вычислить величины m_1 и m_2, так как $m = 4m_1 + m_2$ и $m = 16m_1 + m_2$ в первом и втором случае, соответственно.

Рассмотрим вначале случай поля $GF(17)$. Величины m_1 и m_2 можно вычислить по формулам, аналогичным формуле (4.17).

$$m_{1,2}(x) = \sum_{s=1}^{s=p-1} m_{1,2}(\theta^s)\delta(x-\theta^s) \tag{4.23}$$

Отличие состоит только в характере функций $m_{1,2}(\theta^s)$, стоящих под знаком суммы. Конкретно,

$$m_1(\theta^s) \equiv s(4) \tag{4.24}$$

$$m_2(\theta^s) = \left[\frac{s}{4}\right] \tag{4.25}$$

где $[a]$ – целая часть числа a.

Функция $m_1(\theta^s)$ является периодической с периодом 4, причем на интервал от 0 до 15 укладывается четыре ее периода. Функция $m_2(\theta^s)$ является кусочно-постоянной, она изменяется скачками, изменяясь в пределах от 0 до 3. Для наглядности вид этих функций представлен на рисунке 4.1.

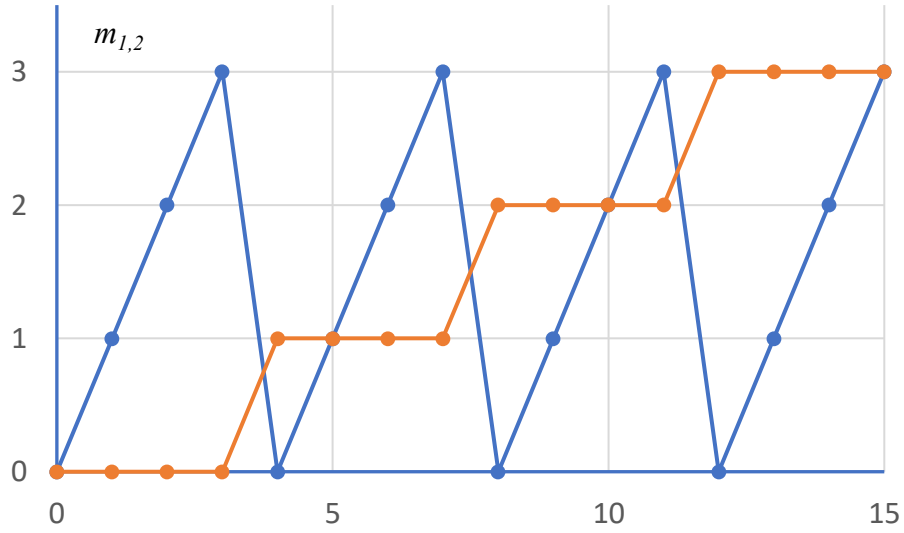


Рисунок 4.1 – Функции $m_1(\theta^s)$ (синяя линия) и $m_1(\theta^s)$ (красная линия) для случая поля $GF(17)$

В соответствии с методикой [183], от формулы (4.23) можно перейти к представлению через ряд Фурье-Галуа, т.е. записать аналог формулы (4.20) для рассматриваемого случая. В частности, обе рассматриваемые функции можно представить рядом Фурье-Галуа.

$$m_{1,2}(x) = -\sum_{n=1}^{n=p-1} x^{p-1-n} Q_n^{(1,2)} \tag{4.26}$$

где

$$Q_n^{(1,2)} = \sum_{s=0}^{s=p-2} m_{1,2}(\theta^s)\, \theta^{ns}\ , \tag{4.27}$$

В поле $GF(17)$ имеется 8 примитивных элементов, одним из которых является 6. С использованием любого из примитивных элементов можно построить базисный набор, который включает в себя следующие последовательности

$$w_k = \left(1, \theta^k, \theta^{2k}, \theta^{3k}, \dots, \theta^{(p-2)k}\right); k = 0,1, \dots, p-2 \tag{4.28}$$

Такие последовательности являются ортогональными [163]

$$\sum_{j=0}^{j=p-2} w_{k_1}^{(j)} w_{k_2}^{(j)} = \begin{cases} 1, k_1 \equiv k_2 \left(mod\ (p-1)\right) \\ 0, k_1 \not\equiv k_2 \left(mod (p-1)\right) \end{cases} \tag{4.29}$$

Величины (4.27) представляют собой разложения функций $m_{1,2}(\theta^s)$ по такому базисному набору.

Пример базисного набора ортогональных последовательностей для случая $GF(17)$ для наглядности представлен в Таблице 4.1. Значения, представленные в данной таблице, получены в соответствии с формулой (4.28), т.е. каждое из представленных значений вычисляется как $w_{kj} = \theta^{kj}$, где k и j изменяются от 1 до 15, а $\theta = 6$.

Таблица 4.1 – Базисный набор ортогональных последовательностей для $GF(17)$

											0	1	2	3	4	5
				2				4	6	1	5		3	0		
					6	5	3						6	5	3	
		2		1	3				6					4	5	0
			6	3			6	3			6	3			6	3
			5			1		2	6	0		4	3			
			3		6			5			3		6			5
		4			3	2	5		6			0				1
		6		6		6		6		6		6		6		6
		1				0			6		5	2	3			4
0		5			6		3			5			6		3	
1					3	4		0	6	2		1			5	
2		3	6			3	6			3	6			3	6	
3		0	5	4					6				3	1		2
4			3	5	6						3	5	6			
5				0	3		5	1	6	4				2		

Можно видеть, что из 16-ти последовательностей только четыре являются периодическими с периодом, равным 4. Соответствующие ячейки выделены в Таблице 4.1 цветом. Этот факт не является случайным, он вытекает из того, что в рассматриваемом поле имеет место

$$(x^4)^4 = 1, \forall x \tag{4.30}$$

Т.е. рассматриваемое поле содержит четыре корня из единицы (1, 4, 16 и 13). В представлении через отрицательные числа эти корни выражаются как 1, 4, -1 и – 4.

Следовательно, только в разложении функции $m_1(\theta^s)$ по последовательностям из рассматриваемого базиса будут учувствовать только четыре из них, иначе для этого случая из величин $Q_n^{(1)}$ только четыре будут отличны от нуля.

$$Q_{4n_1}^{(1)} = 4\sum_{s=0}^{s=3} s\,\theta^{4n_1 s}; n_1 = 0,1,2,3\ , \tag{4.31}$$

Из (4.30) вытекает, что $\theta^{4n_1} = 4^{n_1}$, поэтому формуле (4.31) можно представить в максимально наглядном виде (все вычисления, как и выше, проводятся в смысле используемого поля Галуа)

$$Q_{4n_1}^{(1)} = 4(4^{n_1} + 2\cdot 4^{2n_1} + 2\cdot 4^{3n_1}); n_1 = 0,1,2,3\ , \tag{4.32}$$

Покажем, что аналогичный вывод справедлив и по отношению к функции $m_2(\theta^s)$.

Подставляя формулу (4.25) в (4.27), получаем

$$Q_n^{(2)} = \sum_{s=4}^{s=7}\theta^{ns} + 2\sum_{s=8}^{s=11}\theta^{ns} + 3\sum_{s=12}^{s=15}\theta^{ns}\ , \tag{4.33}$$

Вынесем в данном выражении множители $\theta^{4n} = 4^n$ за знаки суммирования. Имеем

$$Q_n^{(2)} = (4^n + 2\cdot 4^{2n} + 3\cdot 4^{3n})\sum_{s=0}^{s=3}\theta^{ns}\ , \tag{4.34}$$

Видно, что с точностью до постоянного множителя, относящегося к первому из четырех периодов, выражение (4.34) совпадает с выражением (4.32).

Покажем, что аналогичный результат справедлив и для поля $GF(257)$, представляющего непосредственный прикладной интерес. Для данного поля имеет место

$$(x^{16})^{16} = 1, \forall x \tag{4.35}$$

Одним из корней 16-той степени из единицы является элемент поля 2, т.е.

$$\theta^{16} = 2 \tag{4.36}$$

В частности, это означает, что можно пользоваться соотношениями

$$\theta^{m} = \theta^{16m_1+m_2} = 2^{m_1}\,\theta^{m_2} \tag{4.37}$$

Используя формулы (37), можно получить аналоги формул (4.31) и (4.33) для рассматриваемого поля

$$Q_{16n_1}^{(1)} = 16\sum_{s=0}^{s=15} s\,\theta^{16n_1 s} = 16\sum_{s=0}^{s=15} s\,2^{n_1 s};\; n_1 = 0{,}1,\ldots,15\ , \tag{4.38}$$

$$Q_{n}^{(2)} = \left(\sum_{s=0}^{s=15} s\,2^{ns}\right)\left(\sum_{s=0}^{s=15} \theta^{ns}\right), \tag{4.39}$$

Подчеркиваем, что суммы в выражении (4.39) вычисляются независимым друг от друга образом.

Представим некоторые оценки, позволяющие сравнить предлагаемый подход с существующими методами вычисления дискретных логарифмов. Для малых полей GF(17) и GF(257) предложенные реализации дискретного логарифма обес-печивают 1 такт на символ при минимальных ресурсах: комбинаторная версия для GF(17) обходится без ПЗУ, а табличная для GF(257) требует порядка 2 кбит ROM (256×8), что на ПЛИС реализуется примерно в 32 LUT6 или одном BRAM. Извест-ные алгоритмы вычисления дискретных логарифмов — Pohlig–Hellman (PH) и Baby-Step/Giant-Step (BSGS) — оказываются многотактными: для GF(257) PH требует порядка трёх десятков тактов на символ (поразрядное извлечение), а BSGS — не менее 16 шагов из-за $\sqrt{|G|}$ -зависимости. В итоге именно для малых полей «жёсткое» требование детерминированной однотактной обработки выполнятся только для предложенного метода вычисления дискретных логарифмов.

Покажем, что предлагаемый метод вычисления дискретных логарифмов может быть использован для практических целей.

4.4. Алгоритм обфускации данных на основе вычисления дискретных логарифмов

Как подчеркивалось выше, в настоящее время существует широкий спектр систем защиты информации, отличающихся, в том числе, по назначению. Уместно также еще раз подчеркнуть, что все более широкое использование БПЛА различного назначения делает актуальным совершенствование криптографических методов в части снижения вычислительных ресурсов, требуемых для шифрования и дешифрования [207-

209]. Однако могут быть предложены и альтернативные подходы к защите информации [93,94], которые, в том числе, могут быть скомбинированы с методами обфускации данных. Такие методы, впрочем, могут быть применены и для других целей [210,211].

Существенное упрощение метода вычисления дискретных логарифмов позволяет предложить следующий способ обфускации данных (рисунок 4.2). Схема предназначена для случая использования канала связи, содержащему 256 уровней. Работа схемы основана на том, что каждому из таких уровней можно поставить в соответствие ненулевой элемент поля $GF(257)$.

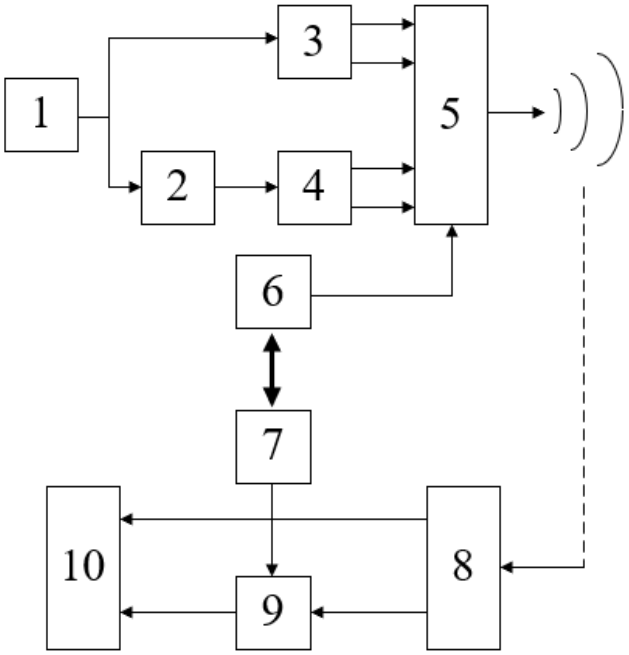


Рисунок 4.2 – Блок-схема системы обфускации данных на основе вычисления дискретных логарифмов

Исходный сигнал $U(t)$ формируется блоком 1. Блок 2 вносит в данный сигнал некоторую задержку по времени, т.е. на его выходе формируется сигнал $U(t+T_0)$. Блоки 3 и 4 осуществляют вычисление парциальных дискретных логарифмов, отвечающих формулам (4.38) и (4.39), т.е. на их выходах формируются функции $f_1(t)$ и $f_2(t)$, отвечающие представлению исходного сигнала в форме

$$U(t) = 2^{f_1(t)}\theta^{f_2(t)}, \tag{4.40}$$

Функции $f_1(t)$ и $f_2(t)$, таким образом, обладают разрядностью 4 бита. Блок 5 осуществляет операцию, аналогичную даваемую формулой (4.40), но используя задержку по времени. Конкретно, сигнал на его выходе отвечает формуле

$$U(t) = 2^{F_1(t)}\theta^{F_2(t)}, \tag{4.41}$$

где

$$F_1(t) = \zeta(t) f_1(t) + \big(1 - \zeta(t)\big) f_1(t + T_0)\,, \tag{4.42}$$

$$F_2(t) = \big(1 - \zeta(t)\big) f_2(t) + \zeta(t) f_2(t + T_0)\,, \tag{4.43}$$

Функция $\zeta(t)$, которая принимает значения 0 или 1, обеспечивает шифрование. Она генерируется блоком 6 в передающей части схемы и синхронизируется с блоком 7, относящимся к принимающей части. В ней операции вычисления парциальных цифровых логарифмов осуществляются блоком 8, блок 9 вносит задержку по времени, а блок 10 осуществляет восстановление исходного сигнала.

Для экономии вычислений достаточно передавать лишь ключ. Очевидно, что объем данных, подлежащих шифрованию, в этом случае гораздо меньше, чем объем данных, которые содержатся в исходном сигнале. При этом сам поток $\zeta(t)$ может порождаться от физического источника, например, термошума резистора. Оцифрованный и предварительно «обелённый» шум может быть использован для генерации $\zeta(t)$, который затем детерминированно воспроизводится на приёмной стороне из того же начального состояния.

Для наглядности, проведем также сопоставление с лёгкими криптопримитивами по ресурсу, что является допустимым, несмотря на различие классов решаемых задач, особенно в контексте комбинирования предлагаемых методов с методами [93,94]. Компактные блочные шифры и лёгкие хэши (например, PRESENT, SPONGENT) занимают ~0.7–2 тыс. GE в серийных реализациях и обрабатывают данные блоками с десятками тактов на блок (при 1 раунде за такт). Предлагаемый подход требует существенно более низких ресурсов: GF(17) — единицы LUT без ROM; GF(257) — небольшая ROM-таблица (~2 кбит) и та же 1-тактная обработка на символ. Таким образом, когда цель — не криптографическая защита, а обратимое перемешивание/интерливинг и конечнопольная арифметика с жёсткими ограничениями по времени/площади/энергии, предлагаемый подход имеет явное преимущество по латентности и аппаратной стоимости.

Отметим, что такой подход отвечает также современным тенденциям на использование физических процессов для защиты информации (например, основанные на использовании невоспроизводимых последовательностей данных [82-84]), но могут дополнить их, используя методы обфускации.

4.5. Алгоритм перехода к знакопеременной двоичной системе счисления для квази-мерсенновских полей Галуа

В работе [184] было показано, что для вычисления дискретных логарифмов в квази-мерсенновских полях Галуа целесообразно использовать

двоичное знакопеременное представление чисел. Такое представление по виду совпадает с обычным представлением чисел в двоичной форме

$$A = 2^n \cdot a_n + \cdots + 2^1 \cdot a_1 + 2^0 \cdot a_0 \quad (4.44)$$

Отличие состоит в том, что a_i принимают значения +1 и – 1. В частности, для поля $GF(17)$ выражение (4.44) принимает вид

$$A = 2^3 \cdot a_3 + 2^2 \cdot a_2 + 2^1 \cdot a_1 + 2^0 \cdot a_0 \quad (4.45)$$

Обоснование возможности использования представления (4.44) состоит в следующем [184]. Комбинации вида (4.44) отвечают перечислению всех нечетных чисел в диапазоне $-2^{n+1} < A < 2^{n+1}$. Таких чисел насчитывается ровно 2^n, в частности для случая поля $GF(17)$ число таких комбинаций равно 16. Число 2^n, в свою очередь, равно числу ненулевых элементов квази-мерсенновского поля Галуа $GF(2^n + 1)$. К любому из чисел в диапазоне $-2^{n+1} < A < 0$ можно прибавить $2^n + 1$. Эта операция отвечает переходу от одного «представителя» элемента поля Галуа (т.е. определенного класса вычетов) к другому «представителю» того же самого элемента. Тем самым доказывается, что нечетные числа из указанного диапазона отвечают четным числам из диапазона $0 < A < 2^{n+1}$.

Для наглядности элементы поля $GF(17)$ в знакопеременной кодировке показаны в Таблице 4.2.

Таблица 4.2 – Элементы поля $GF(17)$ в знакопеременной двоичной кодировке

a_3	a_2	a_1	a_0	$A(\pm)$	A
1	1	1	1	15	15
1	1	1	-1	13	13
1	1	-1	1	11	11
1	1	-1	-1	9	9
1	-1	1	1	7	7
1	-1	1	-1	5	5
1	-1	-1	1	3	3
1	-1	-1	-1	1	1
-1	1	1	1	-1	16
-1	1	1	-1	-3	14
-1	1	-1	1	-5	12
-1	1	-1	-1	-7	10
-1	-1	1	1	-9	8
-1	-1	1	-1	-11	6
-1	-1	-1	1	-13	4
-1	-1	-1	-1	-15	2

Преимущество использования знакопеременной кодировки для полей $GF(2^n + 1)$ состоит в следующем. От представления (4.44) можно перейти к форме, аналогичной традиционной, т.е. записывать число (точнее, элемент поля Галуа рассматриваемого типа) следующим образом

$$A = a_n \dots a_1 a_0 \tag{4.46}$$

Тогда справедлива формула [184] (вычисление проводится по модулю $2^n + 1$)

$$2 \cdot A = 2 \cdot a_n a_{n-1} \dots a_1 a_0 = a_{n-1} \dots a_1 a_0 (-a_n) \tag{4.47}$$

Эта формула выражает свойство, аналогичное свойству, присущему мерсенновским полям Галуа. А именно при вычислении по модулю $2^n - 1$ имеет место [115]

$$2 \cdot A = 2 \cdot a_n a_{n-1} \dots a_1 a_0 = a_{n-1} \dots a_1 a_0 a_n \tag{4.48}$$

Умножение числа, записанного в традиционной двоичной кодировке, на 2 в поле $GF(2^n - 1)$ приводит к циклической перестановке двоичных символов. Выражение (4.47) имеет аналогичный смысл, но только в этом случае символ a_n при перестановке меняет знак.

Справедливость формулы (4.44) вытекает из следующих соображений. Удаление старшего разряда отвечает операции вычитания числа 2^{n+1}. Для приведения результата умножения на 2 к результату по модулю $2^n + 1$ надо вычесть или прибавить еще единицу. В знакопеременной кодировке это отвечает использованию младшего разряда с противоположным знаком.

Покажем, что свойство (4.48) позволяет реализовать аппаратное вычисление дискретного логарифма достаточно простым способом. Для наглядности максимально подробно рассмотрим пример аппаратного вычисления дискретного логарифма в поле $GF(17)$.

Таблицы 4.3 и 4.4 показывают, что ненулевые элементы поля $GF(17)$ распадаются на два подмножества. В таблице 4.3 показаны восемь элементов, образованных преобразованием (4.47), применяемым к числу 2, записанному в знакопеременной кодировке. То же преобразование, применяемое к числу 6, записанному в той же кодировке, дает еще восемь элементов того же поля. Они перечислены в Таблице 4.4.

Таблица 4.3 – Элементы поля $GF(17)$, отвечающие степеням 2

a_3	a_2	a_1	a_0	$A(\pm)$	A
-1	-1	-1	-1	-15	2
-1	-1	-1	1	-13	4
-1	-1	1	1	-9	8
-1	1	1	1	-1	16

1	1	1	1	15	15
1	1	1	-1	13	13
1	1	-1	-1	9	9
1	-1	-1	-1	1	1

Таблица 4.4 – Элементы поля $GF(17)$, отвечающие степеням 2, умноженным на 6

a_3	a_2	a_1	a_0	$A(\pm)$	A
-1	1	-1	1	-5	12
1	-1	1	1	7	7
-1	1	1	-1	-3	14
1	1	-1	1	11	11
1	-1	1	-1	5	5
-1	1	-1	-1	-7	10
1	-1	-1	1	3	3
-1	-1	1	-1	-11	6

Как вытекает из представленных таблиц, произвольный ненулевой элемент поля $GF(17)$ может быть представлен в форме

$$A = 2^{n_1}6^{n_2} \tag{4.49}$$

где

$$n_1 = 1,2,\dots,8; n_2 = 0,1 \tag{4.50}$$

Примем также во внимание, что

$$2^4 = 16 \equiv -1(17) \tag{4.51}$$

Тогда формулу (4.49) можно записать так

$$A = (-1)^{n_0}2^{n_1}6^{n_2} \tag{4.52}$$

где

$$n_0 = 0,1;\ n_1 = 1,2,3,4; n_2 = 0,1 \tag{4.53}$$

Сравнивая формулу (4.52) с формулой (4.21), можно видеть, что представление (4.52) также позволяет определять значения парциальных дискретных логарифмов. Его преимущество состоит в том, что оно позволяет реализовать удобный аппаратный способ.

Следуя [184], будем использовать следующие величины

$$u_3 = a_3a_2; u_2 = a_2a_1; u_1 = a_1a_0; u_0 = -a_0a_3 \quad (4.54)$$

$$U_i = \begin{cases} 0, u_i = 1 \\ 1, u_i = -1 \end{cases} \quad (4.55)$$

Величины U_i показаны в Таблицах 4.5 и 4.6 для тех же элементов, что и в Таблицах 4.3 и 4.4 в том же порядке.

Таблица 4.5 – Идентификаторы, отвечающие вычислению дискретного логарифма для элементов Таблицы 4.3

A	U_3	U_2	U_1	U_0	ΣU_i	$-a_3$
2	0	0	0	1	1	1
4	0	0	1	0	1	1
8	0	1	0	0	1	1
16	1	0	0	0	1	1
15	0	0	0	1	1	-1
13	0	0	1	0	1	-1
9	0	1	0	0	1	-1
1	1	0	0	0	1	-1

Таблица 4.6 – Идентификаторы, отвечающие вычислению дискретного логарифма для элементов Таблицы 4.4

A	U_3	U_2	U_1	U_0	ΣU_i	$a_3(-1)^{U_1}$
6	0	1	1	1	3	1
12	1	1	1	0	3	1
7	1	1	0	1	3	1
14	1	0	1	1	3	1
11	0	1	1	1	3	-1
5	1	1	1	0	3	-1
10	1	1	0	1	3	-1
3	1	0	1	1	3	-1

Данные величины обеспечивают возможность вычисления дискретного логарифма при помощи электронной схемы, рассматриваемой ниже.

4.6. Электронный вычислитель дискретного логарифма в поле $GF(17)$

Принцип действия данного вычислителя основан на использовании идентификаторов, отраженных в Таблицах 4.5 и 4.6.

Схема (рисунок 4.3) вычисляет идентификатор ΣU_i, значение которого может быть равно либо 1, либо 3. Если данное значение есть 1, то тогда $n_2 = 0$ и $n_2 = 1$ в противоположном случае.

Если $\Sigma U_i = 1$, то:

- На выход схемы, отвечающему значению n_0, подается сигнал, отвечающий значению $-a_3$. Если $-a_3 = 1$, то $n_0 = 0$, если $-a_3 = -1$, то $n_0 = 1$.

- На выходы схемы, обеспечивающие идентификацию значения n_1, подаются сигналы, отвечающие значениям U_i в порядке U_0, U_1, U_2, U_3. Номер выхода, на котором формируется логическая единица, отвечает значению n_1, которое изменяется от 1 до 4.

Если $\Sigma U_i = 1$, то:

- На выход схемы, отвечающему значению n_0, подается сигнал, отвечающий значению $a_3(-1)^{U_1}$. Если $a_3(-1)^{U_1} = 1$, то $n_0 = 0$, если $a_3(-1)^{U_1} = -1$, то $n_0 = 1$.

- На выходы схемы, обеспечивающие идентификацию значения n_1, подаются инвертированные сигналы, отвечающие значениям U_i в порядке U_3, U_0, U_1, U_2. Номер выхода, на котором формируется логическая единица, отвечает значению n_1, которое изменяется от 1 до 4.

Принципиальная схема данного вычислителя показана на рисунке 4.3. На рисунке 4.4 продемонстрирован результат ее отработки в программе Proteus 8.17.

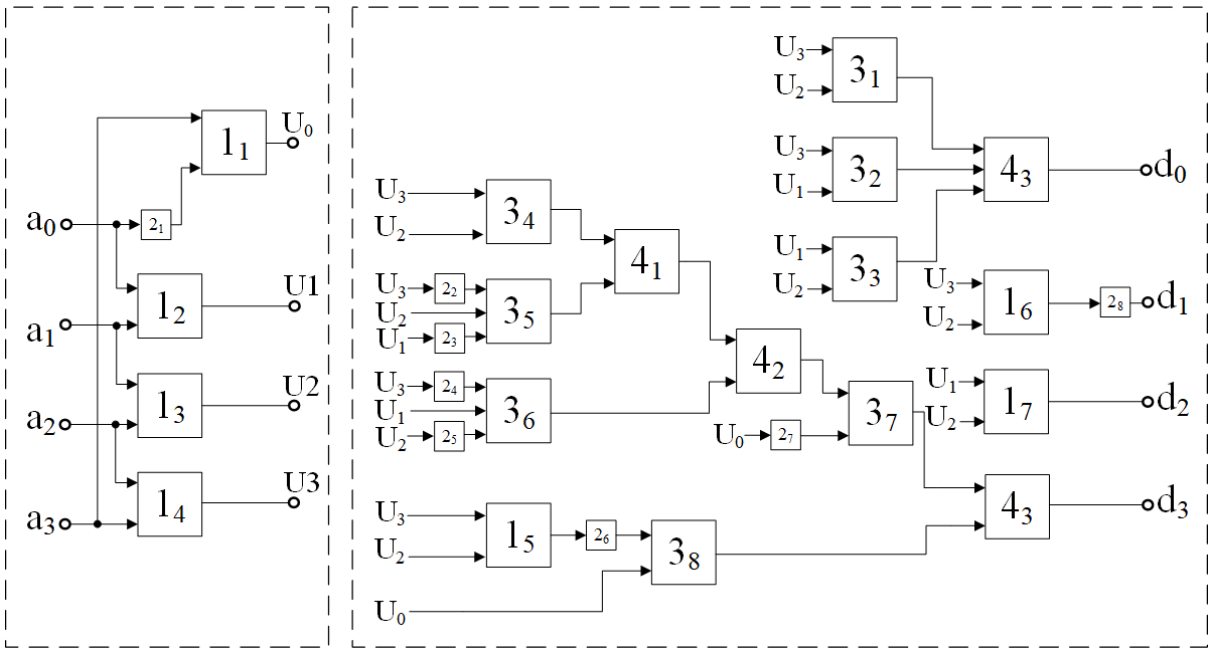


Рисунок 4.3 – Принципиальная схема: 1 – логические элементы XOR; 2 – логические элементы NOT; 3 – логические элементы AND; 4 – логические элементы OR

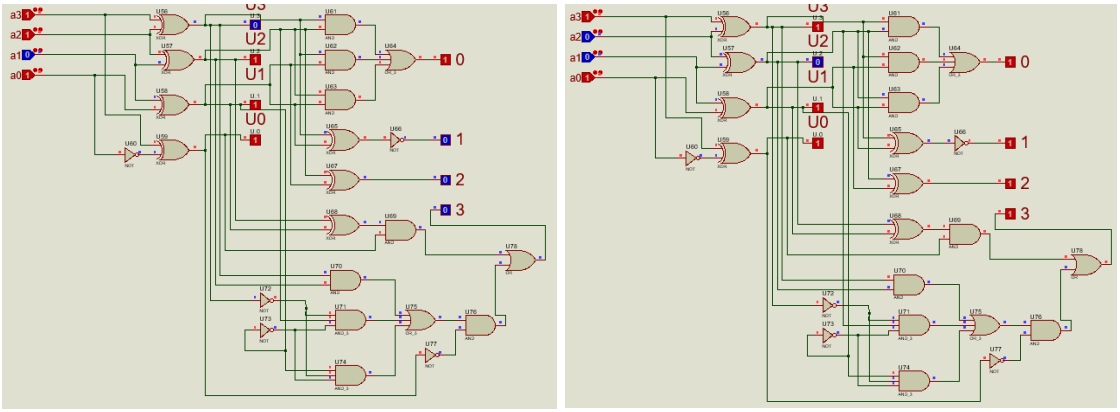


Рисунок 4.4 – Отработка алгоритма в программной среде Proteus 8.17

Представленная выше схема использует также следующий алгоритм перехода к знакопеременной кодировке (отметим, что высокий и низкий уровни сигнала, которые используют стандартные двоичные компоненты могут быть интерпретированы и как пара 0 и 1, и как пара -1 и 1).

Для наглядности рассмотрим случай поля $GF(17)$, а затем перейдем к обобщению. Как вытекает из сказанного выше, для всех нечетных чисел на первом месте будет находится символ 1, а для нечетных – -1. Следовательно, первый символ в знакопеременной кодировке однозначно определяется четностью исходного числа.

Оттолкнемся от записи числа 15 в традиционной кодировке, которое совпадает с представлением в знакопеременной кодировке.

$$15 \leftrightarrow 1111 \tag{4.56}$$

Для того, чтобы от записи (4.56) перейти к представлению другого нечетного числа b, $0 < b < 15$, надо из (4.56) вычесть четное число $c = 15 - b$. Такое вычитание можно осуществить следующим образом. Изменение знака символа 1, который стоит на третьей от конца позиции в записи (4.56) эквивалентно вычитанию числа 2^3, на второй - 2^2, на первой - 2^1. Любое четное число c из рассматриваемого интервала представимо в форме

$$c \leftrightarrow c_3 c_2 c_1 0 \tag{4.57}$$

Или

$$c = 2^3 c_3 + 2^2 c_2 + 2 c_1 \tag{4.58}$$

Где c_i – двоичные символы.

Следовательно, чтобы вычесть число c из 15 нужно поменять знак на противоположный в третьей от конца позиции, если $c_3 \neq 0$, а также во второй и/или первой, если $c_2 \neq 0$ и/или $c_1 \neq 0$. Это означает, что можно составить число

$$c_1 = \frac{c}{2} \leftrightarrow c_3 c_2 c_1 \quad (4.59)$$

Нужное число получится после того, как в записи (4.56) знак единиц будет изменен на противоположный в тех позициях, для которых c_i в записи (4.59) отличается от нуля. Этот алгоритм иллюстрирует Таблица 4.7.

Таблица 4.7 – Переход к знакопеременной кодировке для случая нечетных чисел, отвечающих элементам поля $GF(17)$

b	c	$\frac{c}{2}$	c_3	c_2	c_1	a_3	a_2	a_1	a_0
15	0	0	0	0	0	1	1	1	1
13	2	1	0	0	1	1	1	1	-1
11	4	2	0	1	0	1	1	-1	1
9	6	3	0	1	1	1	1	-1	-1
7	8	4	1	0	0	1	-1	1	1
5	10	5	1	0	1	1	-1	1	-1
3	12	6	1	1	0	1	-1	-1	1
1	14	7	1	1	1	1	-1	-1	-1

Таблица 4.8 – Переход к знакопеременной кодировке для случая четных чисел, отвечающих элементам поля $GF(17)$

b	c	$\frac{c}{2}$	c_3	c_2	c_1	a_3	a_2	a_1	a_0
-15	0	0	0	0	0	-1	-1	-1	-1
-13	2	1	0	0	1	-1	-1	-1	1
-11	4	2	0	1	0	-1	-1	1	-1
-9	6	3	0	1	1	-1	-1	1	1
-7	8	4	1	0	0	-1	1	-1	-1
-5	10	5	1	0	1	-1	1	-1	1
-3	12	6	1	1	0	-1	1	1	-1
-1	14	7	1	1	1	-1	1	1	1

Таким образом, те поля Галуа, которые представляют существенный интерес с точки зрения практических приложений ((в частности, отвечающие цифровым сигналам, представляемым через 256 уровней) действительно обладают выраженными особенностями, что отвечает точке зрения [184]. Эти особенности требуют, в том числе, модернизации метода вычисления дискретных логарифмов, предложенного ранее [183].

Предложенный в данной работе подход, тем не менее, сохраняет основное преимущество метода [183]. А именно, особенности квази-мерсенновских простых полей Галуа также позволяет развить аналог метода парциальных дискретных логарифмов. Отличие от метода [183] состоит в том, что в рассматриваемом случае парциальные дискретные логарифмы отвечают степеням числа 2. Это также позволяет привести вычисление дискретных

логарифмов к вычислению тех компонент спектра Фурье-Галуа, которые отвечают коротким периодам. Применительно к полю $GF(17)$, это – четырехчленные периоды, а применительно к полю $GF(257)$ – периоды, содержащие 16 тактов.

Этот факт существенно упрощает схемотехнику вычислителя дискретных логарифмов. Как показано в данной работе, такой вычислитель может быть построен на предельно простой комбинационной логике, что заведомо облегчает тайминг и снижает энергопотребление, что относится к любым практическим применениям предложенного метода вычисления дискретных логарифмов.

Предложенный метод, как показано в данной работе, применим, в частности, для разработки новых подходов к обфускации данных, передаваемых по по каналам связи, число уровней в которых комплементарно простому квази-мерсенновскому числу. Наиболее важным является частный случай, отвечающий 256 уровней, что отвечает полю $GF(257)$. Уместно подчеркнуть еще раз, что число 256 может быть поставлено в соответствии числу ненулевых уровней указанного поля, что позволяет проводить обработку любых сигналов, отвечающих такому числу уровней, в терминах дискретных логарифмов.

Предложенный метод обфускации данных основывается на вычислении дискретного логарифма с последующим использованием «смеси» преобразованного исходного сигнала с тем же сигналом (также в преобразованной форме), но только со сдвигом по времени. Такой подход позволяет перейти к использованию ключей, отвечающих существенно пониженному объему информации (по сравнению с исходным сигналом). Это позволяет утверждать, что предложенный подход потенциально применим, как минимум, в тех задачах, где «физическая» защита информации дополняется дополнительными средствами, ориентированными на использование максимально простых вычислительных процедур.

Данный вывод непосредственно подтверждается моделированием прототипа в Proteus для $GF(17)$, которое продемонстрировало корректность предлагаемых алгоритмов, а также их потенциальную пригодность для обфускации данных, ориентированных, в частности, на групповое применение БПЛА. Существующие тенденции, отвечающие использованию «роев» БПЛА [212-214], предусматривают не только обмен информацией между отдельными БПЛА и оператором, но и обмен информацией между физическими компонентами роя. Такой подход, отвечает, в том числе, возможности инсталляции «распределенного» AI на рой, рассматриваемый как целое [215,216], что соответствует одному из магистральных направлений развития AI [217].

За рамками данной работы остаются многочисленные вопросы, связанные с реальным использованием протоколов, основанных на использовании предлагаемой методики вычисления дискретных логарифмов (оценка уязвимостей по побочным каналам, отказоустойчивость,

энергопотребление и т.д.). Эти вопросы, однако, выходят за рамки настоящей работы, основной целью которой было доказательство возможности распространения метода вычисления парциальных цифровых логарифмов, ранее предложенного в [183], на особые случае (квази-мерсенновские поля Галуа).

Использование таких полей, разумеется, не исключает, что аналогичный подход к защите информации может быть реализован на методе вычисления дискретных логарифмов, изначально предложенном в [183], и ориентированном на использования полей Галуа других типов. Более того, троичная логика, которая обладает некоторыми преимуществами по сравнению с двоичной [218-220], вообще говоря, также позволяет перейти к использованию аналогов квази-мерсенновских чисел, построенных на основе степеней числа 3. Тем самым, есть основания полагать, что предложенный подход в перспективе может стать основой для создания целого семейства систем защиты информации, ориентированных на использование конечных алгебраических структур различного типа.

Выводы по Главе 4

В данной главе предложен и теоретически обоснован подход к вычислению дискретных логарифмов в квазимерсенновских полях Галуа ($p = 2^k + 1$), сохраняющий идею частичных логарифмов и основанный на представлении базиса Фурье–Галуа. Ключевым эффектом такой структуры являются короткие спектральные периоды и малое количество ненулевых коэффициентов, что упрощает алгоритмическую и аппаратную реализацию. Предложенное знакопеременное двоичное кодирование, в котором умножение на 2 сводится к циклическому сдвигу со сменой знака, дополнительно уменьшает логическую глубину и способствует достижению целевых частот без увеличения энергопотребления.

Продемонстрирована корректность полученных результатов для GF(17): разложение с периодом 4 по базису Фурье–Галуа приводит к компактным формулам и минимальному числу операций, а моделирование прототипа в Proteus подтвердило его корректность. Предложенный метод без существенных затруднений обобщается и на поле GF(257), операции в котором представляют выраженный практический интерес, в том числе, с точки зрения совершенствования методов обфускации данных, что также показано в данной работе.

ЗАКЛЮЧЕНИЕ

Отталкиваясь от существенных трансформаций в характере использования БПЛА вблизи линии боевого соприкосновения, где, в частности, используются дроны, управляемые по сверхтонкому оптоволокну, предложена модернизация метода защиты информации, предназначенного для передачи команд от оператора к рою дронов, основанная на определении местоположения источника радиосигнала. Метод основан на обмене данными между БПЛА, формирующими группу, по оптоволокну и предназначен для использования в зоне прямой радиовидимости. Показано, что в данном случае допустимо перейти к использованию каналов передачи данных от оператора к рою БПЛА, обладающему низкой пропускной способностью (менее десятков бит в секунду), так как допустимо отказаться от сложных методов шифрования. Это позволяет перейти к использованию длинноволнового радиодиапазона, что, в свою очередь, позволяет идентифицировать местоположение источника радиосигнала по разности фаз между сигналами, поступающими на приемники БПЛА, составляющими группу. Показано, что в рассматриваемом случае для определения фазовых сдвигов целесообразно использовать метод фазовых портретов, которые представляют собой зависимость производной исследуемой функции по времени от самой этой функции. Продемонстрированы преимущества предлагаемого подхода, в том числе, на примерах, связанных с разработкой конкретных электронных схем.

Метод фазовых портретов, используемый в данной работе, позволяет определить мгновенное значение частоты и фазы сигнала, детектируя при этом отклонения от гармонического. На его основе в работе предложена конкретная схема, обеспечивающая защиту информации при передаче команд группе БПЛА за счет идентификации местоположения источника радиосигнала и обмена данными между БПЛА по оптоволокну.

Таким образом, использование оптоволоконной связи между БПЛА, составляющими группу (рой), создает вполне определенные преимущества с точки зрения защиты информации, передаваемой от оператора к данной группе. С одной стороны, в данном случае сохраняются все те преимущества, которые обеспечиваются при прямой передаче команд от оператора к БПЛА по оптоволокну. С другой стороны, в данном случае возникает возможность существенно уменьшить протяженность оптоволоконных линий связи.

Такой метод защиты информации предназначен для использования в зоне прямой радиовидимости и основан на независимом определении координат источника сигнала бортовыми вычислительными системами группы БПЛА.

В диссертационной работе продемонстрирована корректность полученных результатов для GF(17): разложение с периодом 4 по базису Фурье–Галуа приводит к компактным формулам и минимальному числу операций, а моделирование прототипа в Proteus подтвердило его корректность. Предложенный метод без существенных затруднений обобщается и на поле GF(257), операции в котором представляют выраженный

практический интерес, в том числе, с точки зрения совершенствования методов обфускации данных, что также показано в данной работе.

ЛИТЕРАТУРА

[1] Мун Г.А., Витулёва Е.С., Байпакбаева С.Т., Кабдушев Ш.Б., Сулейменов И.Э. Проблематика постиндустриальной войны и деловые образовательные экосистемы // Вестник Национальной инженерной академии Республики Казахстан. 2020. No 4 (78), С. 88-93.

[2] Микитенко, В. М. Особенности применения средств воздушного нападения и сил противовоздушной обороны в локальных конфликтах / В. М. Микитенко, Д. В. Бухтиаров, В. Г. Бутенко // Динамика развития системы военного образования : Материалы V Международной научно-практической конференции, Омск, 17 марта 2023 года / Под общей редакцией К.В. Костина. – Омск: Омский государственный технический университет, 2023. – С. 440-447.

[3] Шудря, В. А., Сатин, Б. В., Прус, Ю. И., & Степанов, С. В. (2020). Особенности применения ультралегких беспилотных летательных аппаратов в вооруженном конфликте в Сирии. Научный резерв, (1), 8-17.

[4] Ананьев А. В., Филатов С. В. Обоснование нового способа совместного применения авиации и беспилотных летательных аппаратов малой дальности в операциях //Военная мысль. – 2018. – №. 6. – С. 5-13.

[5] Васильченко А. С., Иванов М. С., Колмыков Г. Н. Формирование маршрутов полета беспилотных летательных аппаратов с учетом местоположения средств противовоздушной обороны и радиоэлектронного подавления //Системы управления, связи и безопасности. – 2019. – №. 4. – С. 403-420.

[6] Гаджиева С. А., Курбанов С. К. Беспилотные летательные аппараты применение и перспективы их развития //Компьютерные технологии и моделирование в науке, технике, экономике, образовании и управлении: тенденции и развитие. – 2019. – С. 140-142.

[7] Скуднева О. В. Безальтернативность беспилотных летательных аппаратов в реалиях сегодняшней геополитики //Научные тенденции: вопросы точных и технических наук. – 2018. – С. 27-35.

[8] Сташкевич С. П., Кабанов В. А., Хуснутдинов Т. Д. Использование беспилотных летательных аппаратов в военных и гражданских целях //Актуальные проблемы авиации и космонавтики. – 2019. – Т. 1. – С. 171-173.

[9] Афонин, И. Е., Макаренко, С. И., Петров, С. В., & Привалов, А. А. (2020). Анализ опыта боевого применения групп беспилотных летательных аппаратов для поражения зенитно-ракетных комплексов системы противовоздушной обороны в военных конфликтах в Сирии, в Ливии и в Нагорном Карабахе. Системы управления, связи и безопасности, (4), 163-191.

[10] Когтин А. В., Шайдуров Г. Я. Перспективы развития малых беспилотных летательных аппаратов и проблема их обнаружения //Военная мысль. – 2023. – №. 1. – С. 61-65.

[11] Новик А. В., Кудряшов А. С. БЕСПИЛОТНЫЕ ЛЕТАТЕЛЬНЫЕ АППАРАТЫ, ПЕРСПЕКТИВЫ РАЗВИТИЯ, КЛАССИФИКАЦИЯ И СПОСОБЫ БОРЬБЫ С НИМИ //Научные чтения имени профессора Н.Е. Жуковского. – 2023. – С. 420-425.

[12] Лось А. П., Ткачёв В. Р. Особенности применения беспилотных летательных аппаратов в Военно-Морском Флоте //Военная мысль. – 2023. – №. 12. – С. 29-34.

[13] Залужный В.Ф. КОНЦЕПЦИЯ ВОЙНЫ ИЗМЕНИЛАСЬ «ЗЕРКАЛО НЕДЕЛИ. УКРАИНА»: интернет-портал. – URL: https://zn.ua/war/kontseptsija-vojny-izmenilas-zaluzhnyj-nazval-novye-prioritety-v-state-dlja-cnn.html. (дата обращения: 17.03.24).

[14] Гвоздев М. Г. К вопросу о появлении основных концепций применения ВВС в межвоенный период //Актуальные проблемы гуманитарных и естественных наук. – 2013. – №. 4. – С. 71-74.

[15] Формирование исследовательских программ как задача прикладной философии / Е. С. Витулева, О. А. Габриелян, П. Е. Григорьев [и др.] // Практическая философия: состояние и перспективы: сборник материалов научной конференции, Симферополь, 27–28 мая 2021 года. – Симферополь: Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2021. – С. 140-156.

[16] Иванов Б. Современная философия техники: проблемы и перспективы //Мысль: Журнал Петербургского философского общества. – 2009. – Т. 8. – №. 1. – С. 194-202.

[17] Сулейменов, И. Э., Габриелян, О. А., Пак, И. Т., Панченко, С. В., & Мун, Г. А. (2016). Инновационные сценарии в постиндустриальном обществе. Print Express.

[18] Мун Г. А., Витулёва Е. С., Сулейменов И. Э. К теории решения инновационных задач //Вестник Алматинского университета энергетики и связи. – 2019. – №. 1. – С. 72-78.

[19] SULEIMENOV, I., GABRIELYAN, O. and VITULYOVA, Y. 2022. Dialectics of Scientific Revolutions from the Point of View of Innovations Theory. WISDOM. 24, 4 (Dec. 2022), 25–35.

[20] Платонова С. И. Логика научного развития: парадигма Т. Куна и четвертая парадигма Дж. Грея //Контекст и рефлексия: философия о мире и человеке. – 2020. – Т. 9. – №. 1А. – С. 144-151.

[21] Буренок В. М., Дурнев Р. А., Крюков К. Ю. Разумное вооружение: будущее искусственного интеллекта в военном деле //Вооружение и экономика. – 2018. – №. 1. – С. 4-13.

[22] Галкин Д. В., Коляндра П. А., Степанов А. В. Состояние и перспективы использования искусственного интеллекта в военном деле //Военная мысль. – 2021. – №. 1. – С. 113-124.

[23] Абросимов В. К. Искусственный интеллект и проблемы развития вооружения и военной техники //Вооружение и экономика. – 2021. – №. 2. – С. 5-21.

[24] Беликова К. М. «Война брендов» производителей роботизированных автономных (беспилотных), оснащенных и неоснащенных искусственным интеллектом, систем вооружений (дронов) и границы применения патентов и ноу-хау //Социально-политические науки. – 2021. – Т. 11. – №. 4. – С. 92-106.

[25] Чернявский А. Г., Сибилева О. П. Автономное высокоточное оружие как вызов международному гуманитарному праву //Военное право. – 2020. – №. 4 (62). – С. 229.

[26] Корсунский В. А., Наумов В. Н. Перспективы развития военных мобильных робототехнических комплексов наземного базирования в России //Инженерный журнал: наука и инновации. – 2012. – №. 10 (10). – С. 29.

[27] Рубцов И. В. Вопросы состояния и перспективы развития отечественной наземной робототехники военного и специального назначения //Известия Южного федерального университета. Технические науки. – 2013. – №. 3 (140). – С. 14-21.

[28] Кун Т. Структура научных революций. Пер. с англ. И. Налетова. М.: Прогресс, 1977. 300 с.

[29] Hey T., Tansley S., Tolle K. Jim Grey on eScience: A transformed scientific method // The Fourth Paradigm: Data-Intensive Scientific Discovery / Eds: Hey T., Tansley S., Tolle K. Redmond: Microsoft Research, 2009. Pp. XVII-XXXI.

[30] Бондарев А. Н., Киричек Р. В. Обзор беспилотных летательных аппаратов общего пользования и регулирования воздушного движения БПЛА в разных странах //Информационные технологии и телекоммуникации. – 2016. – Т. 4. – №. 4. – С. 13.

[31] Коротаев А. А., Новопашин Л. А. Применение беспилотных летательных аппаратов для мониторирования сельскохозяйственных угодий и посевных площадей в аграрном секторе //Аграрный вестник Урала. – 2015. – №. 12 (142). – С. 38-42.

[32] Шевченко А. В., Мигачев А. Н. Обзор состояния мирового рынка беспилотных летательных аппаратов и их применения в сельском хозяйстве //Робототехника и техническая кибернетика. – 2019. – Т. 7. – №. 3. – С. 183-195.

[33] Джанибеков Р. Ю., Аббасов И. Б. Особенности применения морских дронов в специальной военной операции на Украине, перспективы развития военно-морских робототехнических комплексов //Мат. Конф. «Памятные даты-дни воинской славы России. Посвящается 80-летию Курской битвы и 210-летию Битвы народов», Омск, 13 октября 2023. – С. 267-274.

[34] Старая авиабомба с мотором от канадского гидроцикла: как устроены морские дроны ВСУ/ Новые известия: [сайт]. 2023.

[35] Тулешов, А., Сейдахмет, А., Бисембаев, К., Джамалов, Н., & Удербаева, А. (2024). ДИНАМИКА ТРАНСПОРТНОГО МОБИЛЬНОГО РОБОТА С МОДИФИЦИРОВАННЫМ МЕХАНИЗМОМ АККЕРМАНА В КВАЗИКООРДИНАТАХ. Вестник КазАТК, 130(1), 70-78.

[36] Яцун, С. Ф., Чжо, П. В., Мальчиков, А. В., & Савин, С. И. (2013). Экспериментальные исследования мобильного гусеничного робота при прямолинейном движении. Известия Юго-Западного государственного университета. Серия: Техника и технологии, (1), 85-90.

[37] Павлюковец С. А., Вельченко А. А., Радкевич А. А. Математическая модель системы управления мобильным гусеничным роботом с учетом кинематических и динамических параметров //Системный анализ и прикладная информатика. – 2023. – №. 3. – С. 33-38.

[38] Павловский В. Е. О разработках шагающих машин //Препринты Института прикладной математики им. МВ Келдыша РАН. – 2013. – №. 0. – С. 101-32.

[39] Дмитрий Невзоров / Гигантский робот ВСУ не смог уползти от FPV-дрона / Д. Невзоров. – Текст: электронный // Сводка СВО за 20 марта. «Аргументы и Факты»: интернет-портал. – URL: https://aif.ru/politics/world/gigantskiy-robot-vsu-ne-smog-upolzti-ot-fpv-drona-svodka-svo-za-20-marta- (дата обращения: 25.03.2024).

[40] Патент RU 2 364 500 C2, МПК B25J 5/00, Лебедев Владимир Вячеславович Эльстин Виталий Иванович (Яковлев Сергей Федорович Медвецкий Сергей Владимирович (Космачев Павел Владимирович Кудряшов Владимир Борисович Дементей Виктор Петрович Галин Валерий Семенович

[41] Патент RU №2595097C1, МПК F41H 11/02. Многофункциональная наземная гиростабилизирующая платформа обнаружения воздушных целей и борьбы с ними. № 201813763: заявл. 11.03.2029: опубл. 18.10.2019 / Шишков С.В., Устинов Е.М., Барсуков В.А., Лысенко Е.Н., Синяев Е.Г., Петренко В.И., Борщин Ю.Н., Колесников И.Б., Пашинян Д.Б., Немов О.Н., Дюндяев А.В., Дорошев А.А., Кутьменев А.В., Кудрявцев П.Ю.

[42] Patent CZ307386B6, 18.07.2018. An actuation and steering module of robotic wheeled vehicles / Pavel Mikunda, Ladislav Kuběna, Jan Dvořák, František Omaník, Martin Prokeš, Marek Dobrovský, Jaroslav Kočnar, Michal Barnáš, Zbyněk Fusek, Dušan Kahánek.

[43] Patent US20100155156A1, 24.06.2010. Energetically autonomous tactical robot and associated methodology of operation / Robert Finkelstein.

[44] Патент RU 2 743 130 C1, МПК B25J 5/00, F41H 7/02 Гречушкин Игорь Васильевич Прутчиков Игорь Олегович Сергеев Владислав Владимирович Фадеев Дмитрий Юрьевич Федосеев Алексей Викторович (Каширин Павел Евгеньевич Зорин Сергей Дмитриевич Есичко Сергей Валерьевич

[45] Патент РК № 2022/0525.1, 27.08.2022. Робот для разминирования // Мун Григорий Алексеевич; Байпакбаева Салтанат Туркестанкызы; Кабдушев Шернияз Булатулы; Қадыржан Қайсарәлі Нұрланұлы; Витулёва Елизавета Сергеевна; Сулейменов Ибрагим Эсенович.

[46] Woonghee Lee, "Federated Reinforcement Learning-Based UAV Swarm System for Aerial Remote Sensing", Wireless Communications and Mobile Computing, vol. 2022, Article ID 4327380, 15 pages, 2022. https://doi.org/10.1155/2022/4327380

[47] Wang, C.; Su, Y.; Wang, J.; Wang, T.; Gao, Q. UAV Swarm Dataset: An Unmanned Aerial Vehicle Swarm Dataset for Multiple Object Tracking. Remote Sens. 2022, 14, 2601. https://doi.org/10.3390/rs14112601

[48] Liu, J.; Liao, X.; Ye, H.; Yue, H.; Wang, Y.; Tan, X.; Wang, D. UAV Swarm Scheduling Method for Remote Sensing Observations during Emergency Scenarios. Remote Sens. 2022, 14, 1406. https://doi.org/10.3390/rs14061406

[49] Mitch Campion, Prakash Ranganathan, and Saleh Faruque. 2019. UAV swarm communication and control architectures: a review. Journal of Unmanned Vehicle Systems. 7(2): 93-106. https://doi.org/10.1139/juvs-2018-0009

[50] Saffre, F., Karvonen, H., Hildmann, H. (2024). Wild Swarms: Autonomous Drones for Environmental Monitoring and Protection. In: Westerlund, T., Peña Queralta, J. (eds) New Developments and Environmental Applications of Drones. FinDrones 2023. Springer, Cham. https://doi.org/10.1007/978-3-031-44607-8_1

[51] Y. Liu, J. Nie, X. Li, S. H. Ahmed, W. Y. B. Lim and C. Miao, "Federated Learning in the Sky: Aerial-Ground Air Quality Sensing Framework With UAV Swarms," in IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9827-9837, 15 June15, 2021, doi: 10.1109/JIOT.2020.3021006.

[52] N. Hossein Motlagh et al., "Unmanned Aerial Vehicles for Air Pollution Monitoring: A Survey," in IEEE Internet of Things Journal, vol. 10, no. 24, pp. 21687-21704, 15 Dec.15, 2023, doi: 10.1109/JIOT.2023.3290508.

[53] Y. Zhou, B. Rao and W. Wang, "UAV Swarm Intelligence: Recent Advances and Future Trends," in IEEE Access, vol. 8, pp. 183856-183878, 2020, doi: 10.1109/ACCESS.2020.3028865.

[54] P. Tosato, D. Facinelli, M. Prada, L. Gemma, M. Rossi and D. Brunelli, "An Autonomous Swarm of Drones for Industrial Gas Sensing Applications," 2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Washington, DC, USA, 2019, pp. 1-6, doi: 10.1109/WoWMoM.2019.8793043.

[55] Ju C, Son HI. A distributed swarm control for an agricultural multiple unmanned aerial vehicle system. Proceedings of the Institution of Mechanical Engineers, Part I: Journal of Systems and Control Engineering. 2019;233(10):1298-1308. doi:10.1177/0959651819828460

[56] R. McCune et al., "Investigations of DDDAS for command and control of UAV swarms with agent-based modeling," 2013 Winter Simulations Conference (WSC), Washington, DC, USA, 2013, pp. 1467-1478, doi: 10.1109/WSC.2013.6721531.

[57] J. S. Lee, Y. -S. Yoo, H. Choi, T. Kim and J. K. Choi, "Group Connectivity-Based UAV Positioning and Data Slot Allocation for Tactical MANET," in IEEE Access, vol. 8, pp. 220570-220584, 2020, doi: 10.1109/ACCESS.2020.3042795.

[58] https://www.newscientist.com/article/2282656-israel-used-worlds-first-ai-guided-combat-drone-swarm-in-gaza-attacks/

[59] Cheah, C. C., Hou, S. P., & Slotine, J. J. E. (2009). Region-based shape control for a swarm of robots. Automatica, 45(10), 2406-2411.

[60] Bayındır, L. (2016). A review of swarm robotics tasks. Neurocomputing, 172, 292-321.

[61] Dorigo, M., Theraulaz, G., & Trianni, V. (2021). Swarm robotics: Past, present, and future [point of view]. Proceedings of the IEEE, 109(7), 1152-1165.

[62] Chung, S. J., Paranjape, A. A., Dames, P., Shen, S., & Kumar, V. (2018). A survey on aerial swarm robotics. IEEE Transactions on Robotics, 34(4), 837-855.

[63] Chunyu Li, Jianan Wang, Junhui Liu, Jiayuan Shan, "Cooperative Visual–Range–Inertial Navigation for Multiple Unmanned Aerial Vehicles", IEEE Transactions on Aerospace and Electronic Systems, vol.59, no.6, pp.7851-7865, 2023.

[64] Zhao, H., Liu, H., Leung, Y. W., & Chu, X. (2018). Self-adaptive collective motion of swarm robots. IEEE Transactions on Automation Science and Engineering, 15(4), 1533-1545.

[65] Yahao Ding, Zhaohui Yang, Quoc-Viet Pham, Ye Hu, Zhaoyang Zhang, Mohammad Shikh-Bahaei, "Distributed Machine Learning for UAV Swarms: Computing, Sensing, and Semantics", IEEE Internet of Things Journal, vol.11, no.5, pp.7447-7473, 2024.

[66] Cunhao Li, Guanghui Guo, Peng Yi, Yiguang Hong, "Distributed Pose-Graph Optimization With Multi-Level Partitioning for Multi-Robot SLAM", IEEE Robotics and Automation Letters, vol.9, no.6, pp.4926-4933, 2024.

[67] Wei Liu, Zhijun Gao. A distributed flocking control strategy for UAV groups. Computer Communications, Volume 153, 2020. P. 95-101, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2020.01.076.

[68] Wang Xinhua, Chen Guanyu, Gong Huajun, Jiang Ju. UAV swarm autonomous control based on Internet of Things and artificial intelligence algorithms. Journal of Intelligent & Fuzzy Systems, vol. 40, no. 4, pp. 7121-7133, 2021. DOI: 10.3233/JIFS-189541.

[69] Zheng Y, Huepe C, Han Z. Experimental capabilities and limitations of a position-based control algorithm for swarm robotics. Adaptive Behavior. 2022;30(1):19-35. doi:10.1177/1059712320930418

[70] Raffaele Carli, Graziana Cavone, Nicola Epicoco, Mario Ferdinando, Paolo Scarabaggio, Mariagrazia Dotoli. Consensus-Based Algorithms for Controlling Swarms of Unmanned Aerial Vehicles. Ad-Hoc, Mobile, and Wireless Networks, 2020, Volume 12338. ISBN : 978-3-030-61745-5

[71] Asaamoning, G.; Mendes, P.; Rosário, D.; Cerqueira, E. Drone Swarms as Networked Control Systems by Integration of Networking and Computing. Sensors 2021, 21, 2642. https://doi.org/10.3390/s21082642

[72] Elkilany, B.G., Abouelsoud, A.A., Fathelbab, A.M.R. et al. A proposed decentralized formation control algorithm for robot swarm based on an optimized potential field method. Neural Comput & Applic 33, 487–499 (2021). https://doi.org/10.1007/s00521-020-05032-0

[73] Quesada, W.O. et al. (2018). Leader-Follower Formation for UAV Robot Swarm Based on Fuzzy Logic Theory. In: Rutkowski, L., Scherer, R., Korytkowski, M., Pedrycz, W., Tadeusiewicz, R., Zurada, J. (eds) Artificial Intelligence and Soft Computing. ICAISC 2018. Lecture Notes in Computer Science(), vol 10842. Springer, Cham. https://doi.org/10.1007/978-3-319-91262-2_65

[74] A. T. Hafez and M. A. Kamel, "Fault-tolerant control for cooperative unmanned aerial vehicles formation via fuzzy logic," 2016 International Conference on Unmanned Aircraft Systems (ICUAS), Arlington, VA, USA, 2016, pp. 1261-1266, doi: 10.1109/ICUAS.2016.7502660.

[75] Селин А. И., Туркин И. К. Обзор целевых объектов применения беспилотных летательных аппаратов, работающих в составе группы //Научный вестник Московского государственного технического университета гражданской авиации. – 2023. – Т. 26. – №. 2. – С. 91-105.

[76] Юйцин Ч. Формирование управления полетом группы беспилотных летательных аппаратов на основе алгоритма многоагентной модели роения //Информатика, телекоммуникации и управление. – 2022. – Т. 15. – №. 4. – С. 22-36.

[77] Егорова К. В. Имитационная модель управления полетом группы беспилотных летательных аппаратов на основе алгоритма пчелиной колонии //Вестник Воронежского государственного технического университета. – 2023. – Т. 19. – №. 2. – С. 68-71.

[78] Иванов С. В. Методика построения субоптимальных маршрутов для группы беспилотных летательных аппаратов на основе биоинспирированных алгоритмов при наличии препятствий //Системы управления, связи и безопасности. – 2022. – №. 2. – С. 1-23.

[79] Пантелеймонов, И. Н., Белозерцев, А. В., Монастыренко, А. А., Боцва, В. В., & Наумкин, А. В. (2020). Основные направления создания высоконадежной системы связи и управления БПЛА. Известия высших учебных заведений. Машиностроение, (6 (723)), 78-88.

[80] Васильев В. П., Родионов Д. В. Использование малогабаритных беспилотных летательных аппаратов в качестве ретранслятора связи //Вестник Воронежского института ФСИН России. – 2015. – №. 2. – С. 11-14.

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

[82] Wang, D.; Bai, B.; Zhao, W.; Han, Z. A Survey of Optimization Approaches for Wireless Physical Layer Security. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 1878–1911.

[83] Zoli, M.; Mitev, M.; Barreto, A.N.; Fettweis, G. Estimation of the secret key rate in wideband wireless physical-layer-security. In Proceedings of the 2021 International Symposium on Wireless Communication Systems (ISWCS), Berlin, Germany, 2021. https://doi.org/10.1109/ISWCS49558.2021.9562135.

[84] Hamamreh, J.M.; Furqan, H.M.; Arslan, H. Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2019**. https://doi.org/10.1109/COMST.2018.2878035.

[85] Abu-Faraj, M. A., Al-Hyari, A., Altaharwa, I., Alqadi, Z., & Ali, B. (2023). Increasing the security of transmitted text messages using chaotic key and image key cryptography. International Journal of Data and Network Science, 7(2), 809-820.

[86] Khan, H. N., Chaudhuri, A., Das, A., & Chaudhuri, A. (2020). An ultra robust session key based image cryptography. Microsystem Technologies, 26(7), 2193-2201.

[87] Subramani, S., & Svn, S. K. (2023). Review of security methods based on classical cryptography and quantum cryptography. Cybernetics and Systems, 1-19.

[88] Sixto, X., Currás-Lorenzo, G., Tamaki, K., & Curty, M. (2023). Secret key rate bounds for quantum key distribution with faulty active phase randomization. EPJ Quantum Technology, 10(1), 1-26.

[89] Gupta, M., Gupta, M., & Deshmukh, M. (2020). Single secret image sharing scheme using neural cryptography. Multimedia tools and applications, 79, 12183-12204.

[90] Meraouche, I., Dutta, S., Tan, H., & Sakurai, K. (2021). Neural networks-based cryptography: A survey. IEEE Access, 9, 124727-124740.

[91] D. Becker and L. Schalk, "Enabling Air-to-Air Wideband Channel Measurements between Small Unmanned Aerial Vehicles with Optical Fibers," 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC), San Diego, CA, USA, 2019, pp. 1-7, doi: 10.1109/DASC43569.2019.9081691.

[92] Shindo, N., Kobatake, T., Masson, D., Fafard, S., & Matsuura, M. (2022). Optically Powered and Controlled Drones Using Optical Fibers for Airborne Base Stations. Photonics, 9(11), 882. https://doi.org/10.3390/photonics9110882

[93] Ermukhambetova, B.; Mun, G.; Kabdushev, S.; Kadyrzhan, A.; Kadyrzhan, K.; Vitulyova, Y.; Suleimenov, I.E. New approaches to the development of information security systems for unmanned vehicles. *Indones J Electr Eng Comput Sci* **2023**, *31*, 810. http://doi.org/10.11591/ijeecs.v31.i2.pp810-819.

[94] Vitulyova, Y., Kadyrzhan, K., Kadyrzhan, A., & Suleimenov, I. (2024). Application of focusing systems to the protection of information during data transmission in the zone of direct radio visibility. International Journal of Electronics and Telecommunications, 699-705.

[95] Kadyrzhan, A.; Matrassulova, D.; Vitulyova, Y.; Suleimenov, I. Discrete Cartesian Coordinate Transformations: Using Algebraic Extension Methods. *Appl. Sci.* 2025, *15*, 1464. https://doi.org/10.3390/app15031464

[96] Kuptsov, V.; Badenko, V.; Ivanov, S.; Fedotov, A. Method for Remote Determination of Object Coordinates in Space Based on Exact Analytical Solution of Hyperbolic Equations. *Sensors* **2020**, *20*, 5472. https://doi.org/10.3390/s20195472.

[97] Legros, Q., Fourer, D., Meignen, S., & Colominas, M. A. (2024). Instantaneous frequency and amplitude estimation in multicomponent signals using an em-based algorithm. IEEE Transactions on Signal Processing, 72, 1130-1140.

[98] Li, M., Wang, T., Kong, Y., & Chu, F. (2021). Synchro-reassigning transform for instantaneous frequency estimation and signal reconstruction. IEEE transactions on industrial electronics, 69(7), 7263-7274.

[99] Seddighi, Z., Taban, M. R., & Gazor, S. (2024). Optimal time-frequency distribution for instantaneous frequency estimation of signals with known IF patterns. IEEE Transactions on Aerospace and Electronic Systems.

[100] Goodman, J. W., & Sutton, P. (1996). Introduction to Fourier optics. Quantum and Semiclassical Optics-Journal of the European Optical Society Part B, 8(5), 1095.

[101] Vitulyova, Y. S., Suleimenov, I. E., Matrassulova, D. K., & Bakirov, A. S. (2023). Discrete form of the Huygens-Fresnel principle: to the multi-dimensional analog of the Nyquist–Shannon sampling theorem. International Journal of Information Technology, 15(7), 3751-3759.

[102] Vitulyova, Y., Kadyrzhan, K., Kadyrzhan, A., Shaltykova, D., & Suleimenov, I. (2024). Reducing the description of arbitrary wave field converters to tensor form. International Journal of Information Technology, 1-10.

[103] Ivashov, S. I., Capineri, L., Bechtel, T. D., Razevig, V. V., Inagaki, M., Gueorguiev, N. L., & Kizilay, A. (2021). Design and Applications of Multi-Frequency Holographic Subsurface Radar: Review and Case Histories. Remote Sensing, 13(17), 3487. https://doi.org/10.3390/rs13173487

[104] Popov, A. V., Reznikov, A. E., Berkut, A. I., Edemsky, D. E., Morozov, P. A., & Prokopovich, I. V. (2022). Methods and Algorithms of Subsurface Holographic Sounding. Remote Sensing, 14(20), 5274. https://doi.org/10.3390/rs14205274

[105] Vijayakumar, S. D. ., Vijayakumari, G. ., Praveenkumar, R. ., Kumar, V. ., & Velmurugan, T. . (2024). Effective RF Transmitter and Receiver System Using 2.4 GHz for Unmanned Aerial Vehicles. Current Approaches in Engineering Research and Technology Vol. 7, 103–114. https://doi.org/10.9734/bpi/caert/v7/1590

[106] F. A. Warsi et al., "Yaw, Pitch and Roll controller design for fixed-wing UAV under uncertainty and perturbed condition," 2014 IEEE 10th International Colloquium on Signal Processing and its Applications, Kuala Lumpur, Malaysia, 2014, pp. 151-156, doi: 10.1109/CSPA.2014.6805738.

[107] Seonhyeok Kang, H. Jin Kim, Jin-Ik Lee, Byung-Eul Jun, and Min-Jea Tahk (2009). Roll-Pitch-Yaw Integrated Robust Autopilot Design for a High Angle-of-Attack Missile. Journal of Guidance, Control, and Dynamics. 32:5, 1622-1628. https://doi.org/10.2514/1.39812

[108] Barvinok, A.; Rudelson, M. When a system of real quadratic equations has a solution. Adv. Math. 2022, 403, 108391.

[109] Chi, Y.; Lu, Y.M. Kaczmarz method for solving quadratic equations. IEEE Signal Process. Lett. 2016, 23, 1183-1187.

[110] Huang, M.; Xu, Z. Solving systems of quadratic equations via exponential-type gradient descent algorithm. arXiv 2018, 1806.00904.

[111] Moldakhan I., Matrassulova D. K., Shaltykova D.B., Suleimenov I.E. Some advantages of non-binary Galois fields for digital signal processing // Indonesian Journal of Electrical Engineering and Computer Science, Vol. 23, No. 2, August 2021, pp. 871~877, ISSN: 2502-4752, DOI: 10.11591/ijeecs.v23.i2.pp871-877 http://ijeecs.iaescore.com/index.php/IJEECS/article/view/24911

[112] Elizaveta S. Vitulyova, Dinara K. Matrassulova, Ibragim E. Suleimenov. Application of Non-binary Galois Fields Fourier Transform for Digital Signal Processing: to the

Digital Convolution Theorem // Indonesian Journal of Electrical Engineering and Computer Science Vol. 23, No. 3, September 2021, pp. 1718~1726

[113] Dinara Matrassulova, Yelizaveta Vitulyova, Sergey Konshin1, Ibragim Suleimenov Algebraic fields and rings as a digital signal processing tool Indonesian Journal of Electrical Engineering and Computer Science Vol. 29, No. 1, January 2023, pp. 206~216 ISSN: 2502-4752, DOI: 10.11591/ijeecs.v29.i1.pp206-216

[114] Suleimenov, I.E., Vitulyova, Y.S., Kabdushev, S.B. et al. Improving the efficiency of using multivalued logic tools: application of algebraic rings. Sci Rep 13, 22021 (2023). https://doi.org/10.1038/s41598-023-49593-1

[115] Suleimenov, I. E., Vitulyova, Y. S., & Matrassulova, D. K. (2023). Features of digital signal processing algorithms using Galois fields GF (2n+ 1). Plos one, 18(10), e0293294.

[116] Suleimenov, I.; Kadyrzhan, A.; Vitulyova, Y.; et al. The use of fiber optics for securing information during command transmission to UAV groups. Int. J. Inf. Technol. 2025. https://doi.org/10.1007/s41870-025-02719-2

[117] Shaltykova, D., Kadyrzhan, A., Vitulyova, Y., & Suleimenov, I. (2026). The Provision of Physical Protection of Information During the Transmission of Commands to a Group of UAVs Using Fiber Optic Communication Within the Group. *Drones*, *10*(1), 24. https://doi.org/10.3390/drones10010024

[118] Goldstein, H., Poole, C., Safko, J., & Addison, S. R. (2002). Classical mechanics.

[119] Arnol'd, V. I. (2013). Mathematical methods of classical mechanics (Vol. 60). Springer Science & Business Media.

[120] van Rossum, H. H. (2019). Moving average quality control: principles, practical application and future perspectives. Clinical Chemistry and Laboratory Medicine (CCLM), 57(6), 773-782.

[121] Hansun, S. (2013, November). A new approach of moving average method in time series analysis. In 2013 conference on new media studies (CoNMedia) (pp. 1-4). IEEE.

[122] Патент № 2693616 Российская Федерация, B64D 35/04. Многовинтовой летательный аппарат: 2017118430: заявл. 03.07.2019: опубл. 03.07.2019 Бюл. № 19 / ЮНГ Андерс; заявитель АКК ИННОВЕЙШН АБ. - 27 с.

[123] Патент № 2704771 Российская Федерация, B64C27/24. Летательный аппарат, выполненный с возможностью вертикального взлета: 2016102944: заявл. 30.10.2019: опубл. 30.10.2019 / Ханс Нидцбалла; заявитель Эйрбас Дефенс энд Спэйс ГмбХ. - 21 с.

[124] Патент № 2769822 Российская Федерация, B64C 27/08. Летательные аппараты с несвязанными степенями свободы: 2021115298: заявл. 06.04.2022: опубл. 06.04.2022 Бюл. № 10 / Инаки, И. А., Хосеба, Л. А. - 32 с.

[125] Патент № 222488 Российская Федерация, F41H 11/02. Устройство для борьбы с миниатюрными беспилотными аппаратами: 2023115097: заявл. 28.12.2023: опубл. 28.12.2023 Бюл. № 1 / Трофимов В.И., Трофимов О. В; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования "Тверской государственный технический университет". - 12 с.

[126] Патент № 2791754 Российская Федерация, B64C 39/02. МНОГОЦЕЛЕВАЯ БЕСПИЛОТНАЯ АВИАЦИОННАЯ РАКЕТНАЯ СИСТЕМА: 2022112336: заявл. 13.03.2023: опубл. 13.03.2023 Бюл. № 8 / Дуров Д.С. - 16 с.

[127] Патент № 2021 United States, B64C 39/02, B64C 27/52, B64C 37/00. ROCKET PROPELLED DRONE: 16: заявл. 26.05.2020: опубл. 04.02.2021 / Randy MARTEL. - 54 с.

[128] Патент № 37453 РК, B64C 39/00. Способ реализации беспилотного летательного аппарата-носителя боеприпаса воздушного базирования. 2024/0382.1: заявл. 14.05.2024: опубл. 01.08.2025 Бюл. № 31. / Сулейменов И.Э., Мун Г.А., Байпакбаева С.Т., Кадыржан А.Б.

[129] Thakor, V.A.; Razzaque, M.A.; Khandaker, M.R.A. Lightweight Cryptography for IoT: A State-of-the-Art. arXiv 2020, arXiv:2006.13813 [cs.CR]. Available online: https://arxiv.org/abs/2006.13813 (accessed on 9 August 2025).

[130] El Gaabouri, I.; Senhadji, M.; Belkasmi, M. A Survey on Lightweight Cryptography Approach for IoT Devices Security. In Proceedings of the 2022 5th International Conference on Networking, Information Systems and Security: Envisage Intelligent Systems in 5G/6G-Based Interconnected Digital Worlds (NISS), Bandung, Indonesia, 30–31 March 2022; pp. 1–8. https://doi.org/10.1109/NISS55057.2022.10085144.

[131] Mouha, Nicky & Mennink, Bart & Herrewege, Anthony & Watanabe, Dai & Preneel, Bart & Verbauwhede, Ingrid. (2014). Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers. 306-323. 10.1007/978-3-319-13051-4_19.

[132] Enireddy, V.; Somasundaram, K.; Prabhu, M.R.; Babu, D.V. Data obfuscation technique in cloud security. In Proceedings of the 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), October 2021; pp. 358–362. IEEE.

[133] Gao, Z.; Huang, Y.; Zheng, L.; Lu, H.; Wu, B.; Zhang, J. Protecting location privacy of users based on trajectory obfuscation in mobile crowdsensing. IEEE Trans. Ind. Inform. 2022, 18, 6290–6299.

[134] Al-Balasmeh, H.; Singh, M.; Singh, R. Framework of data privacy preservation and location obfuscation in vehicular cloud networks. Concurr. Comput. Pract. Exp. 2022, 34, e6682.

[135] Fiedler, R., Hetzler, H., & Bäuerle, S. (2024). Efficient numerical calculation of Lyapunov-exponents and stability assessment for quasi-periodic motions in nonlinear systems. Nonlinear Dynamics, 112(10), 8299-8327.

[136] Li, M., & Haller, G. (2022). Nonlinear analysis of forced mechanical systems with internal resonance using spectral submanifolds, Part II: Bifurcation and quasi-periodic response. Nonlinear Dynamics, 110(2), 1045-1080.

[137] Durst, F., & Arnold, I. (2008). Fluid mechanics: an introduction to the theory of fluid flows (Vol. 675). Berlin: Springer.

[138] Gomes, J. P., & Lienhart, H. (2013). Fluid–structure interaction-induced oscillation of flexible structures in laminar and turbulent flows. Journal of Fluid Mechanics, 715, 537-572.

[139] Zharkova, V. , Vasilieva, I. , Shepherd, S. and Popova, E. (2023) Periodicities in Solar Activity, Solar Radiation and Their Links with Terrestrial Environment. Natural Science, 15, 111-147. doi: 10.4236/ns.2023.153010.

[140] Williams, B., Kadri, U., & Abdolali, A. (2021). Acoustic–gravity waves from multi-fault rupture. Journal of Fluid Mechanics, 915, A108.

[141] Meza-Valle, C., Kadri, U., & Ortega, J. H. (2023). Acoustic-gravity waves generated by surface disturbances. European Journal of Mechanics-B/Fluids, 98, 1-7.

[142] Warminski, J. (2020). Nonlinear dynamics of self-, parametric, and externally excited oscillator with time delay: van der Pol versus Rayleigh models. Nonlinear Dynamics, 99(1), 35-56.

[143] Sharma, A., & Sinha, S. C. (2020). Control of nonlinear systems exhibiting chaos to desired periodic or quasi-periodic motions. Nonlinear Dynamics, 99(1), 559-574.

[144] Chng, T. L., Orel, I. S., Starikovskaia, S. M., & Adamovich, I. V. (2019). Electric field induced second harmonic (E-FISH) generation for characterization of fast ionization wave discharges at moderate and low pressures. Plasma Sources Science and Technology, 28(4), 045004.

[145] Zhu, Y., Chen, X., Wu, Y., Hao, J., Ma, X., Lu, P., & Tardiveau, P. (2021). Simulation of ionization-wave discharges: a direct comparison between the fluid model and E-FISH measurements. Plasma Sources Science and Technology, 30(7), 075025.

[146] Mishakov, V. G., Suleimenov, I. E., Kuranov, A. L., Tkachenko, T. L., Nekuchaev, V. O., & Pokrovskaya, T. A. (1996). Random behavior of ionization waves in the presence of electron energy losses due to elastic collisions. Plasma Physics Reports, 22.

[147] Guan, Y., Yin, B., Yang, Z., & Li, L. K. (2024). Forced synchronization of self-excited chaotic thermoacoustic oscillations. Journal of Fluid Mechanics, 982, A9.

[148] Sahay, A., Roy, A., Pawar, S. A., & Sujith, R. I. (2021). Dynamics of coupled thermoacoustic oscillators under asymmetric forcing. Physical Review Applied, 15(4), 044011.

[149] Marple Jr, S. L. (2019). Digital spectral analysis. Courier Dover Publications.

[150] Rauscher, C., Janssen, V., & Minihold, R. (2007). Fundamentals of spectrum analysis (Vol. 25). Rohde & Schwarz.

[151] Dutkay, D. E., Picioroaga, G., & Silvestrov, S. (2019). On generalized Walsh bases. Acta Applicandae Mathematicae, 163(1), 73-90.

[152] Pruvost, G., Derbel, B., Liefooghe, A., Verel, S., & Zhang, Q. (2020, June). Surrogate-assisted multi-objective combinatorial optimization based on decomposition and walsh basis. In Proceedings of the 2020 genetic and evolutionary computation conference (pp. 542-550).

[153] Walnut, D. F. (2013). An introduction to wavelet analysis. Springer Science & Business Media.

[154] Guo, T., Zhang, T., Lim, E., Lopez-Benitez, M., Ma, F., & Yu, L. (2022). A review of wavelet analysis and its applications: Challenges and opportunities. IEEe Access, 10, 58869-58903.

[155] Losa, G. A., Ristanović, D., Ristanović, D., Zaletel, I., & Beltraminelli, S. (2016). From fractal geometry to fractal analysis. Applied Mathematics, 7(4), 346-354.

[156] Riley, M. A., Bonnette, S., Kuznetsov, N., Wallot, S., & Gao, J. (2012). A tutorial introduction to adaptive fractal analysis. Frontiers in physiology, 3, 371.

[157] Lu, H. W., Liu, J. C., Chang, C. C., & Horng, J. H. (2024). Reversible Data Hiding in Crypto-Space Images with Polynomial Secret Sharing over Galois Field. Electronics, 13(14), 2860.

[158] Nardo, L. G., Nepomuceno, E. G., Bastos, G. T., Santos, T. A., Butusov, D. N., & Arias-Garcia, J. (2021). A reliable chaos-based cryptography using Galois field. Chaos: An Interdisciplinary Journal of Nonlinear Science, 31(9).

[159] Hazzazi, M. M., Attuluri, S., Bassfar, Z., & Joshi, K. (2023). A novel cipher-based data encryption with Galois field theory. Sensors, 23(6), 3287.

[160] Nazarov, L. E., & Batanov, V. V. (2022). Analysis of Noise Immunity of Optimal Symbol-by-Symbol Reception of Phase-Keyed Signals with Correcting Codes in Non-Binary Galois Fields. Journal of Communications Technology and Electronics, 67(8), 973-978.

[161] Kuo, Y. M., Garcia-Herrero, F., Ruano, O., & Maestro, J. A. (2022). RISC-V Galois field ISA extension for non-binary error-correction codes and classical and post-quantum cryptography. IEEE Transactions on Computers, 72(3), 682-692.

[162] Lehnigk-Emden, T., & Wehn, N. (2010, September). Complexity evaluation of non-binary Galois field LDPC code decoders. In 2010 6th International Symposium on Turbo Codes & Iterative Information Processing (pp. 53-57). IEEE.

[163] Vitulyova, E. S., Matrassulova, D. K., & Suleimenov, I. E. (2021). New application of non-binary Galois fields Fourier transform: Digital analog of convolution theorem. Indonesian Journal of Electrical Engineering and Computer Science, 23(3), 1718-1726.

[164] van der Waerden B.L. Algebra, Vol. 1, Springer-Verlag New York, Inc. 1991, 265 p.

[165] Hubáček, P., Jančová, Ľ., & Králová, V. (2022). On the Distributed Discrete Logarithm Problem with Preprocessing. Cryptology ePrint Archive.

[166] Adj, G., Canales-Martínez, I., Cruz-Cortés, N., Menezes, A., Oliveira, T., Rivera-Zamarripa, L., & Rodríguez-Henríquez, F. (2016). Computing discrete logarithms in cryptographically-interesting characteristic-three finite fields. Cryptology ePrint Archive.

[167] Zhang, J., Yang, Y., Chen, Y., & Chen, F. (2017, June). A secure cloud storage system based on discrete logarithm problem. In 2017 IEEE/ACM 25th International Symposium on Quality of Service (IWQoS) (pp. 1-10). IEEE.

[168] Granger, R., Kleinjung, T., Lenstra, A., Wesolowski, B., & Zumbrägel, J. (2021). Computation of a 30750-bit binary field discrete logarithm. Mathematics of computation, 90(332), 2997-3022.

[169] Wronski, M., & Dzierzkowski, L. (2024). Base of exponent representation matters-more efficient reduction of discrete logarithm problem and elliptic curve discrete logarithm problem to the QUBO problem. Quantum Inf. Comput., 24(7&8), 541-564.

[170] Roetteler, M., Naehrig, M., Svore, K. M., & Lauter, K. (2017, November). Quantum resource estimates for computing elliptic curve discrete logarithms. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 241-270). Cham: Springer International Publishing.

[171] Mohammed, A. (2018). Quantum-Resistant Cryptography: Developing Encryption Against Quantum Attacks. Journal of Innovative Technologies, 1(1).

[172] Adj, G., Menezes, A., Oliveira, T., & Rodriguez-Henriquez, F. (2015). Computing discrete logarithms using Joux's algorithm. ACM Commun. Comput. Algebra, 49(2), 60.

[173] Galbraith, S. D., Wang, P., & Zhang, F. (2015). Computing elliptic curve discrete logarithms with improved baby-step giant-step algorithm. Cryptology ePrint Archive.

[174] Rubinstein-Salzedo, S. (2018). The Diffie–Hellman key exchange and the discrete logarithm problem. In Cryptography (pp. 99-112). Cham: Springer International Publishing.

[175] Pohlig, S. C., & Hellman, M. E. (2022). An improved algorithm for computing logarithms over GF (p) and its cryptographic significance. In Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman (pp. 415-430).

[176] Lin, K., Wang, W., Wang, L., & Zhao, C. A. (2021). An alternative approach for computing discrete logarithms in compressed SIDH. arXiv preprint arXiv:2111.10226.

[177] Barbulescu, R., Gaudry, P., Joux, A., & Thomé, E. (2014, May). A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 1-16). Berlin, Heidelberg: Springer Berlin Heidelberg.

[178] Larasati, H. T., & Kim, H. (2021). Quantum cryptanalysis landscape of Shor's algorithm for elliptic curve discrete logarithm problem. In International Conference on Information Security Applications (pp. 91-104). Springer, Cham.

[179] Ekerå, M. (2019). Revisiting Shor's quantum algorithm for computing general discrete logarithms. arXiv preprint arXiv:1905.09084.

[180] Odlyzko, A. Discrete Logarithms: The Past and the Future. Designs, Codes and Cryptography 19, 129–145 (2000). https://doi.org/10.1023/A:1008350005447

[181] Sarkar, A., Guha Roy, D., Datta, P. (2024). An Overview of the Discrete Logarithm Problem in Cryptography. In: Giri, D., Das, S., Corchado Rodríguez, J.M., De, D. (eds) Proceedings of Third International Conference on Advanced Computing and Applications. ICACA 2024. Lecture Notes in Networks and Systems, vol 1045. Springer, Singapore. https://doi.org/10.1007/978-981-97-4799-3_10.

[182] Hubáček, P., & Václavek, J. (2021). On search complexity of discrete logarithm. arXiv preprint arXiv:2107.02617.

[183] Shaltykova, D.; Vitulyova, Y.; Kadyrzhan, K.; Suleimenov, I. Application of Partial Discrete Logarithms for Discrete Logarithm Computation. Computers 2025, 14, 343. doi: 10.3390/computers14090343

[184] Bakirov, A., Matrassulova, D., Vitulyova, Y., Shaltykova, D., & Suleimenov, I. (2024). The specifics of the Galois field GF (257) and its use for digital signal processing. Scientific Reports, 14(1), 15376.

[185] A., Shanooja M., and Anil Kumar M. N. 2025. "A Technique for Image Encryption Using the Modular Multiplicative Inverse Property of Mersenne Primes" Symmetry 17, no. 2: 166. https://doi.org/10.3390/sym17020166

[186] S. S. Erdem and S. S. Erdem, "Efficient and Constant Time Modular Reduction With Generalized Mersenne Primes," in IEEE Access, vol. 12, pp. 189307-189316, 2024, doi: 10.1109/ACCESS.2024.3514918.

[187] C. Flynt, Tcl/Tk: A Developer's Guide, 3rd ed. Burlington, MA, USA: Morgan Kaufmann (Elsevier), 2012. ISBN: 978-0-12-384717-1.

[188] Xunzhi Jiang, Shen Wang, Yuxin Gong, Tingyue Yu, Li Liu, Xiangzhan Yu, HAformer. Semantic fusion of hex machine code and assembly code for cross-architecture binary vulnerability detection. Computers & Security. Volume 145, 2024, 104029. https://doi.org/10.1016/j.cose.2024.104029.

[189] Jay McCarthy. 2016. Bithoven: Gödel encoding of chamber music and functional 8-bit audio synthesis. In Proceedings of the 4th International Workshop on Functional Art, Music, Modelling, and Design (FARM 2016). Association for Computing Machinery, New York, NY, USA, 1–7. https://doi.org/10.1145/2975980.2975981

[190] M. Doshi and R. Zane, "Digital Architecture for Driving Large LED Arrays with Dynamic Bus Voltage Regulation and Phase Shifted PWM," APEC 07 - Twenty-Second Annual IEEE Applied Power Electronics Conference and Exposition, Anaheim, CA, USA, 2007, pp. 287-293, doi: 10.1109/APEX.2007.357528.

[191] Garg, Sanjam & Gentry, Craig & Halevi, Shai & Raykova, Mariana & Sahai, Amit & Waters, Brent. (2013). Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits. Foundations of Computer Science, 1975., 16th Annual Symposium on. 2013. 40-49. 10.1109/FOCS.2013.13.

[192] Barak, Boaz & Goldreich, Oded & Impagliazzo, Russell & Rudich, Steven & Sahai, Amit & Vadhan, Salil & Yang, Ke. (2001). On the (Im)possibility of Obfuscating Programs. IACR Cryptology ePrint Archive. 2001. 69. 10.1145/2160158.2160159.

[193] Mamatha, D.G., Dimri, N., & Sinha, R. (2024). Post-Quantum Cryptography: Securing Digital Communication in the Quantum Era. ArXiv, abs/2403.11741.

[194] Yalamuri, Gagan & Honnavalli, Prasad & Eswaran, Sivaraman. (2022). A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats. Procedia Computer Science. 215. 834-845. 10.1016/j.procs.2022.12.086.

[195] Preuß Mattsson, John & Smeets, Ben & Thormarker, Erik. (2021). Quantum-Resistant Cryptography. 10.48550/arXiv.2112.00399.

[196] El-hajj, M.; Mousawi, H.; Fadlallah, A. Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platform. Future Internet 2023, 15, 54. https://doi.org/10.3390/fi15020054

[197] Guo, Hognpeng & Liu, Tianyuan & Lui, King-Shan & Danilov, Claudiu & Nahrstedt, Klara. (2020). Secure Broadcast Protocol for Unmanned Aerial Vehicle Swarms. 1-9. 10.1109/ICCCN49398.2020.9209739.

[198] Han, P., Sui, A., & Wu, J. (2025). Lightweight Secure Communication Supporting Batch Authentication for UAV Swarm. Drones, 9(2), 139. https://doi.org/10.3390/drones9020139

[199] He, L., Zhao, M., Wang, X., Wang, J., Wang, Z., & Liu, S. (2025). A Post-Quantum Authentication and Key Agreement Scheme for Drone Swarms. Electronics, 14(17), 3364. https://doi.org/10.3390/electronics14173364

[200] Bogdanov, A. et al. (2007). PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds) Cryptographic Hardware and Embedded Systems - CHES 2007. CHES 2007. Lecture Notes in Computer Science, vol 4727. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74735-2_31

[201] Bogdanov, A., Knežević, M., Leander, G., Toz, D., Varıcı, K., Verbauwhede, I. (2011). SPONGENT: A Lightweight Hash Function. In: Preneel, B., Takagi, T. (eds) Cryptographic Hardware and Embedded Systems – CHES 2011. CHES 2011. Lecture Notes in Computer Science, vol 6917. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-23951-9_21

[202] J. Marcos “On a Problem of da Costa”, Essays on the Foundations of Mathematics and Logic 2 / Ed. by G. Sica. Polimetrica, pp. 53–69, 2005

[203] Lee, E.T. (1995), "Representations of logic functions", Kybernetes, Vol. 24 No. 3, pp. 50-58. https://doi.org/10.1108/03684929510087260

[204] Isupov, K. (2021). High-performance computation in residue number system using floating-point arithmetic. Computation, 9(2), 9.

[205] Kalmykov, I. A., Pashintsev, V. P., Tyncherov, K. T., Olenev, A. A., & Chistousov, N. K. (2022). Error-correction coding using polynomial residue number system. Applied Sciences, 12(7), 3365.

[206] Suleimenov, I., Kadyrzhan, A., Matrassulova, D., & Vitulyova, Y. (2024). Peculiarities of Applying Partial Convolutions to the Computation of Reduced Numerical Convolutions. Applied Sciences (2076-3417), 14(14).

[207] Sarkar, S., Shafaei, S., Jones, T. S., & Totaro, M. W. (2025). Secure Communication in Drone Networks: A Comprehensive Survey of Lightweight Encryption and Key Management Techniques. Drones, 9(8), 583. https://doi.org/10.3390/drones9080583

[208] Dong, Wenlong & Wang, Xiujun & Li, Juyan. (2025). A secure lightweight identity authentication and key agreement scheme for internet of drones. Computer Networks. 270. 111503. 10.1016/j.comnet.2025.111503.

[209] Soto-Cruz, J., Ruiz-Ibarra, E., Vázquez-Castillo, J., Espinoza-Ruiz, A., Castillo-Atoche, A., & Mass-Sanchez, J. (2025). A Survey of Efficient Lightweight Cryptography for Power-Constrained Microcontrollers. Technologies, 13(1), 3. https://doi.org/10.3390/technologies13010003

[210] Hu, Kun & Wang, Mingpei & Ma, Xiaohui & Chen, Jia & Wang, Xiaochao & Wang, Xingjun. (2024). Learning-based image steganography and watermarking: A survey. Expert Systems with Applications. 249. 123715. 10.1016/j.eswa.2024.123715.

[211] Alzoubi, Yehia & Mishra, Alok. (2025). Differential privacy and artificial intelligence: potentials, challenges, and future avenues. EURASIP Journal on Information Security. 2025. 10.1186/s13635-025-00203-9.

[212] Pan Cao, Lei Lei, Shengsuo Cai, Gaoqing Shen, Xiaojiao Liu, Xinyi Wang, Lijuan Zhang, Liang Zhou, and Mohsen Guizani. 2024. Computational Intelligence Algorithms for UAV Swarm Networking and Collaboration: A Comprehensive Survey and Future Directions. Commun. Surveys Tuts. 26, 4 (Fourthquarter 2024), 2684–2728. https://doi.org/10.1109/COMST.2024.3395358

[213] Alqudsi, Yunus & Makaraci, Murat. (2025). UAV swarms: research, challenges, and future directions. Journal of Engineering and Applied Science. 72. 10.1186/s44147-025-00582-3.

[214] Conceição, Maria & Grilo, Antonio & Basiri, Meysam. (2025). Communication and Motion Coordination Awareness in Networked Aerial Robot Teams. Ad Hoc Networks. 176. 103875. 10.1016/j.adhoc.2025.103875.

[215] Jung, W., Park, C., Lee, S., & Kim, H. (2024). Enhancing UAV Swarm Tactics with Edge AI: Adaptive Decision Making in Changing Environments. Drones, 8(10), 582. https://doi.org/10.3390/drones8100582

[216] Adoni, W. Y. H., Fareedh, J. S., Lorenz, S., Gloaguen, R., Madriz, Y., Singh, A., & Kühne, T. D. (2024). Intelligent Swarm: Concept, Design and Validation of Self-Organized UAVs Based on Leader–Followers Paradigm for Autonomous Mission Planning. Drones, 8(10), 575. https://doi.org/10.3390/drones8100575

[217] Kalimoldayev, M. N.; Pak, I. T.; Baipakbayeva, S. T.; Mun, G. A.; Shaltykova, D. B.; & Suleimenov, I. E. Methodological basis for the development strategy of artificial intelligence systems in the Republic of Kazakhstan in the message of the president of the Republic of Kazakhstan dated October 5, 2018. News of the National Academy of Sciences of the Republic of the Kazakhstan–Series of geology and technical sciences. 2018, 6, 47-54. https://doi.org/10.32014/2018.2518-170X.34.

[218] Sandhie, Zarin Tasnim & Patel, Jill & Ahmed, Farid Uddin & Chowdhury, Masud. (2021). Investigation of Multiple-valued Logic Technologies for Beyond-binary Era.

[219] Wang, Xiao-Yuan & Dong, Chuan-Tao & Wu, Zhi-Ru & Cheng程, Zhi-Qun知群. (2021). A review on the design of Ternary Logic Circuits. Chinese Physics B. 30. 10.1088/1674-1056/ac248b.

[220] Suleimenov, I. E., Bakirov, A. S., & Matrassulova, D. K. (2021). A technique for analyzing neural networks in terms of ternary logic. Journal of Theoretical and Applied Information Technology, 99(11), 2537-2553.

ПРИЛОЖЕНИЕ А

Патент

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ РЕСПУБЛИКА КАЗАХСТАН

REPUBLIC OF KAZAKHSTAN

ПАТЕНТ
PATENT

№ 37453

ӨНЕРТАБЫСҚА / НА ИЗОБРЕТЕНИЕ / FOR INVENTION

(21) 2024/0382.1

(22) 14.05.2024

(45) 01.08.2025

(54) Ұшқышсыз көлікті іске асыруға негізделген әуе ок-дәрілерін тасымалдайтын тәсіл
Способ реализации беспилотного аппарата-носителя боеприпаса воздушного базирования
Method for implementing an unmanned aerial vehicle-airborne munition carrier

(73) Сулейменов Ибрагим Эсенович (KZ); Байпакбаева Салтанат Туркестанкызы (KZ); Қадыржан Аружан Булатовна (KZ); Мун Григорий Алексеевич (KZ)
Suleimenov Ibragim Esenovich (KZ); Baipakbaeva Saltanat Turkestankyzy (KZ); Kadyrzhan Aruzhan Bulatovna (KZ); Mun Grigory Alekseevich (KZ)

(72)

Мун Григорий Алексеевич (KZ)	Mun Grigory Alekseevich (KZ)
Байпакбаева Салтанат Туркестанкызы (KZ)	Baipakbaeva Saltanat Turkestankyzy (KZ)
Кабдушев Шернияз Булатулы (KZ)	Kabdushev Sherniyaz Bulatuly (KZ)
Қадыржан Қайсарәлі Нұрланұлы (KZ)	Kadyrzhan Kaisarali Nurlanuly (KZ)
Қадыржан Аружан Булатовна (KZ)	Kadyrzhan Aruzhan Bulatovna (KZ)
Витулёва Елизавета Сергеевна (KZ)	Vitulyova Yelizaveta Sergeyevna (KZ)
Сулейменов Ибрагим Эсенович (KZ)	Suleimenov Ibragim Esenovich (KZ)

ЭЦҚ қол қойылды
Подписано ЭЦП
Signed with EDS

С. Ахметов
С. Ахметов
S. Akhmetov

«Ұлттық зияткерлік меншік институты» РМК директоры
Директор РГП «Национальный институт интеллектуальной собственности»
Director of the «National Institute of Intellectual Property» RSE

ПРИЛОЖЕНИЕ Б

Акт внедрения

Акт внедрения результатов научно-исследовательских, научно-технических работ, (или) результатов научной и (или) научно-технической деятельности

1. Наименование научно-исследовательских, научно-технических работ и (или) результатов научной и (или) научно-технической деятельности:

«Разработка новых средств защиты информации в зоне прямой радиовидимости».

2. Краткая аннотация:

В диссертационной работе разработан и обоснован комплексный подход к защите командно-информационного обмена при групповом применении БПЛА в условиях прямой радиовидимости. Предложена архитектура, сочетающая внутригрупповую волоконно-оптическую синхронизацию/обмен для повышения устойчивости координации и уменьшения требований к межбортовой синхронизации, а также радиотехническую идентификацию источника команд на основе измерения разностей времени прихода и/или фазовых разностей между сигналами, принимаемыми бортами формации из трёх БПЛА, с геометрической обработкой по пересечениям асимптот гипербол. Для задач анализа квазигармонических сигналов рассмотрен метод извлечения мгновенных параметров (частоты, амплитуды, фазы) с использованием фазовых портретов. Разработан аппаратно-ориентированный метод вычисления дискретных логарифмов в квазимерсенновских полях Галуа вида GF(2^n+1) с использованием разреженных разложений Фурье–Галуа и знакочередующей двоичной кодировки; на его основе предложен метод обфускации данных для 256-уровневых каналов. Полученные результаты предназначены для применения в встраиваемых средствах управления и защиты каналов связи группы БПЛА при ограниченных вычислительных и энергетических ресурсах.

3. Эффект от внедрения (экономический, социальный, экологический), подчеркнуть область эффекта):

Социально-экономический эффект: повышение защищённости и надёжности управления группой БПЛА снижает риск несанкционированного воздействия на канал управления (подмена команд, радиопомехи/спуфинг), повышает безопасность эксплуатации в гражданских и ведомственных

сценариях (мониторинг, поисково-спасательные работы, охрана объектов), а также уменьшает затраты на развертывание и сопровождение защищённой инфраструктуры связи за счёт аппаратно-ориентированных решений с умеренными ресурсными требованиями.

4. Место и время внедрения:

г. Алматы, Байтурсынулы, д. 113, дата: 04.08.2025 г.

5. Форма внедрения:

Внедрение разработанных методов и алгоритмов в опытно-экспериментальные исследования и учебно-исследовательские работы по тематике защищённого управления группой БПЛА: использование в составе стенда/прототипа канала передачи команд для оценки устойчивости к подмене и радиопомехам, а также применение предложенных алгоритмов преобразования (обфускации) данных и процедур радиотехнической идентификации источника команд при разработке и отработке технических решений.

Подписи:

1. Представитель/представители заявителя (налогоплательщик), внедривший результаты научно-исследовательских, научно-технических работ и (или) результаты научной и (или) научно-технической деятельности

НАО АУЭС, Докторант _____ (подпись) А.Б. Қадыржан

НАО АУЭС, Научный руководитель профессор, доктор PhD _____ (подпись) Ж. Әлғазы

2. Представитель/представители организации исполнителя научно-исследовательских, научно-технических работ и (или) научной и (или) научно-технической деятельности (внедренных)

НАО АУЭС, зав.каф. Аэрокосмической и электронной инженерии Доктор PhD _____ (подпись) Е.С. Нұрғизат

Согласовано:

Представитель/представители уполномоченного органа соответствующей отрасли, в которой были внедрены результаты научно-исследовательских, научно-технических работ и (или) результаты научной и (или) научно-технической деятельности

ТОО «НИИ «ПРИКЛАДНЫХ НАУК И ТЕХНОЛОГИЙ»»
Директор А.М. Узбекбаев

ПРИЛОЖЕНИЕ В

Код

```
"""
Python implementation for constructing hyperbola asymptotes and intersection points.

Purpose:
    Given three foci on a circle (one common focus F0 and two other foci F1, F2),
    and a reference point P0, the script:
      1) computes delta1, delta2 such that P0 lies on both hyperbolas,
      2) constructs asymptotes of both hyperbolas in closed form,
      3) computes four intersection points of the asymptotes,
      4) plots the geometry and saves the figure.

Key inputs:
    R          : circle radius for foci placement
    phi1_deg   : angle of F1 on the circle (degrees)
    phi2_deg   : angle of F2 on the circle (degrees)
    rho0       : radius of P0 in polar coordinates
    theta0_deg : angle of P0 in polar coordinates (degrees)

Outputs:
    Printed: delta1, delta2, and intersection coordinates
    Saved:   a PNG figure with foci, asymptotes, and intersections
"""

import numpy as np
import math
import matplotlib.pyplot as plt


def circle_point(R: float, phi: float) -> np.ndarray:
    """
    Point on a circle of radius R at polar angle phi (radians).

    Returns:
        np.ndarray([x, y])
    """
    return np.array([R * math.cos(phi), R * math.sin(phi)], dtype=float)


def asymptotes_from_foci_and_delta(Fc, F, delta, tol: float = 1e-12):
    """
    Constructs asymptotes for a hyperbola defined by:
        |X - Fc| - |X - F| = delta.

    Geometry:
        For a hyperbola with foci Fc and F, the distance between foci is d.
        Standard parameters:
            2a = |delta|
            2c = d
            b = sqrt(c^2 - a^2)
```

```
        Real (non-degenerate) hyperbola requires:
            a < c  <=>  |delta| < d

    Returns:
        (m, d_plus, d_minus), where
            m       : center of the hyperbola
            d_plus  : direction vector of the 1st asymptote
            d_minus : direction vector of the 2nd asymptote

    If the hyperbola is degenerate/non-real (|delta| >= |F-Fc|), returns None.
    """
    Fc = np.array(Fc, dtype=float)
    F = np.array(F, dtype=float)

    d = np.linalg.norm(F - Fc)
    if d < tol:
        return None

    # Standard parameters: 2a = |delta|, 2c = d
    a = abs(delta) / 2.0
    c = d / 2.0

    # Real non-degenerate hyperbola requires |delta| < d
    if a >= c - tol:
        return None

    b = math.sqrt(max(c * c - a * a, 0.0))

    # Local orthonormal basis:
    # ex is along the foci axis, ey is perpendicular to ex
    ex = (F - Fc) / d
    ey = np.array([-ex[1], ex[0]], dtype=float)

    # Center of the hyperbola is the midpoint between foci
    m = (Fc + F) / 2.0

    # Asymptotes in local coordinates: y = ±(b/a) x
    # Direction vectors (a, ±b) mapped to global frame:
    d_plus = a * ex + b * ey
    d_minus = a * ex - b * ey

    return m, d_plus, d_minus


def line_intersection(p1, d1, p2, d2, tol: float = 1e-12):
    """
    Intersection of infinite 2D lines:
        L1: p1 + t d1
        L2: p2 + s d2

    Returns:
        intersection point (np.ndarray shape (2,)) or None if lines are parallel.
```

```
    """
    p1 = np.array(p1, dtype=float)
    d1 = np.array(d1, dtype=float)
    p2 = np.array(p2, dtype=float)
    d2 = np.array(d2, dtype=float)

    def cross2(a, b) -> float:
        """2D cross product (scalar): a_x*b_y - a_y*b_x."""
        return a[0] * b[1] - a[1] * b[0]

    denom = cross2(d1, d2)
    if abs(denom) < tol:
        # Parallel (or nearly parallel) lines: no robust intersection
        return None

    t = cross2(p2 - p1, d2) / denom
    return p1 + t * d1


def build_and_plot(
    R: float = 1.0,
    phi1_deg: float = 60.0,
    phi2_deg: float = 150.0,
    rho0: float = 6.0,
    theta0_deg: float = 20.0,
    save_path: str = "hyperbola_asymptote_intersections.png",
):
    """
    Constructs and plots:
      - circle of radius R
      - foci F0 (common on OX), F1(phi1), F2(phi2)
      - reference point P0(rho0, theta0)
      - asymptotes of two hyperbolas:
            H1: |X-F0| - |X-F1| = delta1
            H2: |X-F0| - |X-F2| = delta2
        where delta1, delta2 are computed from P0
      - 4 intersection points of asymptotes (2x2): I1..I4

    Prints deltas and intersection coordinates for verification.
    """
    phi1 = math.radians(phi1_deg)
    phi2 = math.radians(phi2_deg)
    theta0 = math.radians(theta0_deg)

    # Common focus (example geometry)
    F0 = np.array([R, 0.0], dtype=float)

    # Other foci on the circle
    F1 = circle_point(R, phi1)
    F2 = circle_point(R, phi2)

    # Reference point in polar coordinates
```

```
P0 = np.array([rho0 * math.cos(theta0), rho0 * math.sin(theta0)], dtype=float)

# Deltas derived from P0 so that P0 lies on both hyperbolas
delta1 = np.linalg.norm(P0 - F0) - np.linalg.norm(P0 - F1)
delta2 = np.linalg.norm(P0 - F0) - np.linalg.norm(P0 - F2)

A1 = asymptotes_from_foci_and_delta(F0, F1, delta1)
A2 = asymptotes_from_foci_and_delta(F0, F2, delta2)

if A1 is None or A2 is None:
    raise ValueError(
        "Degenerate/non-real hyperbola for these parameters. "
        "Check the condition |delta| < distance_between_foci."
    )

m1, d1p, d1m = A1
m2, d2p, d2m = A2

# 4 intersections: each asymptote of H1 with each asymptote of H2
lines1 = [(m1, d1p), (m1, d1m)]
lines2 = [(m2, d2p), (m2, d2m)]

intersections = []
for p1, v1 in lines1:
    for p2, v2 in lines2:
        intersections.append(line_intersection(p1, v1, p2, v2))

# Plot extents based on all key points
pts = [F0, F1, F2, P0] + [q for q in intersections if q is not None]
max_norm = max(np.linalg.norm(p) for p in pts)
lim = max(1.6 * max_norm, 2.5 * R)

fig, ax = plt.subplots(figsize=(7.2, 7.2), dpi=180)

# Circle
ang = np.linspace(0, 2 * np.pi, 400)
ax.plot(R * np.cos(ang), R * np.sin(ang),
        linewidth=1.2, alpha=0.6, label="Circle of foci (R)")

# Foci
ax.scatter([F0[0], F1[0], F2[0]], [F0[1], F1[1], F2[1]], s=55, marker="o")
ax.annotate("F0 (common)", F0 + np.array([0.08 * R, 0.08 * R]))
ax.annotate("F1", F1 + np.array([0.08 * R, 0.08 * R]))
ax.annotate("F2", F2 + np.array([0.08 * R, 0.08 * R]))

# Reference point
ax.scatter([P0[0]], [P0[1]], s=70, marker="*", zorder=5)
ax.annotate("P0 (given)", P0 + np.array([0.10 * R, 0.10 * R]))

# Helper: draw a long segment for each asymptote line
def draw_line(point, direction, label=None):
    d = np.array(direction, dtype=float)
```

```
    d = d / (np.linalg.norm(d) + 1e-15)
    p = np.array(point, dtype=float)
    t = np.array([-lim, lim])
    seg = p[None, :] + t[:, None] * d[None, :]
    ax.plot(seg[:, 0], seg[:, 1], linewidth=1.1, alpha=0.85, label=label)

# Asymptotes of both hyperbolas
draw_line(m1, d1p, label="Asymptotes of H1 (F0,F1)")
draw_line(m1, d1m)
draw_line(m2, d2p, label="Asymptotes of H2 (F0,F2)")
draw_line(m2, d2m)

# Intersection points
labels = ["I1", "I2", "I3", "I4"]
for i, q in enumerate(intersections):
    if q is None:
        continue
    ax.scatter([q[0]], [q[1]], s=45, marker="x", zorder=6)
    ax.annotate(labels[i], q + np.array([0.12 * R, 0.12 * R]))

# Axes and formatting
ax.axhline(0, linewidth=0.8, alpha=0.4)
ax.axvline(0, linewidth=0.8, alpha=0.4)
ax.set_aspect("equal", adjustable="box")
ax.set_xlim(-lim, lim)
ax.set_ylim(-lim, lim)
ax.grid(True, alpha=0.25)

ax.set_title("Intersections of hyperbola asymptotes (parameters from P0)")
ax.set_xlabel("x")
ax.set_ylabel("y")
ax.legend(loc="upper right", fontsize=8, framealpha=0.85)

fig.tight_layout()
fig.savefig(save_path, bbox_inches="tight")
plt.close(fig)

# Numeric output for verification
print("Input parameters:")
print(f"  R={R}, phi1={phi1_deg}°, phi2={phi2_deg}°, rho0={rho0}, theta0={theta0_deg}°")
print("Deltas (from P0):")
print(f"  delta1 = |P0-F0| - |P0-F1| = {delta1:.6f}")
print(f"  delta2 = |P0-F0| - |P0-F2| = {delta2:.6f}")
print("Intersection points (I1..I4):")
for i, q in enumerate(intersections, start=1):
    if q is None:
        print(f"  I{i}: parallel lines (no intersection)")
    else:
        print(f"  I{i}: ({q[0]:.6f}, {q[1]:.6f})")
print(f"Saved figure to: {save_path}")
```

```
if __name__ == "__main__":
    # Example run (edit parameters here)
    build_and_plot(
        R=1.0,
        phi1_deg=60.0,
        phi2_deg=150.0,
        rho0=6.0,
        theta0_deg=20.0,
        save_path="hyperbola_asymptote_intersections.png",
    )
```